Natarajan Meghanathan
Dhinaharan Nagamalai (Eds)

Computer Science & Information Technology

9th International Conference on Computer Science, Engineering and Applications (CCSEA 2019) July 13~14, 2019, Toronto, Canada

AIRCC Publishing Corporation

Volume Editors

Natarajan Meghanathan,
Jackson State University, USA
E-mail: nmeghanathan@jsums.edu

Dhinaharan Nagamalai,
Wireilla Net Solutions, Australia
E-mail: dhinthia@yahoo.com

ISSN: 2231 - 5403
ISBN: 978-1-925953-05-3
DOI : 10.5121/csit.2019.90901- 10.5121/csit.2019.90931

Typesetting: Camera-ready by author, data conversion by NnN Net Solutions Private Ltd., Chennai, India

Preface

The 9th International Conference on Computer Science, Engineering and Applications (CCSEA 2019), July 13~14, 2019, Toronto, Canada, 8th International Conference on Cloud Computing: Services and Architecture (CLOUD 2019), 5th International Conference on Signal and Image Processing (SIPRO 2019), 7th International Conference on Data Mining & Knowledge Management Process (DKMP 2019), 5th International Conference on Artificial Intelligence and Applications (AIFU 2019), 8th International Conference on Software Engineering and Applications (SEA 2019), 5th International Conference on Networks & Communications (NCOM 2019)was collocated with 9th International Conference on Computer Science, Engineering and Applications (CCSEA 2019) The conferences attracted many local and international delegates, presenting a balanced mixture of intellect from the East and from the West.

The goal of this conference series is to bring together researchers and practitioners from academia and industry to focus on understanding computer science and information technology and to establish new collaborations in these areas. Authors are invited to contribute to the conference by submitting articles that illustrate research results, projects, survey work and industrial experiences describing significant advances in all areas of computer science and information technology.

The CCSEA 2019, CLOUD 2019, SIPRO 2019, DKMP 2019, AIFU 2019, SEA 2019, NCOM 2019 Committees rigorously invited submissions for many months from researchers, scientists, engineers, students and practitioners related to the relevant themes and tracks of the workshop. This effort guaranteed submissions from an unparalleled number of internationally recognized top-level researchers. All the submissions underwent a strenuous peer review process which comprised expert reviewers. These reviewers were selected from a talented pool of Technical Committee members and external reviewers on the basis of their expertise. The papers were then reviewed based on their contributions, technical content, originality and clarity. The entire process, which includes the submission, review and acceptance processes, was done electronically.

In closing, CCSEA 2019, CLOUD 2019, SIPRO 2019, DKMP 2019, AIFU 2019, SEA 2019, NCOM 2019 brought together researchers, scientists, engineers, students and practitioners to exchange and share their experiences, new ideas and research results in all aspects of the main workshop themes and tracks, and to discuss the practical challenges encountered and the solutions adopted. The book is organized as a collection of papers from the CCSEA 2019, CLOUD 2019, SIPRO 2019, DKMP 2019, AIFU 2019, SEA 2019, NCOM 2019

We would like to thank the General and Program Chairs, organization staff, the members of the Technical Program Committees and external reviewers for their excellent and tireless work. We sincerely wish that all attendees benefited scientifically from the conference and wish them every success in their research. It is the humble wish of the conference organizers that the professional dialogue among the researchers, scientists, engineers, students and educators continues beyond the event and that the friendships and collaborations forged will linger and prosper for many years to come.

Natarajan Meghanathan
Dhinaharan Nagamalai

Organization

General Chair

Natarajan Meghanathan	Jackson State University, USA
Dhinaharan Nagamalai,	Wireilla Net Solutions, Australia

Program Committee Members

Abd El-Aziz Ahmed,	Cairo University, Egypt
Abdelmajid Hajami,	FST Settat, Morocco
Ahmed Nabih Zaki Rashed,	Menoufia University, Egypt
Carlos Juiz,	University Of The Balearic Islands, Spain
Dac-Nhuong Le,	Haiphong University, Vietnam
Daniel Ekpenyong Asuquo,	University of Uyo, Nigeria
Der-Chyuan Lou,	Chang Gung University, Taiwan
Dinh-Thuan Do,	Eastern International University, Vietnam
El Mostapha Aboulhamid,	Universite de Montreal, Canada
Emad Awada,	Applied Science University, Jordan
Fatiha Boubekeur,	Mouloud Mammeri University Of Tizi-Ouzou, Algeria
Hamid Alasadi,	Basra University, Iraq
Isa Maleki,	Islamic Azad University, Iran
Ishfaq Ahmad,	The University of Texas at Arlington, U.S.A
Ivo Pierozzi Junior,	Embrapa Agricultural Informatics, Brazil
Jafar Mansouri,	Ferdowsi University of Mashhad, Iran
Jamal El Abbadi,	Mohammadia V University Rabat, Morocco
John Tass,	University of Patras, Greece
Jun Zhang,	South China University of Technology, China
Mamun Bin Ibne Reaz,	Universiti Kebangsaan, Malaysia
Baghdad Atmani,	University of Oran, Algeria
Bahram Lavi,	EMU, North Cyprus
Bhagwati Prasad Chamola,	Jaypee Institute of Information Technology-Noida, India
Bilal H. Abed-Alguni,	Yarmouk University Irbid, Jordan
Brent Langhals,	Air Force Institute of Technology, United States
Deepak Garg,	Bennett University, India
Francesco Tajani,	Sapienza University of Rome, Italy
Hamed Taherdoost,	Hamta Business Solution Sdn Bhd, Malaysia
Himanshu Mehta,	Eurecom and Telecom ParisTech, France
Isa Maleki,	Islamic Azad University, Iran
Issam Haamdi,	Universite de Sfax, Tunisia
Jinde Cao,	Southeast University, China
Juan J. Flores,	University of Michoacan, Mexico
Karim Djem,	University of Leeds, UK
Karima BERRAMLA,	Teacher at university of ain temouchent, Algeria
Mamoun Alazab,	Macquarie University, Australia

Technically Sponsored by

Computer Science & Information Technology Community (CSITC)

Artificial Intelligence Community (AIC)

Soft Computing Community (SCC)

Digital Signal & Image Processing Community (DSIPC)

Organized By

Academy & Industry Research Collaboration Center (AIRCC)

TABLE OF CONTENTS

9th International Conference on Computer Science, Engineering and Applications (CCSEA 2019)

Automatic Extraction of Feature Lines on 3D Surface…… 01 - 11
Zhihong Mao, Ruichao Wang and Yulin Zhou

Context-Aware Trust-Based Access Control For Ubiquitous Systems……...13 - 32
Malika Yaici, Faiza Ainennas and Nassima Zidi

Construction Of an Oral Cancer Auto-Classify system Based On Machine-Learning for Artificial Intelligence ..... 33 - 39
Meng-Jia Lian, Chih-Ling Huang and Tzer-Min Lee

Efficient Tough Random Symmetric 3-SAT Generator……. 41 - 49
Robert Amador, Chen-Fu Chiang, and Chang-Yu Hsieh

Data Analysis of Wireless Networks Using Classification Techniques……51 - 61
Daniel Rosa Canêdo and Alexandre Ricardo Soares Romariz

A Survey of State-of-the-Art GAN-based Approaches To Image Synthesis…. 63 - 76
Shirin Nasr Esfahani and Shahram Latifi

IoT -Based Approach To Monitor Parking Space In Cities ……77 - 84
Fatin Farhan Haque, Weijia Zhou, Jun-Shuo Ng, Ahmed Abdelgawad, Kumar Yelamarthi and Frank Walsh

Query Performance Optimization in Databases for Big Data ……..…….. 85 - 90
Manoj Muniswamaiah, Dr. Tilak Agerwala and Dr. Charles Tappert

Maximizing the Total Number of On TIME Jobs on Identical Machines…... 91 - 97
Hairong Zhao

8th International Conference on Cloud Computing: Services and Architecture (CLOUD 2019)

Service Level Driven Job Scheduling in Multi-Tier Cloud Computing: A Biologically Inspired Approach…… 99 - 118
Husam Suleiman and Otman Basir

Threat Modelling for the Virtual Machine Image in Cloud Computing…… 119 - 132
Raid Khalid Hussein and Vladimiro Sassone

QOS-Driven Job Scheduling: Multi-Tier Dependency Considerations……. 133 - 155
Husam Suleiman and Otman Basir

Trust Modelling for Security of IoT Devices …….…….. 157 - 167
Naresh K. Sehgal, Shiv Shankar and John M. Acken

Virtual Enterprise Architecture Supply Chain (VEASC) Model on Cloud Computing: A simulation-based study through OPNET modeling ……... 169 - 186
Tlamelo Phetlhu and Sam Lubbe

Security Considerations for Edge Computing ……. 187 - 194
John M. Acken and Naresh K. Sehgal

A Map Reduce based Algorithm for Data Migration in a Private Cloud Environment …… 195 - 212
Anurag Kumar Pandey, Ruppa K. Thulasiram and A. Thavaneswaran

Integrating Cloud Computing to Solve ERP Cost Challenge ……. 213 - 219
Amal Alhosban and Anvitha Akurathi

Challenges of Big Data Applications in Cloud Computing …… 221 - 232
Manoj Muniswamaiah, Dr. Tilak Agerwala and Dr. Charles Tappert

Security Issues in Cloud-Based Businesses …… 341 - 352
Mohamad Ibrahim AL Ladan

Enabling Edge Computing Using Container Orchestration and Software Defined Wide Area Networks…… 353 - 372
Felipe Rodriguez Yaguache and Kimmo Ahola

5th International Conference on Signal and Image Processing (SIPRO 2019)

Blind Image Quality Assessment Using Singular Value Decomposition Based Dominant Eigenvectors for Feature Selection…….. 233 - 242
Besma Sadou, Atidel Lahoulou, Toufik Bouden, Anderson R. Avila, Tiago H. Falk and Zahid Akhtar

Motion Compensated Restoration of Colonoscopy Images …… 243 - 256
Nidhal Azawi and John Gauch

Sea Surface Electromagnetic Scattering Characteristics of JONSWAP Spectrum Influenced by its Parameters ……..… 257 - 265
Xiaolin Mi, Xiaobing Wang, Xinyi He and Fei Dai

Three-Dimensional Reconstruction Using the Depth Map ……. 267 - 274
A.El abderrahmani , R.Lasri and K.Satori

5th International Conference on Artificial Intelligence and Applications (AIFU 2019)

Data Augmentation Based on Pixel-level Image Blend and Domain Adaptation ……275 - 285
Di LIU,Xiao-Chun HOU,Yan-Bo LIU , Lei Liu and Yan-Cheng Wang

Effective Service Composition Approach based on Pruning Performance Bottlenecks …….. 287 - 296
Navinderjit Kaur Kahlon and Kuljit Kaur Chahal

Ensemble Learning Using Frequent Itemset Mining for Anomaly Detection …….. 373 - 389
Saeid Soheily-Khah and Yiming Wu

8th International Conference on Software Engineering and Applications (SEA 2019)

Data Virtualization for Analytics and Business Intelligence in Big Data ….. 297 - 302
Manoj Muniswamaiah, Tilak Agerwala and Charles Tappert

An Innovative Approach to User Interface Engineering …… 303 - 314
Pradip Peter Dey, Bhaskar Raj Sinha, Mohammad Amin and Hassan Badkoobehi

7th International Conference on Data Mining & Knowledge Management Process (DKMP 2019)

Attribute Reduction and Decision Tree Pruning to Simplify Liver Fibrosis Prediction Algorithms a Cohort Study …….. 315 - 326
Mahasen Mabrouk, Abubakr Awad, Hend Shousha, Wafaa Alakel,Ahmed Salama and Tahany Awad

5th International Conference on Networks & Communications (NCOM 2019)

Optimizing DSCP Marking to Ensure VoIP's QoS over HFC Network ….. 327 – 339
Shaher Daoud and Yanzhen Qu

AUTOMATIC EXTRACTION OF FEATURE LINES ON 3D SURFACE

Zhihong Mao, Ruichao Wang and Yulin Zhou

Division of Intelligent Manufacturing, Wuyi University,
Jiangmen529020, China

ABSTRACT

Many applications in mesh processing require the detection of feature lines. Feature lines convey the inherent features of the shape. Existing techniques to find feature lines in discrete surfaces are relied on user-specified thresholds, inaccurate and time-consuming. We use an automatic approximation technique to estimate the optimal threshold for detecting feature lines. Some examples are presented to show our method is effective, which leads to improve the feature lines visualization.

KEY WORDS

Feature Lines; Extraction; Meshes

1. INTRODUCTION

Advances in scanner technology and algorithms for constructing polygonal meshes made polygonal models currently dominate the field of 3D computer graphics. In addition, meshes support wide variations in complexity. Almost any shape representation may be converted with arbitrary accuracy to a polygonal mesh. Fine shape representation is important for 3D geometry processing, such as shape analysis, shape matching and shape editing. Many applications in mesh processing require the detection of feature lines. Feature lines convey the inherent features of the shape. Mathematically feature lines are described via extrema of the surface principal curvatures along their corresponding lines of curvature, which are traced by using high-order curvature derivatives. Forrester Cole et al. [1] pointed out that current computer graphics line drawing techniques can effectively depict shape and even match the effectiveness of artist's drawings, and that errors in depiction are often localized.

Recent research in 3D computer graphics has focused on estimating feature lines over triangle mesh models [2-6]. The basic idea of these papers is first to robustly estimate surface principal curvature and then to identify the feature lines as lines of curvature extrema. Polygonal surface models usually have large flat regions with sharp creases on which the surface bend sharply.

One obvious way to extract the sharp creases from the model is to select a threshold T that separates these points with surface curvature extrema. Because of its intuitive properties and simplicity of implementation, the threshold method is used by most existing methods to achieve the extraction of the sharp features on a mesh model. The success of this method depends largely on how to set the threshold. Unfortunately, improper threshold produces many spurious feature lines. It is difficult for a user to modify the threshold if no any apriori knowledge. A successful outcome demands a lot of skills for the threshold method.

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 01-11, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90901

We present an automatic method for robustly extracting feature lines on triangle mesh models. In the first step, fundamental descriptors for shape analysis--namely, the principal curvature and corresponding direction—are computed for each vertex in the mesh. However, the computation of curvature and its derivatives is sensitive to noise and irregularities of the triangulation. In order to accurately extract the feature lines, in the second step we introduce the saliency value [7, 8] computed by a linear combination of the maximal absolute curvature and the absolute curvature difference, a measure of regional importance for graphics meshes, to reduce the false feature points. Finally, we automatically determine the threshold according to the saliency value.

The paper is structured as follows. Section 2 reviews related work. Section 3 describes necessary background of differential geometry. Section 4 describes the automatic algorithm to robustly extract feature lines from triangulated meshes. Section 5 presents some results and compares them to the other methods. Section 6 concludes the paper.

2. RELATED WORK

Many applications in 3D computer graphics require the extraction of feature lines in a discrete mesh. Mathematically feature lines are defined as extrema of the principal curvatures corresponding to their curvature directions. So extraction of feature lines requires estimation of the principal curvature and direction as a first step.

Estimation of Curvature Briefly, Curvature estimation methods can be categorized as follows: 1) Normal curvature approximation method where the Weingarten matrix is used to estimate the principal curvature and direction [9, 10]. 2) Surface (curve) fitting method where a polynomial surface (curve) is fitted to points in a local region [11, 12]. 3) Discrete differential geometry method [13, 14] where discrete versions of differential geometry theorems, such as the Laplace-Beltrami operator and Gauss-Bonnet theorem, are developed and applied to the neighborhood of each vertex. However, a purely curvature-based metric may not necessarily be a good metric of feature lines extraction. Non-uniform sampling, noise and irregularities of triangulation make the curvature-based method to often get false feature lines or incomplete feature lines.

Saliency Value Saliency map [15] that assigns a saliency value to each image pixel has done excellent work in image processing. By the saliency value, salient image edges will be distinct from their surroundings. Encouraged by the success of the method on 2D problem, Lee [7] introduces the idea of mesh saliency as a measure of regional importance for graphics meshes. Lee discusses how to apply the saliency value to graphics applications such as mesh simplification and viewpoint selection. Ran Gal [8] defined salient geometric features for partial shape matching and similarity by the salient parts of an object. By “salience of a part”, he captured the object’s shape with a small number of parts. He proposed that the salience of a part depends on (at least) two factors: its size relative to the whole object, the number of curvature changes and strength. Similar to the two methods, we will compute the saliency value of each mesh point for our automatic algorithm.

Extraction of Feature Lines Feature lines are curves of curvature extrema and therefore encode important information used in segmentation, registration, matching and surface analysis. Sometimes we also call them ridges and valleys or crest lines.

Feature lines extraction techniques aimed to build an economical and accurate representation of surface features have become increasingly popular in computer graphics[16, 17, 23]. A number of approaches have been described. Feature lines extraction can be roughly classified into image-based method and model-based method. Image-based method extracts feature lines on a rendered projection image by edge detection algorithm in image processing [16]. The result is visually

pleasing and less computational complexity. But pixel-based representation gives low precision. Model-based method extracts lines directly on 3D models in term of the differential geometric properties of the surface. Benefited from the development of 3D scanning techniques, digitizing the model by a high resolution makes it possible to depict the differential geometric properties on the digital model.

There are a number of lines that serve to extract the geometric linear features of the surface. The first class is view-dependent curves. The silhouette (contour) is the curves that are only defined with respect to a viewing screen. Suggestive contours are contours that would first appear with a minimal change in viewpoint [18]. Apparent ridges are defined as the ridges of view-dependent curvature, the variation of surface normal with respect to a viewing screen plane [6]. View-dependent curves depend on the viewing direction and produce visually pleasing line drawings. So they are usually used for non-photorealistic rendering methods. The second class is view-independent curves that depend only on the differential geometric properties of the surface. Many researchers have tried to depict the shape of the 3D model with a high-quality feature lines. But the features are traced using high-order curvature derivatives and are not easy to be detected from discrete surface. The most common curves are ridges and valleys which occur at points of extremal principal curvatures. This paper focuses on the problem of accurately detecting feature lines on surfaces. Ohtake et al. [2] proposed a method for detecting ridge-valley lines by combining multi-level implicit surface fitting and finite difference approximations. Because the method involves computing curvature tensors and their derivatives at each vertex, it is time-consuming. Yoshizawa [3] detected the crest lines based on a modification of Ohtake's method. The method reduced the computation times since Yoshizawa's method estimated the surface derivatives via local polynomial fitting. Soo-Kyun Kim [4] found ridges and valleys in a discrete surface using a modified MLS approximation. The algorithm was quick because the modified MLS approximation exploited locality. Stylianou and Farin [5] presented a reliable, automatic method for extracting crest lines from triangulated meshes. The algorithm identified every crest point, and then joined them using region growing and skeletonization.

Other types of curves aren't defined as the maximum of curvature, but defined as the zero crossings of some function of curvature. Demarcating curves [19] are the loci of points for which there is a zero crossing of the curvature in the curvature gradient direction. Demarcating curves can be viewed as the curves that typically separate ridges and valleys on 3D surface. Relief edges [20] are defined as the zero crossing of the normal curvature in the direction perpendicular to the edge. Compared to view-dependent curves, view-independent curves are locked to the object surface, and do not slide along it when the viewpoint changes. Moreover, they are pure geometrical and convey prominent and meaningful information about the shape, we believe there is merit in using these curves.

Our approach is closely related to traditional ridges and valleys. They define the so-called feature lines as the extrema of the surface principal curvatures along their corresponding curvature lines.

3. PRELIMINARIES

A good introduction to differential geometry can be found in [21]. We just recall some notions of differential geometry, useful for the introduction of the extraction of feature lines on 3D meshes.

3.1 Polyhedral Surfaces

A polyhedral surface $M \subset R^3$ is a connected topological 2-manifold which is made up of flat triangles that are glued along their common edges such that no vertex appears in the interior of an edge. We will focus on discrete surfaces represented by triangular meshes, i.e., by a couple

$(\mathbf{V}, \mathrm{T}, \mathbf{N})$ where $\mathbf{V}$ is a set of n vertices $\mathbf{V} = \{\mathbf{V}_i \subset \mathrm{R}^3 \mid 0 \le i \le n-1\}$, T is a set of triplets $T_i(i_1, i_2, i_3) \in \{0,1,2,.....,n-1\}$ and (i_1, i_2, i_3) represents the indices of vertices forming a triangle, $\mathbf{N}$ is a set of the normal vectors attached to the corresponding vertices, $\mathbf{N} = \{\mathbf{N}_i \in \mathrm{R}^3 \mid 0 \le i \le n-1\}$.

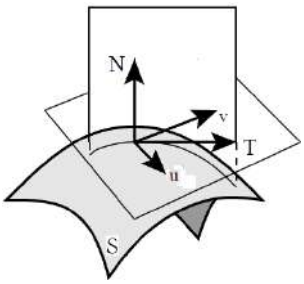


Figure 1 Normal section of Surface S.

3.2 Differential Geometry

Differential geometry of a 2D manifold embedded in 3D is the study of the intrinsic properties of the surface. Here, we will recall basic notions of differential geometry required in this paper. The unit normal N of a surface S at p is the vector perpendicular to S, i.e., the tangent plane of S at p. A normal section curve at p is constructed by intersecting S with a plane normal to it, i.e., a plane that contains N and a tangent direction T. The curvature of this curve is the normal curvature of S in the direction T (See Fig.1).

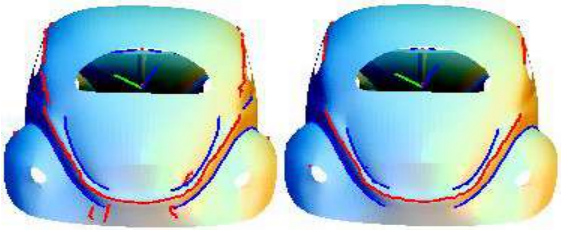


Figure 2: Comparison of the detection algorithm by saliency values with the algorithm only by principal curvatures. Left: Detect the feature lines only by principal curvatures; Right: Detect the feature lines by saliency values, a measure of regional importance.

For a smooth surface, the normal curvature in direction V is $k(\mathrm{V}) = \mathrm{V}^T II \mathrm{V}$, where the symmetric matrix II is the second fundamental form. The eigenvalues of II are the principal curvature values $(k_{\max}, k_{\min})$. The eigenvectors of II are the coordinates of the principal curvature directions $(\mathrm{t}_{\max}, \mathrm{t}_{\min})$. Let $e_{\max}$ and $e_{\min}$ be the derivatives of the principal curvatures $k_{\max}, k_{\min}$ along their corresponding curvatures directions $\mathrm{t}_{\max}, \mathrm{t}_{\min}$. Mathematically feature lines are described via extrema of the surface principal curvatures along their corresponding lines of curvature:

$$e_{\max} = 0, \quad \nabla e_{\max} \cdot \mathrm{t}_{\max} < 0, \quad k_{\max} > |k_{\min}| \quad \text{(Ridges)} \tag{1}$$

$$e_{\min} = 0, \quad \nabla e_{\min} \cdot \mathrm{t}_{\min} < 0, \quad k_{\min} < -|k_{\max}| \quad \text{(Valleys)} \tag{2}$$

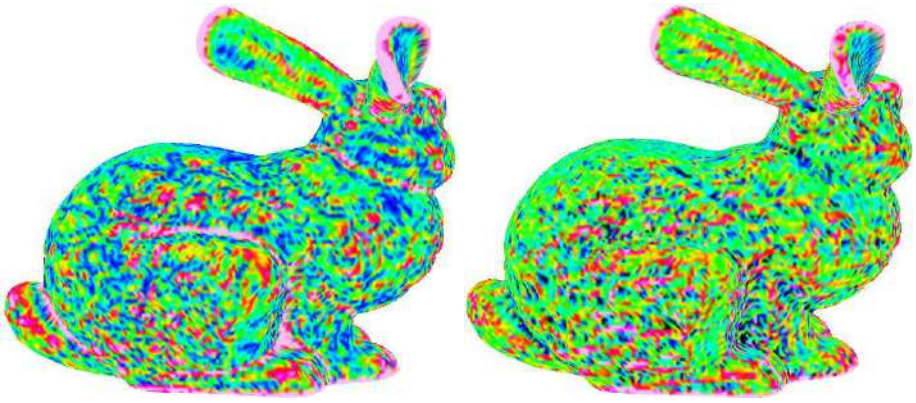


Figure 3: The saliency values can capture the interesting features at all perceptually meaningful scales and reveals the difference between the vertex and its surrounding context. Left: Visualize the saliency values of each mesh points with color. Right: Visualize the principal curvature (max) of each mesh points with color.

4. AUTOMATIC METHOD FOR FEATURE DETECTION

4.1 Detect the Feature Points Via Local Polynomial Fitting

In order to achieve an accurate estimation of the principal curvatures and their derivatives an implicit surface $F(\mathbf{x}) = 0$ need to be constructed to approximate locally the neighborhood of each mesh vertex [3, 4]. We use upper indices for vector components, sub-indices for partial derivatives. So the components of the surface unit normal vector are given by $\mathbf{n}^i = -F_i / |\nabla F|$, where $|\nabla F|$ is the absolute value of the gradient. Let $\kappa, \mathbf{t}$ and s stand for a principal curvature, the associated principal vector, and the arc-length parameter along the associated normal section respectively. Thus the principal curvature κ is given by

$$\kappa = \frac{F_{ij} t^i \mathbf{t}^j}{|\nabla F|} \tag{3}$$

The curvature derivative e is defined by differentiating (3),

$$e = \frac{d\kappa}{ds} = \frac{d}{ds}\left(\frac{F_{ij}\mathbf{t}^i\mathbf{t}^j}{|\nabla F|}\right) = \frac{F_{ijl}\mathbf{t}^i\mathbf{t}^j\mathbf{t}^l + 3\kappa F_{ij}\mathbf{t}^i\mathbf{n}^j}{|\nabla F|} \tag{4}$$

Having found the maximal and minimal curvatures $(k_{\max}, k_{\min})$ and their derivatives $(e_{\max}, e_{\min})$ at each mesh vertex, we can extract ridges and valleys by equation (1) and (2). Computing of the feature lines involves estimation of high-order surface derivatives, so these surface features are very sensitive to noise and irregularities of the triangulation (see Fig.2).

4.2 Modify the Detection Algorithm by Saliency Values

Mesh saliency, a measure of regional importance, can identify regions that are different from their surrounding context and reduce ambiguity in noisy circumstances. In this paper, the computation of the salience value is built on the methods of the salience of visual parts proposed by Ran Gal [8] and mesh saliency proposed by Lee [7]. Differing from the salient parts, we compute a saliency value of each mesh point to identify mesh points that are different from their surrounding

context. We have modified their algorithms slightly to define a saliency value S as a linear combination of two terms :

$$S = W_1 Curv(\mathrm{p}) + W_2 Var(\mathrm{p}) \qquad (5)$$

Where $Curv(\mathrm{p})$ is the maximal absolute curvature of a point p and $Var(\mathrm{p})$ is the absolute curvature difference. The first term of equation (5) expresses the saliency of the mesh point. The second term expresses the degree of the difference between the point and its surrounding context. We use 0.4 for W_1 and 0.6 for W_2. Let $k(\mathbf{p})$ denote the maximal absolute value of the principal curvatures and $G(k(\mathrm{p}))$ denote the Gaussian-weighted average of $k(\mathbf{p})$,

$$G(k(\mathrm{p})) = \frac{\sum_{x \in neighbor(p)} k(\mathrm{x}) \exp[-|\mathrm{x}-\mathrm{p}|^2/(2\sigma^2)]}{\sum_{x \in neighbor(p)} \exp[-|\mathrm{x}-\mathrm{p}|^2/(2\sigma^2)]} \qquad (6)$$

σ is a scale factor that is estimated by $\sigma = \lambda \bar{e}$, where $\bar{e}$ is the average length of edges of the mesh. We compute the saliency value $\varphi_i(\mathrm{p})$ of a vertex p as the absolute difference between the Gaussian-weighted averages $G(k(\mathrm{p}))$ computed at the two neighboring boundaries:

$$\varphi_K(p) = |G(k(p), K+1) - G(k(p), K)| \qquad (7)$$

$Var(p)$ is computed by an average value at multiple scales:

$$Var(p) = \sum_{K=1}^{n} \varphi_K(\mathrm{p}) \qquad (8)$$

Where n is set 3 or 4. We define a salient geometric feature point as a measure of regional importance which is salient and interesting compared to its neighborhood. The top graded points define the salient geometric feature of a given shape. So it is better than the method extracting the feature lines only by the curvature (see Fig.2 and Fig.3).

4.3 An Automatic Feature Points Detection Method

Suppose that the surface points are composed of feature points and flat points. One obvious way to extract the feature points on a mesh is to select a threshold T that separates these mesh points. Because of its intuitive properties and simplicity of implementation, threshold method enjoys a central position in applications of the extraction of the surface feature points. Unfortunately it is difficult for a user to set the threshold if no any apriori knowledge (see Fig.4 and Fig.6)

Our automatic algorithm is based on the observation that polygonal surface models with features usually contain many flat regions and a little sharp edges. Sorting the mesh saliency value of each point by the ascending order, we can find: The saliency values begin to increase slowly and the plot almost corresponds to a planar line, after arriving to a value, the plot rises steeply. Obviously, flat regions correspond to the planar line part of the plot and sharp edges correspond to the steep line part of the plot. So this value is the optimal threshold to extract the feature points (see Fig.5).

Finally, we summarize the automatic feature lines extraction algorithm as follows:

1. Estimate necessary surface curvature and their derivatives via local polynomial fitting.

2. Compute the saliency values as a measure of regional importance for graphics meshes.
3. Seek the optimal threshold by the analysis mentioned above.
4. Extract the feature points by the threshold.

For step 3, we give the pseudocode as follow:

Procedure SeekThreshold(saliency)

1. Quicksort (saliency) /* Sort the mesh saliency value of each point.*/
2. for i = vertex_num / 2 to vertex_num step k
   /* vertex_num represents the number of mesh vertices. Firstly, we search the value at a coarse scale, usually set k = vertex_num /200. */

2.1. m_i = saliency[i] – saliency[i-1]; m_{i-1} = saliency[i-1] – saliency[i-2]

2.2 if $m_i > 1.3 * m_{i-1}$ /*From Fig.5 we can find the plot rises steeply, we used 1.3 for the coefficient.*/

Then shrink the search range in size and repeat step 2 at a finer scale till finding the threshold.

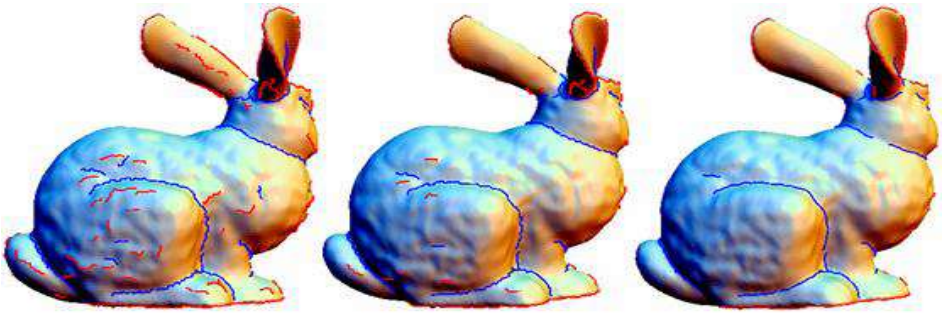


Figure 4 The comparison of the saliency algorithm with different thresholds. Left: Top 30% for ridge points, bottom 30% for valley points; Middle: Top 20% for ridge points, bottom 25% for valley points; Right: Top 8%for ridge points, bottom 15% for valley points.

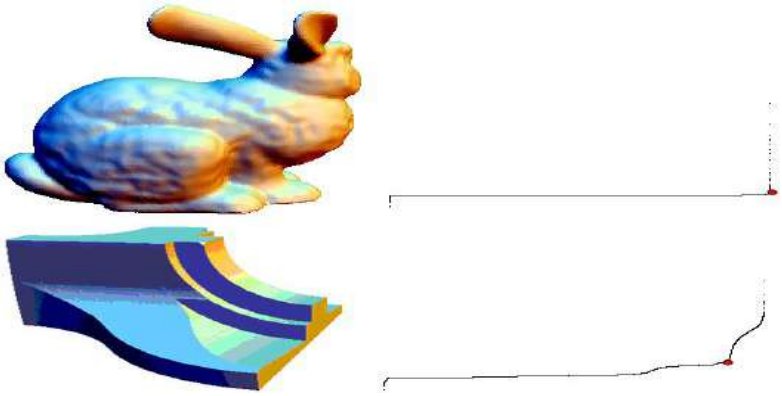


Figure 5 Sort the mesh saliency value of each point by the ascending order, we can get a plot: Firstly, the plot almost corresponds to a planar line, after arriving to a value, the plot rises steeply. Left: 3D model; Right: The plot corresponding to the mesh saliency values by the ascending order.

4.4 Generation of Feature Lines

Once the feature points have been detected, we need to connect them together. We follow the procedure proposed in [4] with an addition which can reduce the fragmentation of the feature lines:

1) Get the optimal threshold in section 4.3. Flag the vertex which saliency value is greater than the threshold T as feature points set M_1. Flag the vertex which saliency value is less than T and greater than $0.8*T$ as weak feature points set M_2. Define k-neighbor of a point p as $N(\mathrm{p},k)$.

2) For a feature point p, examine the point q in $N(\mathrm{p},1)$. If only one point $\mathrm{q} \in \mathrm{M}_1$, then connect it to p.

3) If two or more points $\mathrm{q}_i \in \mathrm{M}_1, i = 1,...,n \text{ and } n \geq 2$, then we connected p to one of them by following the vertex q_i corresponding to the smaller dihedral angle with the orientation of the principal curvature.

4) No any point in M_1, but at least one point $\mathrm{q} \in \mathrm{M}_2$. If having $\mathrm{k} \in N(\mathrm{q},1) \textit{ and } \mathrm{k} \in M_1 \text{ and } \mathrm{k} \notin N(\mathrm{p},1)$, then connect p to q similarly following the rule in step 2 and step 3.

Repeat step 2 to step 4.

5. RESULTS

For evaluating the effectiveness of our automatic mesh saliency method, this section shows results of our algorithm and compares it to the user-specified threshold algorithm. All of our tests were run on a PC with Intel® Core™ 2 1.73.GHz processor and 1.0 GB of main memory.

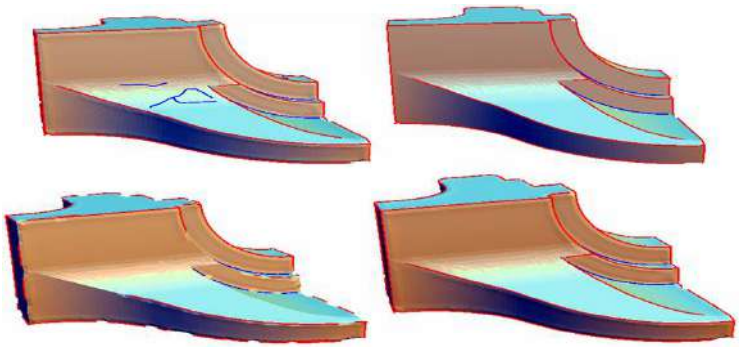


Figure 6 The comparison of the saliency algorithms with different thresholds and our automatic detection algorithm. Upper Left: Top 25% for ridge points, bottom 30% for valley points ; Upper Right: Top 15% for ridge points, bottom 20% for valley points ; Bottom Left: Top 5% for ridge points, bottom 5% for valley points; Bottom Right: The automatic detection algorithm.

Fig.2 and 3 show some results. Fig.2 shows the comparison of the detection algorithm by saliency values and the algorithm only by principal curvatures. Owing to its locality, the method only by principal curvature is sensitive to noise and irregularities of the triangulation and usually produces spurious feature lines. The result shows on the left of Fig.2. Mesh saliency that measure the region importance at multiple scales in the neighborhood can reveal the difference between the vertex and its surrounding context. So it can extract the most salient features points robustly. The result on the right shows that the lines are clearly detected by saliency values. In Fig. 3, we visualize the magnitude of principal curvature value and the saliency value of each point with

color on a bunny model. Warm color corresponds to the sharp features and cool color corresponds to the flat regions. We can find that saliency values differentiate the neck and the leg from their circumferences

.

Fig.4 and Fig.6 show the comparison between the different thresholds. The surface points are composed of feature points and flat points. One obvious way to extract the feature points on the surface is to select a threshold T , for example, TOP 20% means that the feature points are the top 20% points with high saliency values. But improper threshold produces many spurious feature lines. Polygonal surface models can be roughly divided into two classes: CAD-like models showed in Fig.6, which usually have large flat regions; Non-CAD-like model showed in Fig.4, which have many fine details. We can't find a unified threshold for the detection method. So how to decide the threshold is a problem for user-specified threshold methods.

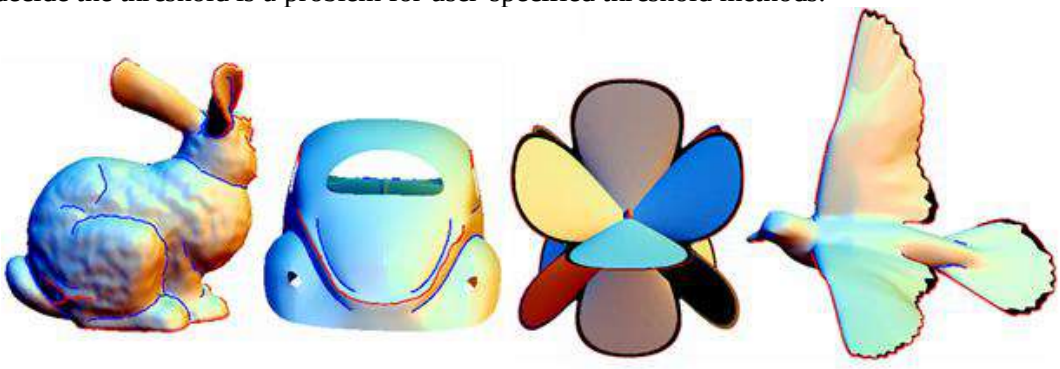


Figure 7 Our automatic algorithm for feature line detection on various models.

Fig.5 gives an analysis for the optimal threshold. On the left are the 3D models, on the right are the corresponding plots of the saliency values in ascending order. The plot begins to rise slowly and almost corresponds to a planar line, after arriving to a value (Flagged in red circle dot), the plot rises steeply. The value at the red circle dot is the threshold we need. Fig.6 shows results from the fandisk CAD model, in which our automatic method works well. Moreover, our method doesn't need a user to select the threshold. It is not easy for a user to modify the threshold if no any apriori knowledge. Fig. 7 illustrates further results on bunny, car, focal and dove model. Ohtake's method [2, 22] is a reliable detection of ridge-valley structures on surfaces approximated by dense triangle meshes and has become a representative method of feature lines detection algorithm.. Fig.8 shows that our automatic method almost has the same precise as Ohtake's method.

6. CONCLUSION

This paper has presented an automatic algorithm for the detection of feature lines on triangular meshes based on the concept of salient geometric features. The utility of saliency values for robustly detecting the feature lines on surface has been demonstrated. The results show saliency values effectively capture important shape features.

Our automatic algorithm is a fully automatic method. It can advantageously select a "good" threshold without any user intervention. The results show that our automatic algorithm can find an optimal threshold to detect the feature lines on 3D meshes. In the future we intend to develop data clustering method into the field of the feature lines detection.

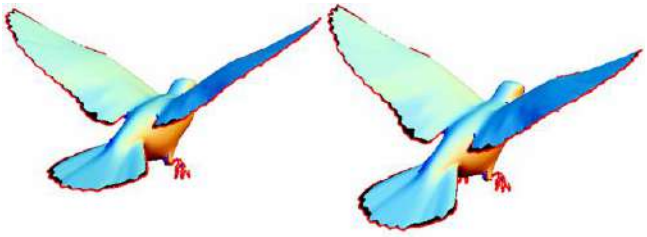


Figure 8 Our automatic algorithm VS. Ohtake's method, left: Our automatic algorithm; right: Ohtake's method.

ACKNOWLEDGEMENT

This study was supported by the Innovation projects of Department of Education of Guangdong Province, China (NO.2017KTSCX183) and the introduction project of Jiangmen innovative research team(2018).

REFERENCES

[1] Forrester Cole, Kevin Sanik, Doug Decarlo, Adam Finkelstein, Thomas Funkhouser, Szymon Rusinkiewicz & Manish Singh, (2009) "How Well Do Line Drawings Depict Shape?", ACM Transaction on Graphics, Vol. 28, No.3, pp43-51.

[2] Ohtake Y., Belyaev A., & Seidel H.P, (2004) "Ridge-valley Lines on Meshes via Implicit Surface Fitting", ACM Transactions on Graphics, Vol. 23, No. 3, pp609-612.

[3] Shin Yoshizawa, Alexander Belyaev & Hans-Perter Seidel, (2005) "Fast and Robust Detection of Crest Lines on Meshes", Symposium on Solid and Physical Modeling'05, pp227-232.

[4] Soo-Kyun Kim & Chang-Hun Kim, (2006) "Finding Ridges and Valleys in A Discrete Surface Using A Modified MLS Approximation", Computer-Aided Design, Vol. 38, No.2, pp173-180.

[5] Georgios Stylianou & Gerald Farin, (2004) "Crest Lines for Surface Segmentation and Flattening", IEEE Transaction on Visualization and Computer Graphics, Vol. 10, No. 5, pp536-543.

[6] Tilke Judd, Fredo Durand & Edward H. Adelson, (2007) " Apparent ridges for line drawing" , ACM Transactions on Graphics, Vol. 26, No. 3, pp19-26.

[7] Chang Ha Lee, Amitabh Varshney & David W.Jacobs, (2005) "Mesh Saliency". Proceedings of ACM Siggraph'05, pp659-666.

[8] Ran Gal & Daniel Cohen-Or, (2006) "Salient Geometric Features for Partial Shape Matching and Similarity", ACM Transactions on Graphics, Vol. 25, No. 1, pp130-150.

[9] Taubin G, (1995) "Estimating the Tensor of Curvature of a Surface from a Polyhedral Approximation", In Proceedings of Fifth International Conference on Computer Vision'95, pp902-907.

[10] Sachin Nigam & Vandana Agrawal, (2013) " A Review: Curvature approximation on triangular meshes", Int. J. of Engineering science and Innovative Technology, Vol. 2, No. 3, pp330-339.

[11] Xunnian Yang & Jiamin Zheng, (2013) "Curvature tensor computation by piecewise surface interpolation", Computer Aided Design, Vol. 45, No. 12, pp1639-1650.

[12] Gady Agam & Xiaojing Tang, (2005) “A Sampling Framework for Accurate Curvature Estimation in Discrete Surfaces”, IEEE Transaction on Visu alization and Computer Graphics, Vol. 11, No. 5, pp573-582.

[13] Meyer M., Desbrun M., Schroder P. & Barr A. H, (2003) “Discrete Differential-geometry Operators for Triangulated 2-manifolds”, In Visualization and Mathematics III’ 03, pp35-57.

[14] Stupariu & Mihai-Sorin, (2016) “An application of triangle mesh models in detecting patterns of vegetation”, WSCG’ 2016, pp87-90.

[15] Chen L., Xie X., Fan X., Ma W., Zhang H., & Zhou H, (2003) “A visual attention model for adapting images on small displays”, ACM Multimedia Systems Journal, Vol. 9, No. 4, pp353-364.

[16] Lee, Y., Markosian, L., Lee, S., & Hughes, J. F, (2007) ”Line drawings via abstracted shading”, ACM Transactions on Graphics, Vol. 26, No. 3, pp1-9.

[17] Jack Szu-Shen & His-Yung FEng, (2017) “Idealization of scanning-derived triangle mesh models of prismatic engineering parts”, International Journal on Interactive Design and Manufacturing, Vol. 11, No. 2, pp205-221.

[18] Decarlo D., Finkelstein A., Rusinkiewicz S. & Santella A,(2003) “Suggestive Contours for Conveying Shape”, ACM Transactions on Graphics, Vol.22, No. 3, pp848-855.

[19] M. Kolomenkin, I. Shimshoni, & A. Tal,(2008) “Demarcating curves for shape illustration”, ACM Transactions on Graphics, Vol.27, No.5, pp157-166.

[20] Michael Kolomenkin,(2009) “Ilan Shimshoni and Ayellet Tal. On Edge Detection on Surface”, IEEE CVPR’ 09, pp2767-2774.

[21] M. P. Do Carmo (2004) Differential geometry of curves and surfaces, Book, China Machine Press.

[22] A. Belyaev, P.-A. Fayolle, & A. Pasko, (2013) “Signed Lp-distance fields”, CAD, Vol.45, No. 2, pp523-528.

[23] Y Zhang, G Geng, X Wei, S Zhang & S Li, (2016) “A statistical approach for extraction of feature lines from point clouds” ,Computers & Graphics, Vol. 56, No. 3, pp31-45.

INTENTIONAL BLANK

CONTEXT-AWARE TRUST-BASED ACCESS CONTROL FOR UBIQUITOUS SYSTEMS

Malika Yaici, Faiza Ainennas and Nassima Zidi

Computer Department, University of Bejaia, Bejaia, Algeria

ABSTRACT

The ubiquitous computing and context-aware applications experience at the present time a very important development. This has led organizations to open more of their information systems, making them available anywhere, at any time and integrating the dimension of mobile users. This cannot be done without taking into account thoughtfully the access security: a pervasive information system must henceforth be able to take into account the contextual features to ensure a robust access control. In this paper, access control and a few existing mechanisms have been exposed. It is intended to show the importance of taking into account context during a request for access. In this regard, our proposal incorporates the concept of trust to establish a trust relationship according to three contextual constraints (location, social situation and time) in order to decide to grant or deny the access request of a user to a service.

KEYWORDS

Pervasive systems, Access Control, RBAC, Context-awareness, Trust management

1. INTRODUCTION

Ubiquitous computing, which is declined under different terms, corresponds to this technical (r)evolution conceived about fifteen years ago by Weiser [1]. In contrast to traditional computing, the novelty lies in the ability of mobility and integration of systems in the physical environment, and this spontaneously and at multiple scales. The limitation of resources, the distribution of applications, the mobility of terminals, the discovery of services and the automatic deployment of software on these terminals make complex and difficult the implementation of ubiquitous applications. Large-scale implementation of these applications is a first major challenge that many research communities are trying to overcome by proposing different approaches.

In pervasive computing, the context plays a crucial role. IT applications extend their interactions with the environment: new inputs and outputs are used, such as sensors and other mobile devices that interact with the real and physical environment. Ubiquitous applications must therefore be aware of the environment in which they are running, what type of terminal they are running, which user profile to consider for the configuration, what type of network they have for communication where the mobile terminal is, and what computing devices are in the environment. A context-aware application is an application that meets the requirements imposed by this context information. Such an application must be able to capture and manage context information to provide appropriate services.

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 13-32, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90902

However, access to certain equipment or users' personal data must be highly secure. Setting up a security system requires considering the following issues:

• Authentication: The identification of a given user must be possible and must take into account his context (time, familiar location, surrounding people etc.)
• Access Control: In pervasive environments information is accessible anywhere and anytime. As a result, the administration and integration of different security policies becomes more complex as they are heterogeneous from a structural (role) and semantic (coding, language) point of view.

• Confidentiality and protection of privacy: The misuse of the new technology can compromise the privacy of users. A user has a very limited perception of potential risks from different on-board equipment.

Access control consists of checking whether a human or logic actor has the rights to access a resource. With access control, we are interested in guaranteeing two fundamental properties: Information confidentiality and integrity. Access control must evolve to integrate a dynamic and reactive authorization, based on information related to the environment and more simply on user trust. Contextual information evolves according to an application-independent dynamic. It is also necessary to detect context changes to re-evaluate the authorization.

Context awareness and access control are two similar concepts. They both go through a decision based on the information collected in input, to output an application whose features can be activated and allowed or inactivated and prohibited. In addition, the security of contextual information, especially for the protection of privacy, is a growing problem in computing.
Fine grain access control for a given service must incorporate all relevant contextual information that has significance on access control. In this paper, context-aware access control models are studied to lead to a proposition of a trust-based role-based access control and taking into account context as location, time and social situation.

After this introduction, section 2 is a summary of related works. The proposed solution is given in section 3 and its validation is presented in section 4. A conclusion and some perspectives finish this paper.

2. RELATED WORKS

Discretionary Access Control (DAC) is a conceptual model whose principle is to limit access to objects in relation to the user's identity (humans, machines, etc.) and / or groups to which they belong. Controls on a resource are said to be discretionary in the sense that a user with defined access permission is able to transmit it (indirectly or directly) to any other user. Discretionary access control is generally defined as opposed to Mandatory Access Control (MAC), which imposes mandatory rules to ensure that the intended security objectives are achieved. In this type of access control, subjects can not intervene in the allocation of access rights [2].

From the company access control policy organizational structure, the Role Based Access Control (RBAC) model is used to facilitate the access control administration and to provide an access control model which matches the existent policy[3]. A role represents in an abstract way a particular function in an organization. The role is an intermediate entity between the access

permissions, also called privilege or access right, and the users. It groups together a set of privileges that will then be assigned to users based on their organizational positions. A role can have multiple permissions and permission can be associated with multiple roles. A user can have multiple roles and a role can be assigned to multiple users.

Traditional access control models (RBAC, MAC, DAC) are rigid. Access control decisions cannot be more than allowing or denying access. With these models access authorizations are considered to be known in advance, but in real-world contexts, errors are made and unforeseen situations or emergencies can occur.

Several model proposals have emerged which have proposed the integration of additional features like context. Among the different contexts taken into account in the access control, existing in the literature, we find the location, the time, the state of execution of the applications, the state of the resources, the bandwidth of networks, the activities of each entity, users' intentions, user emotions and environmental conditions.

Taking into account the context imposes new requirements for the definition of access control solutions. These concern, in particular, context awareness. For this, taking into account the notion of context sensitivity is a priority for the development of access control policies.

From the literature study, we have been able to classify these models into four classes:
- Context-aware access control.
- Role-based context-aware access control.
- Trust-based context-aware access control.
- Hybrid access control based on role, trust and context awareness.

2.1. Context-aware Access Control

The role-based access control model, RBAC and its extensions are not suitable for open and peer-to-peer environments that do not assume predefined roles or permissions.

The authors in [4] propose a context-aware and context quality-aware access model for an access request. They explain that the use of the context alone is not enough. Context-awareness is the contextual information quality that is taken into account to decide on the access granting. They propose to base on the authorization or the prohibition of access to resources thanks to indicators of quality of context, in a ubiquitous environment. The quality of context can be defined by the following parameters: Precision, completeness, freshness and accuracy.

CoDRA (Context-based Dynamically Reconfigurable Access) [5] is an Android’s access control system. It offers dynamically configurable restrictions based on context and fine-granular policy and enforces various policy configurations at different levels of system operation. Context based on resource features is used to reach the fine-granular policy and policy diversifications. Resource contexts are identified and their appropriate OS handlers are modified to accommodate and apply the restrictions through policies. In access control systems based on environmental context, the operating environment of an entity decides on access policies. This environment can be a location, a time, available energy and network bandwidth for the operation of the device.

2.2. Role-based Context-aware Access Control

The role-based model uses roles to manage privileges. It is naturally applied to organizations where users are assigned roles with well-defined access control privileges. However, with the new requirements for ubiquitous applications, the basic RBAC have quickly shown its limits and several extensions have been developed to improve its security. As users are mobile and the number is large enough, the context becomes a factor of first order in access control.

Given the recognized success of RBAC approaches, several solutions have been proposed to enrich RBAC in order to support contextual constraints. In the work cited in [6], the authors use the RBAC model principle, so for each user equipped with an RFID card for identification and authentication is associated a role with predefined access rights but the context adds restrictions on these rights.

Zhang and Parshar [7] propose a DRBAC model (Dynamic RBAC), RBAC roles and model permissions dynamically adapted to the context. Each role is associated with a subset of a set of permissions and each subject is associated with a subset of a set of roles. DRBAC dynamically adjusts the authorization assignment as well as the role assignment based on contextual information of a subject. Contextual information could be any piece of information not just time or location.

Hansen et al. [8] propose an RBAC extension with spatial constraint SRBAC which takes into account the location of users when they require resources which could limit these permissions. In the SRBAC solution, roles / permissions are granted to a user in specific time intervals and / or if the user is in a particular location. Inclusion of the location constraint provides a mechanism to apply access based on location. Thus, a role is activated or deactivated if and only if a certain location constraint is satisfied. The location space is divided into multiple areas. An access authorization, is granted if the condition on the role is satisfied and the subject is in a specific area.

Other RBAC model extensions have been studied in the literature; in GEO-RBAC [9], RBAC is extended by including the positions of the user who would see his permissions vary, but also his role can also vary according to the connection area and resources location. The C-RBAC model (Context-RBAC) proposed by Park et al. [10], the Spatial-Temporal Role-Based Access Control Model ST-RBAC proposed by Ray et al. [11], etc.

2.3. Trust-Based Context-Aware Access Control

The authors, in [12], proposed a framework for retrieving and classifying contextual data from a mobile device and then deciding which access control to provide. They studied two use cases: Smartphone lock to prevent misuse, and defense against the sensory malware, where the user's private information is revealed to unauthorized ports. The authors used two contextual models: location to specify familiar places, using GPS to capture the user's significant locations in the outer areas of a building, for example, and using the wifi for capture significant areas of the user in interior areas; the social context to specify familiar people with the detection of smartphones surrounding the user. This defines the user’s trusted environment.

Cloud File is a personal cloud data access control is proposed in [13], it is based on evaluation of trust in mobile social networks. Social trust is used to protect and control access to personal mobile cloud data and storage using Key Policy–Attribute Based Encryption (KP-ABE). Trust can be evaluated based on the clue showed in mobile social networking. Types of social networking and communications are classified as: a) mobile voice calls; b) voice/video calls via mobile Internet (e.g., VoIP); c) short messages; d) instant social messages; e) pervasive interactions based on local connectivity. Social closeness and trust between two persons is evaluated using the number of voice calls (called and received), the number of interactions and the number of messages (sent and received).

In [14], a scheme using either a General Trust (GT) level issued by a core network or a Local Trust (LT) level evaluated by a device, or both, to control Device to Device (D2D) communication data access by applying Attribute-Based Encryption (ABE) is proposed. Only the devices holding the eligible trust level of GT and/or LT can access the data. Each user's equipment (UE) would select at least one kind trust level of GT or LT to secure communications. If the core network is available and a user device would control its data using GT only, then GT keys are used to encrypt and decrypt data. Otherwise, i.e. the core network is not available, LT-keys are generated for the allowed devices. When the core network is available and a user device would like to use both GT and LT to control its data access, the attribute keys are generated under the control of both GT and LT. Moreover, UE evaluates local trust levels with pseudonyms in order to enhance communication privacy.

TIRIAC (Trust-drIven RIsk-aware Access Control) framework [15] is proposed to enrich Grid access control services by adding an evaluation of trust and a risk management unit. A request may be permitted or denied according to the access policies and without consideration of risk.

But for the other risky accesses, risk policies and utility theory are used to process them. A risk manager evaluates the expected loss and benefit of the access request according to the characteristics of the involved resource as well as the subject's trust degree and confidence. Subsequently, the request may be denied, or extra risk mitigation obligations may be demanded.

2.4. Trust And Role Based Context-Aware Access Control

In [16], to redefine the role-based access control model and entities (users, roles, session, permission) using context, the authors analyzed context factors to classify them and to formalize them according to four system Security, User Confidence, Location and Time.

• The system security is defined in four levels PLT = {TL, HL, ML, JL} such that TL (top level) = 100%, HL (high level)> 80%, ML (middle level)> 50%, JL (junior level) <50%
• Confidence in the user, calculated from access history and usage for each resource in the system.
• Location: for each resource, a set of IP addresses are associated SC = {IP1,. . ., IPi} which represent the familiar locations
• Time: for each user, a set of time intervals are associated: TC = {T1, T2, TJ}.

The authors of [17] propose a Context-Aware Trust and Role-Based Access Control model CATRAC, for access control in composite web services. The assigned roles must be validated by

a third party (role authority) and the trust levels are vectors from 0 to 10 and the new clients have a level of 5. The trust is based on the user's access history to special resources.

In [18], a secure, automated PrBAC architecture and prototype system referred to as the Context-Aware System to Secure Enterprise Content (CASSEC) is introduced. It dealt with two proximity scenarios usually encountered in enterprise: Separation of Duty (SoD) and Absence of Other Users (AOU). A geo-spatial RBAC is used in a monitored space to localize persons using a wireless infrastructure. However, a malicious actor can grant privileges by manipulating the sensors in the monitored space, thus perverting control access decisions. To avoid this scenario, sentience-like constructs have been added to the geo-spatial RBAC, to emulate the confidence in the proximity evaluation as *degrees of reliability* in extracted context, thus allowing CASSEC to make more inferable decisions. Continuous authentication based on co-proximity is performed using PMs and users Bluetooth Low Energy (BLE) capabilities. To guarantee the safety of the client localization with a certain degree of confidence, despite multiple PMs detection, the system uses BLE beacons transmitted during this authentication. The role is constructed such that an access control policy is specified to grant with high confidence that the current devise user is the true owner of the device.

It is clear that context and context awareness must be included in any access control to a service. Access control can be based on context, role and trust and/or a combination of these. The solution we propose is in the last class.

3. PROPOSITION

With the needs of ubiquity and mobility, users can access anywhere and at any time to data from diverse and heterogeneous sources. Thus, access control must take into account the context of the user to manage access and preserve the confidentiality of data.

The concept of role is used as an intermediary between users and permissions. These are granted to roles activated by users during a session, following the RBAC model. However, new requirements for applications in ubiquitous environments are driving us to review and improve the access control system. Indeed, relying solely on the role to make a decision for an access request is not always convincing. In this respect, we add to this concept the notion of trust. Thus, each service will have a level of confidence that the user according to his assigned role can reach or have access to it.

But, the level of trust may be influenced by other types of contexts in this case, the temporal context and the spatial context being of prime importance. Indeed, when a user accesses the same service from two geographically distant locations during a short period of time it is understood that it is not the same person. The trust level becomes low and the system in this case must automatically lock access. The social context can also influence the system decision. If the user is in the right place at the right time but surrounded by unfamiliar people, his confidence level decreases, and access may be denied. Given that the concept of context is dynamic, taking into account the three contexts already mentioned would further strengthen the concept of access control.

We propose a system that establishes a trust relation in the user according to the role and the three contextual constraints and according to this trust the system decides to grant or refuse the request for access. Thus, our system will be classified in the fourth class.

3.1. Case Study

We present in the following our model applied to an access control at the level of a request for a bank service.

The banking system is an important element of the economic life of a country. Banks play a major role in the daily lives of households and businesses: ensuring the fluidity of transactions by providing economic agents with fast, convenient and secure means of payment. For this purpose, the aim of access control systems is to reduce the risk of interference with managed data.

Our work is to propose a system for controlling access to context-aware services. The example of the banking system to validate our proposal is adequate given its required high level of security. We propose a role-based access control, where access rights are assigned to users based on the role they play in the system, and based on trust, where the level of trust varies upon the user's history and context.

3.2. Operations

Users of a system are associated with a defined role in advance. When they want to perform an operation, they will activate a role during a session and they are supposed to be able to perform all the operations allowed by the role during this session, thanks to the privileges with which they are associated. In our example we define three roles: the client, the counter agent and the bank administrator. For each role we associate the following services (assuming that users are already authenticated):

A client can:
• Consult his account balance.
• Transfer money.
• Remove / deposit money on his account.
An agent can:
• Open / Close a client account.
• Make a transfer on the client behalf.
• Retrieve / deposit the client's money.
An administrator can:
• Open / Close a client account.
• Make a transfer on the client behalf.
• Retrieve/ deposit money from a client's account.
• Check transactions made during a day.
• Confirm opening of a new account of a client.

The services of the bank are classified into groups each having a minimum confidence threshold to authorize access, this confidence threshold is determined according to its sensitivity based on one or more contextual constraint(s). The user's access request is checked according to their level of confidence, the confidence value, is determined by:

- A client access history and his behaviour, this level of trust, is used to differentiate between a proven client and an untested client.
- As the client is mobile, hiss context is dynamic. Indeed the context influences the confidence and thus makes it variable, the level of trust as well, can increase or decrease depending on the contextual constraints.

  The level of service access requester confidence is determined in real time, according to the following set of contexts: location context, social context and time context.
- Location context

The location context is an important context in a ubiquitous environment. We note TL (Loc) is the degree of confidence in an access location. By hypothesis, home and workplace are familiar locations for a client or administrator. To determine the degree of access requester trust, table 1 is proposed:

Table 1. Description of Location Context Trust Level

TL(Loc)	Description
Level 0	If the user requests access from two locations very distant geographically and this in a very short period of time.
Level 1	If the user requesting access to the service is not in a location defined as familiar.
Level 2	in the case where a user requesting the service is in a location defined as familiar

- Social Context

We define the social context as being all connected people surrounding the user when the user accesses the service. Once a user logs in, the context manager detects people around him through their login device. All the people familiar with the user are defined when opening a bank account. TL (Social) is the level of trust in the user according to his social context. Table 2 determines the level of trust in the user according to his social context:

Table 2. Description of social context trust level

TL(Social)	Description
Level 0	In the case where the persons surrounding the access requester are foreign people (are not defined as familiar).
Level 1	In the case of the existence of at least one familiar person between those surrounding the access requester.
Level 2	If the user is surrounded only by familiar people.

- Context of time

The context of time is defined by the work hours of the requester of access to the service in the bank, in our case the context of time is taken into account if the role of the user, is an agent at the counter or an administrator. We note TL(Time) the trust level in user according to the context of time. These trust level of trust are defined in table 3:

Table 3. Description of trust level for context of time

TL(Time)	Description
Level 0	If the counter agent requests access to an out-of-hours working service.
Level 1	If the administrator requests access to the service outside work time.
Level 2	In the case the user requests access during working hours.

3.3. Trust Manager

After all types of context are identified as well as their trust levels, we proceed to determine the total value which is the value of the level of trust of an access requester based on the trust level of the different contexts. The value of the Total Trust Level (TTL) will be calculated as follows:

$$TTL = min(TL(Loc), TL(Social), TL(Time)) \quad (1)$$

where *min* is the function that returns the minimum value between these parameters.

3.4. Proposed System Architecture

Figure 1 presents the proposed architecture of the role and trust -based access control system. This implementation includes the following components:

• Context manager: Captures the context of the user to know its location, its social context and its time context, and stores it in a database "user's context". The context manager is not part of our work.
• User Context: Contains the user's contextual information. This context is dynamic, so when the context manager captures the same context with 3 different accesses of a user, this context is therefore defined as familiar and is updated by the context manager.
• Service Context: Contains the different contextual constraints for each service. Contexts for each service are defined according to each role as shown in Table 4.
• Role / permission: Contains all the permissions associated with user roles.
• Trust evaluator: Calculates the access requester's trust value based on his behavior after completing his operations and updating the reports.

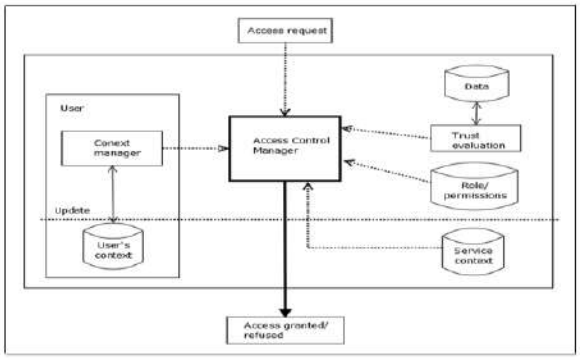


Figure 1. Proposed control access system architecture and operation

• Access control manager: When sending an access request, the access control manager retrieves the user's contexts from the context manager, the role from the database, the user's trust level from the trusted evaluator and finally the contextual constraints for each service registered in the service context database. Based on these information's, the access control manager decides whether or not to accept the access request.

Table 4. Contexts assigned to roles and services

Services \Role	**client**	**Agent at counter**	**Administrator**
	Context		
Account balance consulting	no context consideration	No access	No access
Make a transfer	Familiar location + surrounded by familiar persons	To be in the bank during working hours + client presence	Familiar location + surrounded by familiar persons
money retrieval	Familiar location + surrounded by familiar persons	To be in the bank during working hours + client presence	To be in the bank during working hours
money deposit	Familiar location + surrounded by familiar persons	To be in the bank during working hours	To be in the bank during working hours
Check transactions made during a day	No access	No access	Familiar location + surrounded by familiar persons
Confirm new account opening/closing	No access	No access	Familiar location + surrounded by familiar persons
Open a new account	No access	To be in the bank during working hours + client presence	Familiar location + surrounded by familiar persons

3.5. Case Study Scenarios

In this section we used this terminology and assume some hypothesis:

• U: User of a service whose access to the service is controlled.
• Client: The role is a client.
• Agent: The role of the user is an agent at the counter.
• ADmin: The role is an administrator.
• RR: Role of the user. Can take three values: Client, Agent, Admin.
• SRi: The set of services provided by the bank.
• TLU: System trust level in client. This trust level is calculated at each session and varies mainly according to parameters related to the client behavior. TLU is a real belonging to the interval [0, 0.5].
• TTL: The instant trust level of the system in the client. This trust level is calculated at each session and varies according to parameters related to the context.
• C: The user's trust level, it is the sum of the two TTL and TLU levels.
• STi: Service i threshold, each service has a minimum trust threshold from which the service can be provided to the user if the trust level TL is greater than or equal to STi.

• It is assumed that the user is already authenticated.
• Initially the level of trust of the service in user is equal to 0.3 (half of the interval).
• If the trust level (TLU) is zero then the user U is malicious. In this case, the user must approach the bank for a reset of his profile and verification of past transactions (client history).

In the following scenarios, we will consider that web services have in their databases user identifiers, their role, contextual constraints and trust levels.

3.5.1. Scenario 1: When The User's Role Is A Client

After being authenticated, the user sends an access request request to the banking service. The access control manager obtains user information including its role in the (role / Permission) database and its contextual information through the context manager and its trust level.

The system first checks whether its trust level according to behavior is different from level 0. In case the condition is not satisfied, access is denied. Otherwise, the system checks whether the client contextual information such as its location and the people around him at a given time, are appropriate for those existing in the database (service context). Following this audit, the trust level by location is determined from Table 4.1, and the social context trust level is determined from Table 4.2. Then the access control manager determines the client trust level as follows:

$$TTL = min(TL(Loc), TL(Social)) \quad (2)$$

The total trust value is converted from level to a rate (weight) using the following:

• Level 0 = 0
• Level 1 = 0.33
• Level 2 = 0.5

The access control manager adds the two TTL and TLU values to obtain a trust level C which is compared with the requested service trust level STi. When the trust value C in a client is not lower than the confidence threshold STi predefined to a service SRi, the access is then granted to the client.

In the opposite case a subtraction is performed between the service confidence threshold STi and the new trust value C: DIF = STi - C. Access in this case is granted to the client if the result is less than 0.1, otherwise the request for access to the service is refused.

The following algorithm summarizes the access rules for the client.

Algorithm1 : Algorithm of processing a client service request

```
Service request (ID, SR)
SELECT role
WHERE ID=ID // retrieve the role according to the identity from the database
SELECT TLU
WHERE ID=ID // retrieve the trust level depending on the behavior.
if TLU≥0 then
        // retrieve client location and social context
        TTL=min(TL(Loc), TL(Social)) ;
        C=TTL+TLU ;
        if C≥ST then access granted ;
        else
                DIF←STi-C ;
                if DIF≤0.1 then access granted ;
                else access denied ;
                endif ;
        end if;
end if
end.
```

3.5.2. Scenario 2: When The User's Role Is The Counter Attendant

The agent at the desk supposed to be in the bank only during his working hours sends a request for access to the banking service. The access control manager obtains user information including its role in the (role / Permission) database and its contextual information through the context manager and its confidence level determined by the trust evaluator.

First, the system checks if its trust level, according to the client behaviour, is different from level 0. If it is the case, the access is refused. Otherwise, the system checks whether the contextual information of the user such as its location and the time context of his access request are appropriate to those existing in the database (service context). Following this verification, the trust level of the location is determined from Table 4.1 and the time context trust level is defined in Table 4.3. Then the access control manager determines the user's trust level as follows:

$$TTL = min(TL(Loc), TL(Time)) \quad (3)$$

The total trust value is converted from level to a rate (weight) using the following:

- Level 0 = 0
- Level 1 = 0.33
- Level 2 = 0.5

The access control manager adds the two TTL and TLU values to obtain a trust level C which is compared to the requested service confidence threshold STi. When the trust value C in a user is not lower than the confidence threshold STi predefined to a service SRi, the access is then granted to the client.

In the opposite case, a subtraction is performed between the service confidence threshold STi and the new trust value C: DIF = STi - C. Access in this case is granted to the user if the result is less than 0.1, otherwise the request for access to the service is refused.

If the user is outside his working hours and / or outside the bank, his request for access is automatically refused.

The following algorithm summarizes the access rules for the counter attendant.

Algorithme2: Algorithm for processing the counter attendant service request

```
Requête de service (ID,SR)
SELECT role
WHERE Id=ID // retrieve the role according to the identity from the database
SELECT TLU
WHERE ID=ID // retrieve the trust level depending on the behavior.
if TLU≥0 then
        // retrieve client location and time context
        TTL=min(TL(Loc), TL(Time));
        C=TTL+TLU
        if C≥ST then access granted;
        else
                DIF←STi-C;
                if DIF≤0.1 then access granted;
                else access denied;
                endif
        endif
endif
end.
```

3.5.3. Scenario 3: When The User's Role Is An Administrator

An administrator, after being authenticated, sends an access request to the banking service. The access control manager obtains user information including its role in the (role / Permission) database and its contextual information through the context manager and its trust level.

As before, first, the system checks whether its trust, according to the behavior, is different from level 0, and if it is the case, the access is refused. Otherwise, the system checks whether the user's contextual information such as location, social context, and time context of the access request matches the existing information in the database (service context). According to this verification, the trust level of the location is determined according to Table 4.1, the social context trust level is defined in Table 4.2 and the time context trust level is defined in Table 4.3. Then the access control manager determines the user's trust level as follows:

$$NCT = min(NC\ (loc), NC(Social), NC\ (temps)) \quad (4)$$

The total trust value is then converted from level to a rate (weight) using the following:

- Level 0 = 0
- Level 1 = 0.33
- Level 2 = 0.5

The access control manager adds the two TTL and TLU values to obtain the trust level C which he compares with the requested service confidence threshold STi. When the trust value C in a user is not lower than the confidence threshold STi predefined to a service SRi, the access is then granted to the user.

In the opposite case, a subtraction is performed between the service confidence threshold STi and the new trust value C: DIF = STi - C. Access in this case is granted to the user if the result is less than 0.1, otherwise the request for access to the service is refused.

An administrator is both a client and / or a counter attendant. He plays the role of a client when he confirms an account or checks transactions and acts as a counter attendant in other cases.
The following algorithm summarizes the access rules for the administrator.

Algorithme3: Algorithm for processing the administrator service request

```
Requete de service (ID, SR)
SELECT role
WHERE ID=ID // retrieve the role according to the identity from the database
SELECT TLU
WHERE ID=ID // retrieve the trust level depending on the behavior.
if  TLU≥0 then
        //retrieve client location, social and time context
        TTL=min(TL(Loc), TL(Social), TL(Time) ;
        C=TLU+TTL ;
        if C≥ST then access granted ; //
        else
                DIF←STi-C;
                if DIF≤0.1 then access granted;
                else access denied
                endif
        endif
endif
end
```

3.6. Generalization

In this paper we proposed a new access control approach for ubiquitous systems. In order to highlight the dynamic changes in the environment, the proposal, is based on the RBAC model and employs the notion of trust evaluated by measuring environmental context and social context. When the access requester trust value is not less than the predefined trust threshold, the user can then execute the permissions associated with his role. In this way we retain the administrative benefits of RBAC and at the same time mitigate the inflect ability and static nature of the RBAC by exploiting dynamism through context awareness in the access control decision.

Our context-aware access control approach for banking services has major implications for other context-aware services. For example, it treats contextual attributes as access decision parameters to provide effective and more appropriate security. In addition to location and time, we have taken into account other context that can be used in other context-aware services such as health services, education services and the military.

The proposal is valid for any system where users are identified and the three contexts are paramount. If a system does not meet so many contexts the case study has a situation where two contexts are taken into account. Our example is based on a banking system, but the general architecture can be applied to other systems that have similar context constraints.
The access authorization process is summarized below:

Step 01: After a session is started, a user requests access to a service.

Step 02: The access control manager retrieves the role of the user and the trust value in the database (Role / permission) and in trust Evaluator respectively.

Step 03: This manager verifies the level of trust if it is greater than 0, otherwise access is denied.

Step 04: It calculates the trust value according to the context after the user's context recovery and the service context.

Step 05: The access control manager adds up the two trust values, if the result is greater than or equal to the confidence level then access is granted. Otherwise a subtraction is made between the confidence level and the trust value, if the result is less than 0.1 then access is granted, otherwise access is denied.

The general operation of the access control process is illustrated by the flowchart of figure 2.

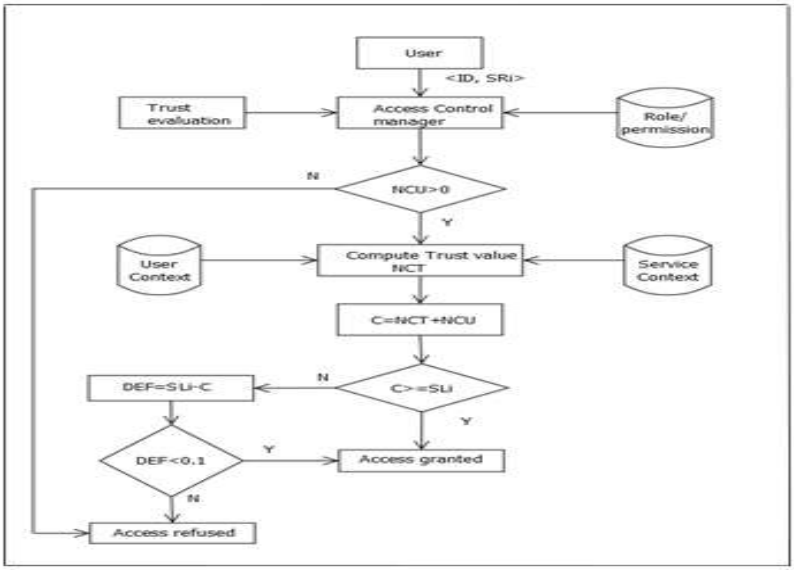


Figure 2. The access control process

4. SYNTHESIS

Our proposal retains the idea of considering the context parameters because it will allow us to have a dynamic access control system, context aware and which adapts the permissions according to current context. We also retain the notion of trust for our system, where we will establish a

relationship of trust with the user according to the contextual constraints and it is with respect to this trust that we will decide to grant or refuse access.

In order to offer a better adapted access control, we include other concepts. Indeed, in addition to the concept of predefined role three types of contexts will be used to enrich the access control system with context-aware access control. The contexts taken into account in our approach are the temporal context, location and social context. Enriching an access control system with different types of contexts makes it more adaptable for any situation and also more flexible.

1) Context-aware access control models:

In [4], only time and location is taken into account in access control. Quality of context is an interesting parameter to be considered in the future, and CoDRA [5] takes into account time and location, but we think that energy and connectivity are not useful for granting or denying access.

2) Role-based context-aware access control models:

RBAC only proposes the consideration of functional roles in access control, but not contextual roles, even if they evoke the usefulness of temporal authorizations. Note that this allows ordering the roles between them, but not to model constraints involving the time explicitly compared to the proposed model where the time context is taken into account. In other words, our approach essentially implements context awareness. In this way, we retain the administrative benefits of RBAC and, at the same time, mitigate the inflexibility and static nature of RBAC by the dynamism exploited through context awareness in access control decision making.

In the SRBAC solution [8], roles / permissions are granted to a user in specific time intervals and / or if the user is in a particular location. But SRBAC does not support the use of a defined role in a limited geographic space. On the other hand, our proposed model allows it thanks to the determination of the familiar places for example, the workplace, the house and the bank in our case study. DRBAC [7] dynamically adjusts the authorization assignment as well as the role assignment based on contextual information of a subject. DRBAC does not really meet our requirements for a context-aware access control solution. But once the roles are determined, which is the case in our proposal, significantly reduces the complexity of managing security.
The rest of the cited models [6, 9, 10, 11] have as inconvenient the fact that only time and location are used to define context. We think that social feature is an important context parameter in access control.

3) Trust-based context-aware access control models:

ConXsense [12] defines familiar locations as user's trusted environment but do not manage trust. Trust is a dynamic relative parameter, and CloudFile [13] considers social context through social networks, but trust is determined only on this social context. In [14], the author's contribution is to consider two trust levels based only on communications behaviour. The trust management is complex and not refined.

TIRIAC [15] takes into account risky accesses and trust is given degrees of confidence which enriches the access control. The advantage of TIRIAC is that it is a framework for grid access control and so the level of security must be as refined as that.

4) Hybrid access control based on role, trust and context awareness models:

The proposed solution belongs to this class, where the models are complete. In[16], the authors consider confidence in the user (trust) as context information and so manage context information to decide on access control. The two managers, trust and context, should be separated for more strongness. CATRAC [17] uses a role authority to assign roles which is not very relevant in our case (roles are fixed), and levels of trust based on user's access history, which limits context. CASSEC 2.0 [18] extends a geo-spatial RBAC by adding degrees of reliability (or trust) in the contextual information to confirm the user's location. Other context features would have been necessary.

Table 4. summarizes the previous comparison based on context role and trust.

Table 4. Context-aware access models comparison

Model	Role	Time	Location	Social	Trust	Other
S-RBAC [8]	X	X	X			
GEO-RBAC [9]	X	X	X			
ST-RBAC [11]	X	X	X			
D-RBAC [7]	X	X	X			
C-RBAC [10]	X	X	X			
RFID-RBAC [6]	X	X	X			
Fine-grained Access Control [16]	X	X	X		X	
CATRAC [17]	X	X	X		X	
ConXsense [12]			X	X	X	
Context Quality-Aware [4]		X	X			Quality of context
General Trust/Local Trust [14]					X	
CoDRA [5]		X	X			Energy/ Bandwidth
TIRIAC [15]			X		X	Risk management
CASSEC 2.0 [18]	X		X		X	Confidence specifiers
CloudFile [13]				X	X	
Proposed approach	X	X	X	X	X	

As mentioned earlier, previous systems check if the client has the proper role to access a particular web service. However, the verification of the client reliability gives more assurance to the provider. Our work has similarities to trust-based access control models. Indeed, the trust level of the client is verified during each access attempt to ensure that it is high enough to access the requested service while being based on contextual constraints. This is what makes our approach more efficient and reliable.

Our model has the following advantages:

- In addition to role concept, a set of three contextual attributes: Time, Location and Social has been taken into account.
- The presence of a correlation between the three contexts.
- Trust is dynamic.
- The role-based policy analysis concludes that they are relatively easy to administer and flexible enough to adapt to each organization.

5. CONCLUSIONS

Using context information is an asset for creating access control models. We focused on context-aware access control in ubiquitous systems. Entities operate in environments that are dynamic and unpredictable, forcing them to be able to guarantee security. In particular, banking systems are complex, feature-rich systems that are becoming more and more demanding in terms of security: confidentiality, integrity, availability and accountability. Therefore, it is essential to first define a security policy that is robust, efficient, flexible, generic and easy to verify.

Our context-aware access control model is based on a cross-use of role; contextual constraints and trust, as flexible enough structuring tools that complement the gaps presented by some models. In the same way that the role binds the users to the privileges, the trust according to the contextual constraints makes it possible to establish a relation between the operations and the objects to be protected. We also frame the concept of context awareness to allow access control respecting the principle of least privilege while ensuring flexibility favoring the user's profit. We have detailed the operation of our system by applying it on a bank where we presented a case study with service, entities, roles and contextual constraints for each service and entity.

Like any research, our model has some limitations. The main thing is that we have not been able, yet, to perform a simulation to highlight the real benefits of this mechanism. So, it would be opportune to pursue research along several lines. First, it would be wise to study the integration of a mechanism to deal with attacks. Indeed, some attacks aim to oppose traditional systems of blocking or protection. It is thus necessary to be able to quickly detect the intrusion to reduce the damage which can be caused by the hacker or the steal of data that it can realize. So the proposed access control system should deflect known attacks, detect ongoing attacks, including those coming from within, and react quickly.

Then, in order to be able to test our mechanism in real size, it is necessary to have realistic context information, through context simulators and also direct captures on a physical environment. The next step is to create a realistic map representing the environment of our case study, in other words, to reproduce a realistic plan of a banking space, then to:

- Simulate the behavior of clients accessing a banking service and carrying out different activities.
- Periodically retrieve the contextual information (Time, location and people around) from the user and send this information periodically to the context manager.
- Implement and deploy a prototype of the proposal in the appropriate environment.

REFERENCES

[1] Weiser, Mark (1999) *Some computer science issues in ubiquitous computing*, Mobility: Processes, Computers, and Agents, ACM Press/Addison-Wesley, NY, pp420-430.

[2] Jemili, S. (2013) *Analyse de risqué dans les systèmes de contrôle d'accès*, Master report, University of Quebec en Outaouais, Canada.

[3] Ferraiolo, D. F, J. A. Cugini, & O. H. Kuhn (1995) "Role-Based Access Control (RBAC) : Features and Motivations". Proceddings of 11th Annual Conference on *Computer Security Applications* pp 241-248.

[4] Filho, J. B. & H. Martin (2008) "A quality-aware context-based access control model for ubiquitous applications", Proceedings of International Conference on *Defects in Insulating Materials (ICDIM)*, Aracaju, Brazil, pp 113-118.

[5] Thanigaivelan, N. K., E. Nigussie, A. Hakkala, S. Virtanen & J. Isoaho (2018) "CoDRA: Context-based dynamically reconfigurable access control system for Android", Journal for *Network and Computer Applications*, Vol. 101, pp1-17.

[6] Khan, M. F. F. & K. Sakamura (2012) "Context-Awareness : Exploring the Imperative Shared Context of Security and Ubiquitous Computing", Proceedings of the 14th International Conference on *Information Integration and Web-based Applications & Services*, Bali, Indonesia, pp101-111.

[7] Zhang, G. & M. Parashar, (2003) "Dynamic Context-aware Access Control for Grid Applications", Proceedings of 4th international Workshop on *Grid Computing*, Washington, USA., pp101-108.

[8] Hansen, F. & V. Oleshchuk (2003) "SRBAC : A Spatial Role-Based Access Control Model for Mobile Systems ", Proccedings of 7th Nordic Workshop on *Secure IT, Systems*, Gjvik, Norvège, pp 136-152

[9] Bertino, E., B. Catania, M. Damiani, & P. Perlasca (2005) "GEO-RBAC : A Spatially Aware RBAC", Proceedings of the tenth ACM symposium on *Access control models and technologies*, Stockholm, Sweden, pp 29-37.

[10] Park , S.H, Y. J. Han & T. M. Chung (2006) "Context-role based access control for context-aware application", In: Gerndt M., Kranzlmüller D. (eds) High Performance Computing and Communications. HPCC vol. 4208.

[11] Ray, I.. & M. Toahchoodee (2007) "A spatio-temporal role-based access control model", Proccedings of 21st Annual International Federation for *Information Processing Working Group*, pp211-226.

[12] Miettinen, M., S. Heuer, W. Kronz, A.-R. Sadeghi & N. Asokan (2014) "ConXsense Automated Context Classification for Context-Aware Access Control", Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, Kyoto, Japan, pp293-304.

[13] Yan Z. & W. Shi (2017) "CloudFile: A cloud data access control system based on mobile social trust", Journal of *Network and Computer Applications*, vol. 86, pp46-58

[14] Yan, Z., H. Xie, P. Zhang & B. B. Gupta (2018) "Flexible data access control in D2D communications", *Future generation computer systems*, pp738-751.

[15] Noggorani, S. D. & R. Jalili (2016) "TIRIAC: A trust-driven risk-aware access control framework for Grid environments", *Future generation computer systems*, Vol. 55, pp238-254.

[16] Hong-Yue, L., D. Miao-Lei & Y. Wei-Dong & (2012) "A Context-aware Fine-grained Access Control Model", Proccedings of 21st the International Conference on *Computer Science and Service System*, pp1099-1102.

[17] Ghali, C., A. Chehab & A. Kayssi (2010) "CATRAC : Context-Aware Trust- and Role-Based Access Control for Composite Web Services", Proceedings of 10th International Conference on *Computer and Information Technology (CIT)*, pp1085-1089.

[18] Oluwatimi, O., M. L. Damiani, E. Bertino (2018) "A context-aware system to secure enterprise content: Incorporating reliability specifiers", *Computers & Security*, vol. 77, pp162-178.

CONSTRUCTION OF AN ORAL CANCER AUTO-CLASSIFY SYSTEM BASED ON MACHINE-LEARNING FOR ARTIFICIAL INTELLIGENCE

Meng-Jia Lian[1], Chih-Ling Huang[2]*, Tzer-Min Lee[1,3]*

[1]School of Dentistry, Kaohsiung Medical University, Kaohsiung, Taiwan
[2]Center for Fundamental Science, Kaohsiung Medical University, Kaohsiung, Taiwan
[3]Institute of Oral Medicine, National Cheng Kung University Medical College, Tainan, Taiwan

ABSTRACT

Oral cancer is one of the most widespread tumors of the head and neck region. An earlier diagnosis can help dentist getting a better therapy plan, giving patients a better treatment and the reliable techniques for detecting oral cancer cells are urgently required. This study proposes an optic and automation method using reflection images obtained with scanned laser pico-projection system, and Gray-Level Co-occurrence Matrix for sampling. Moreover, the artificial intelligence technology, Support Vector Machine, was used to classify samples. Normal Oral Keratinocyte and dysplastic oral keratinocyte were simulating the evolvement of cancer to be classified. The accuracy in distinguishing two cells has reached 85.22%. Compared to existing diagnosis methods, the proposed method possesses many advantages, including a lower cost, a larger sample size, an instant, a non-invasive, and a more reliable diagnostic performance. As a result, it provides a highly promising solution for the early diagnosis of oral squamous carcinoma.

KEYWORDS

Oral Cancer Cell, Normal Oral Keratinocyte (NOK), Dysplastic oral keratinocyte (DOK),Gray-Level Co-occurrence Matrix (GLCM), Scanned Laser Pico-Projection (SLPP), Support Vector Machine (SVM), Machine-Learning.

1. INTRODUCTION

Oral cancer is a common neoplasm worldwide. Over the past decades, it shows a progressive increment in its incidence and mortality. Though there'are some surgical and radiotherapeutic improvements, it still shows a poor prognosis and also low survival rate. As the development of oral cancer, the cell will first become dysplastic, a pre-cancerous stage. Later, the cells will turn into carcinoma *in situ*, that is, the cells are abnormal cells, which might have a high speed of DNA/RNA duplication and undergo ultimate replication out of control. Most importantly, the cells are still in place, an indication of high curabilty after removal and a smaller excition area for faster recovery. Finally, the cells become cancerous, not only carcinomatous, but also gains the ability to move and invade into other tissues, more precisely, metastasis. Earlier detection of the

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 33-39, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90903

abnormal growth of oral tissue can provide a promising future for a better therapy planing and a higher survival rate.

For many years, many non-invasive imaging techniques have been proposed for the clinical diagnosis of cancers, including X-rays, computed tomography (CT), positron emission tomography (PET), ultrasonography (US), magnetic resonance imaging (MRI), and tissue polarimetry. For oral cavity, Dental Cone Beam CT, and impression scan with CAD/CAM is also a new era of making a computed 3D oral model. Recently, due to the higher computing power and smarter artificial intelligence, many computing techniques are now adding to help analyzing the medical images and aid the doctors in diagnosing diseases. Therefore, an urgent requirement exists for more timely, non-invasive, and quantitative system for detecting the presence of abnormal cells and classification of the different stage of oral cancer.

With the scanned laser pico-projection (SLPP) system, Chuang[1]*et al*. put out a method for extracting the two-dimensional (2-D) nanoparticle concentration of solid and liquid solutions through an inspection of the speckle contrast of the images obtained. The feasibility of the proposed approach was demonstrated by measuring Type I collagen concentrations ranging from 0.025 ~ 0.125%.There are many practical benefits, such as infinite focus, inherent high image contrast and also good power efficiency thatSLPP systems can provide in optical diagnosis[2].

Gray-Level Co-occurrence Matrix (GLCM) functions characterize the texture of an image by adding up how often pairs of pixel with specific values and in a specified spatial relationship occur in an image, creating a GLCM, and then extracting statistical measures from this matrix. D. Molina *et al.*[3] used GLCM to analyze the medical imaging on brain tumor heterogeneity obtained from magnetic resonance images (MRI) and find its potential relationship with tumor malignancy. In the past years, the author has proved that image obtained with SLPP and process with GLCM can successfully provide a great discrimination between low metastatic cancer cells and high metastatic cancer cells[4], and the combination of the two techniques is also useful in distinguishing oral pathological sections[5].

Machine-Learning is a part of Artificial Intelligence (AI) that the computer learns without manifestly programmed. With the data inputted and the task set, as the computer programmed learned, the performance of the program is said to be improved as the data increased. In other words, the program optimizes itself to reach a higher performance, that is, accuracy in classify tasks. Support Vector Machine (SVM) is a basic yet clever script used in machine-learning. With label assigned, and data taken as vectors, the SVM is solving the following mathematic problems to find the greatest margin when classify each labels and thus creating a classify model. For the past decades, many more optimization options occured to strengthen the SVM, including the kernels and cross-validation. Kernels are ways to project the data into a higher dimensional space, creating a better distribution for classification. The most common ones are the linear, the polynomial, the radial basis function (RBF), and the sigmoid kernels. Due to the parameters inside the kernel, it needs to be optimized for a better projection. Cross-validation devides the data into several groups, and use one as a testing set, the re

mainings as the training set each time. It is a method for the computer to test itself, and eliminate the effect of some unusual data's. Otherwise, it will create a over-fitted model.

$$\min \frac{\|w\|^2}{2} \quad subject\ to\ \ y_i(w^T x_i + b) \geq 1, i = 1,2, \ldots\ldots, n \quad \{1\}$$

In our study, we will use 2 cell lines to verify the validity of our system. The system is first comprised of a SLPP technique to obtain image, then with GLCM to process the image, extracting some figures out, finally the SVM calculation to create a classification model to achieve the detection of oral cancer. Compared to the existing diagnostic process, the proposed method provides a highly promising solution for the faster, non-invasive, and early diagnosis of oral cancer.

2. MATERIALS AND METHODS

2.1 Sample Preparation

Cell lines were incubated at 37°C with 5% CO_2, and cultured in 2 well silicone separator 48hrs before taking image. Each well was filled with $3x10^4$ cells to form a uniform monolayer. While taking images, the separator is pulled off, forming a blank region on the slide. Then, the samples were washed twice using phosphate buffered saline solution (PBS, 0.1 M, pH = 7.4) or Hank's Balanced Salt Solution (HBSS, no calcium, no magnesium) depending on the cells. The details of each cell line are described in the following.

1. **NOK**, Normal Oral Keratinocyte: The cell line was established from human normal oral mucosa and grown in keratinocyte serum-free medium (KSFM) with low calcium.
2. **DOK,** Dysplastic Oral Keratinocyte: When normal oral keratinocytes go wild and becoming cancerous, it first turn dysplastic, or pre-malignant. This cell line, DOK, was obtained from heavy smoker's dysplastic dorsal tongue epithelium and cultured in Dulbecco's Modified Eagle Medium (DMEM), with 2mM Glutamine, 5μg/ml Hydrocortisone, and 10% Foetal Bovine Serum (FBS).

2.2 Experimental Setup

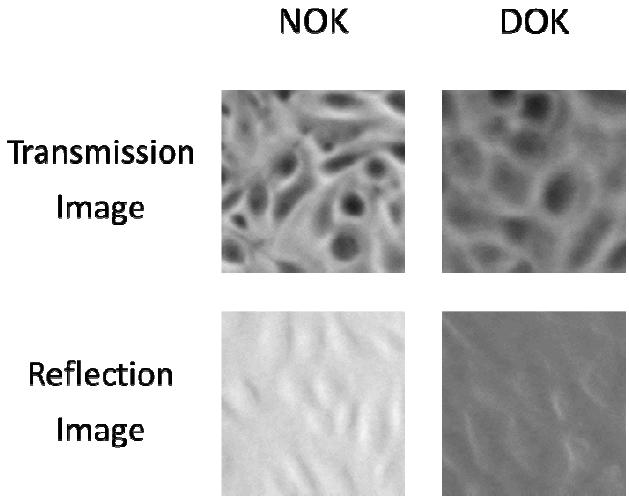
The optical diagnosis system used in this study comprised a SLPP (SONY; Model: MP-CL1A; Resolution: 1920 × 720; Aspect Ratio: 16:9 Widescreen; Contrast Ratio: 80,000:1; Image Size: 40 inch @ 1.15 m) and a microscope (Nikon Eclipse TS-100). In accordance with the findings of a previous study, the samples were illuminated using a green laser source (wavelength = 532 nm) in order to enhance the sensitivity of the reflection image measurements. In obtaining the transmitted images of the cells, the samples were illuminated using a halogen lamp. The cell images and speckle images were captured using a CCD camera (Model: PMD-500) with IS Capture and View image acquisition software. To calibrate the background noise of different image, we calculate SNR (Signal to Noise Ratio). The images (2592×1944 pixels, about 5 megapixels) were partitioned into 2 files, one with cells is regarded as 'Signal' and the other without cell (the blank area caused by the silicone separator) is regarded as 'Noise'. Thus, the image captured can now stand on the same point for comparison.

The GLCM image-processing and SVM model generation is all coded on Matlab R2018a. For each image, it'll first turned into 8bit gray level image, and crop into several sub-images, size 150 × 150 pixels for better performing speed. Then, we use GLCM to gain the pattern of each sub-image, calculate the SNR and written it into the file. After that, we use LIBSVM[6], a SVM

toolbox developed by National Taiwan University, Department of Computer Science, which provide many useful SVM functions together. Originally written in C+, the LIBSVM toolbox can be translated into Matlab for us to compile everything together. To find the best classify model, we perform cross-validation for self-testing of the machine and prevent over-fitting problems. For better data distribution, we also added some kernels to project the data into a higher dimensional distribution for better solving the non-linear separable problems.

3. RESULTS AND DISCUSSION

Figures 1 shows the transmission and reflection images of these two cell lines (NOK and DOK). As Figure 1 shows, all cells are appeared in squamous shape and firmly attach to their neighbouring cells. Compared to NOK, the normal one, DOK cells become more spindle-shaped. The reflection images were taken from SLPP system. In this study, we try to use a new light source system, SLPP, to provide a routine quality assurance for imaging. The SLPP system can decrease the light intensity with Gaussian distribution from central to the margin via the scanning laser pico-projection technique for wide screen. Moreover, SLPP system is a commercial projection device for wide screen and enhance the usability for imaging. We also do the effort in the case of biopsy from the patients, such as characterization for oral cancer by pathological images. SLPP system with GLCM image processing can differentiate normal & cancerous pathological sections and it works on both full field analysis and specific tissue analysis. The discrimination of normal and cancerous tissues depends on the disorder caused by unusual proliferation and division of the chromosomes and nuclei. Compared to existing methods, the proposed method approach has many advantages, including a lower cost, a larger sample size and a more reliable diagnostic performance.



Figures 1. Transmission and reflection images of these two cell lines (NOK and DOK).

In the subsquent step, we run the classify machine for artificial intelligence to distinguish the NOK and the DOK cells. We use 4 transmission image, 3 reflection image of NOK and 8 transmittion image, 8 reflection image of DOK. For each image, we randomly cropped out 5 areas to go under the GLCM analyzing. Totally, 115 datas, each with 4 features, are sampled and

imported into the SVM. The results are shown below. Table 1 shows the use of different SVM kernels for projecting the data into a higher dimension distribution, except the linear one. Accuracy is from the cross-validation, a self-testing method when forming a classify model. Figure 2 shows the optimization of RBF kernel. When optimized, we add a Cost (C) parameter as penalty of the mis-classified points in the original script, and the RBF kernel uses a gamma(γ) as a parameter in its exponential function. Due to previous studies, the most efficient way to optimized the two parameters is to test it exponentially. Therefore, we briefly searched it once using a bigger grade(as shown in figure 2a) and search it again using a smaller grade in a more targeted range(as shown in figure 2b). Accuracy do raised after the optimization.

Table 1. The classify accuracy of NOK and DOK according to the different SVM kernel.

Kernels	Linear	Polynomial	RBF	Sigmoid
Parameter number	1	3	2	3
Accuracy	77.3913%	69.5625%	69.5625%	69.5625%

Note: all the samling steps in GLCM is (x,y)=(1,0).

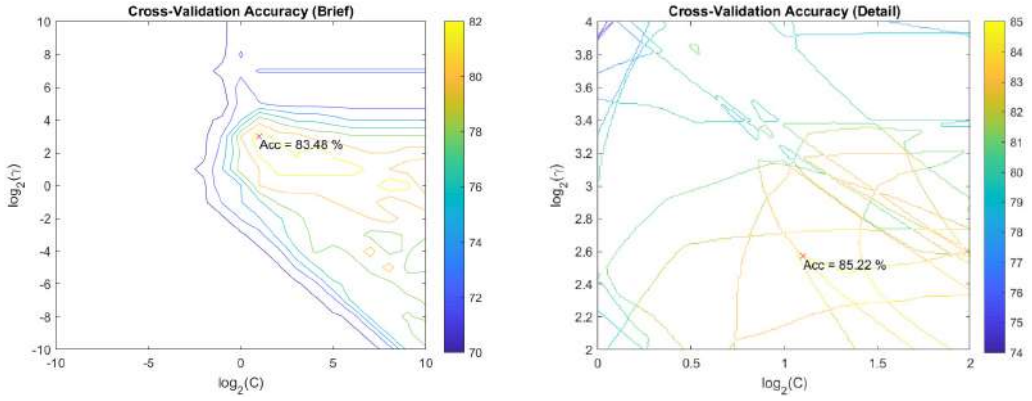


Figure 2a(left)**& 2b**(right) Optimization of RBF kernel with the Cost parameter and gamma optimization.

4. CONCLUSIONS

As the cancer developed, the cells became dysplastic first, turned carcinoma later, and finally invasive. The morphology change of the cells is corresponding to the transformation of cell function. With the aid of SLPP for obtaining a high-resolution image, and the GLCM for better sampling the pattern of the image. With the help of SVM of machine-learning, the system can get the accuracy around 70% in classifying the NOK and DOK. After adding a brief optimization, altering the parameters inside the RBF kernel and the SVM scripts, the classify machine can now reaching 85.22% accuracy, compared to 69.525% without optimization. The result gives out that our method can help to distinguish NOK and DOK, the normal oral keratinocyte and the

dysplastic one, providing a promising future of an instant, non-invasive, and early diagnosis of the existing of pre-cancerous cells.

ACKNOWLEDGEMENTS

The author would like to acknowledge the College Student Research Scholarship, MOST (107-2813-C-006 -179 -B) for supporting this project. The authors also gratefully acknowledge the financial support provided to this study by the Ministry of Science and Technology (MOST) in Taiwan under Grant Nos. MOST-107-2221-E-037-003. Supported by a grant from the Kaohsiung Medical University Research Foundation (KMU-Q107023). Furthermore, authors appreciate the kindly help from Prof. KW Chang from NYMU, ROC; Prof. LW Wu from NCKU, ROC. Prof. YC Lin from KMU, ROC for providing the cell lines; Prof. W.-T. Chiu and Prof. Y.-L. Lo from NCKU for helping solving the problems in cell culture and some technique advises.

REFERENCES

[1] C. H. Chuang, T. W. Sung, C. L. Huang, and Y. L. Lo,(2012) "Relative two-dimensional nanoparticle concentration measurement based on scanned laser pico-projection," Sensors and Actuators B: Chemical, vol. 173, pp. 281-287.

[2] K. V. Chellappan, E. Erden, and H. Urey,(2010) "Laser-based displays: a review," Applied Optics, vol. 49, no. 25, pp. F79-F98.

[3] D. Molina et al., (2016)"Influence of gray level and space discretization on brain tumor heterogeneity measures obtained from magnetic resonance images," Computers in Biology and Medicine, vol. 78, pp. 49-57.

[4] C.-L. H. Meng-Jia Lian, (2018)"Texture feature extraction of gray-level co-occurrence matrix for metastatic cancer cells using scanned laser pico-projection images," Lasers in Medical Science, journal article July 24.

[5] C.-L. H. Meng-Jia Lian, Tzer-Min Lee, (2018)"Automation Characterization for Oral Cancer by Pathological Image Processing with Gray-Level Co-occurrence Matrix," Journal of Image and Graphics, vol. 6, pp. 80-83.

[6] C.-C. a. L. Chang, Chih-Jen, (2011) "{LIBSVM}: A library for support vector machines," ACM Transactions on Intelligent Systems and Technology, vol. 2, no. 3, pp. 27:1--27:27.

AUTHORS

Meng-Jia Lian is a college student of School of Dentistry, Kaohsiung Medical University. Since 2017, he join the research group of Kaohsiung Medical University and his research interest is image processing. He got the Excellent Oral Presentation of 2018 International Conference on Smart Materials Applications (ICSMA 2018), Singapore, Jan. 2018. In 2017 and 2018, he won the Superior award in the competition of Student Clinician Program (SCP) supported by Dentsply, which is the world's largest manufacturer of professional dental products and technologies, combining leading platforms spanning consumables, equipment, technology and specialty products.

Chih-Ling Huang received her BS, MS, and PhD degrees from the Department of Material Science and Engineering, National Cheng Kung University, Taiwan, China, in 2003, 2005, and 2010, respectively. After graduation, she has been a postdoctoral researcher in Department of Mechanical Engineering, National Cheng Kung University. Since 2016, she has been a member of the Center for Fundamental Science, Kaohsiung Medical University, where she is now an assistant professor. She got the 2015 Young Scholar Award of Taiwan Comprehensive University System and 2016 Outstanding Research Award of Kaohsiung Medical University.

Dr. Tzer-Min Lee received the B.S. degree from the B.S., M.S., Ph.D. degrees from National Cheng Kung University (NCKU) in 1991, 1993, and 1998, respectively, all in materials science and engineering. In 2003 he joined the Institute of Oral Medicine at the National Cheng Kung University (NCKU) as an Assistant Professor (non-clinical). In 2006 he was promoted to the position of Associate Professor and was named a full Professor in 2010. He is also Professor of Biomedical Engineering, NCKU. He has served as Vice Dean of College of Medicine, NCKU. He has appointed as Deputy Director of Medical Device Innovation Center (MOE University Advancement). Dr. Lee was named Dean of College of Dental Medicine, Kaohsiung Medical University in 2015. He gained 2005 Young Investigator Research Award, College of Medicine, National Cheng Kung University; 2008 Ta-You Wu Memorial Award, National Science Foundation, Taiwan; 2006/2009/2010/2012/2013/2014/2015 Best Paper Award, Cheng Kung Medicine Foundation for Education. His research activities involve bioactive ceramic coatings, model surfaces for cell culture and animal testing, and implant surface modifications and testing. He has published 65 journal papers, 120 conference papers, and 2 book chapters.

INTENTIONAL BLANK

EFFICIENT TOUGH RANDOM SYMMETRIC 3-SAT GENERATOR

Robert Amador[1], Chen-Fu Chiang[2], and Chang-Yu Hsieh [3]

[1,2]Department of Computer Science, State University of New York Polytechnic Institute, Utica, NY~13502, USA.
[3]This work was done while the author was a post doc at Singapore-MIT Alliance for Research and Technology, USA

ABSTRACT

We designed and implemented an efficient tough random symmetric 3-SAT generator. We quantify the hardness in terms of CPU time, numbers of restarts, decisions, propagations, conflicts and conflicted literals that occur when a solver tries to solve 3-SAT instances. In this experiment, the clause variable ratio was chosen to be around the conventional critical phase transition number 4.24. The experiment shows that instances generated by our generator are significantly harder than instances generated by the Tough K-SAT generator. The difference in hardness between two SAT instance generators exponentiates as the number of Boolean variables used increases.

KEYWORDS

3-SAT, Satisfiability, Efficient Tough Random Symmetric 3-SAT Generator, Critical Phase Transition

1. INTRODUCTION

The 3-satisfiability problem (3-SAT) can be succinctly summarized as follows: find an n-binary-variable configuration to satisfy a conjunction of clauses with each being a disjunction of three literals. It is a widely studied problem for several reasons. First, it plays a crucial role in the historical development of theoretical computer science. For instance, it was the first identified NP-complete problem, [[1], [2]] and one of the most well-studied examples in the inter-disciplinary research program involving computer science, combinatorial optimization [[3], [4]] and statistical physics [[5], [6]]. Besides these interesting developments on the theoretical front, the 3-SAT problem also plays a critical role in many applications such as model checking, planning in artificial intelligences and software verifications. Hence, for both theoretical and practical reasons, there are many strong motivations to devise more efficient algorithms to attack such a problem.

2. PROBLEM STATEMENT & MOTIVATION

The inter-disciplinary approach (especially invoking statistical physics methods and concepts) has certainly helped us to build a comprehensive picture of the complex structures of the 3-SAT

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 41-49, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90904

problem. For instance, the concept of phase transitions in statistical physics has been adopted to elucidate the SAT-UNSAT phase transition of 3-SAT problems. In this statistical framework, the ratio parameter, $(\alpha \equiv m/n)$) for the phase transition is taken to be the ratio of the number of clauses (m) to the number of variables (n). The critical value of this order parameter is $\alpha_c = 4.2$ [[7], [8]] which clearly draws a boundary in the space of all 3-SAT instances. We explore 3-SAT problems with a critical value of 4.2 in comparison to 3-SAT problems generated by a Tough Random K-SAT Generator to better understand how the critical value effects solvability of 3-SAT Problems. Studying this specific subset of 3-SAT problems will enable further research into solving SAT problems more efficiently.

3. BACKGROUND

In various SAT solvers/generators, the commonly used parameters are: n: the number of variables, m: the number of clauses, α: the ratio, which is determined by m/n. For an efficient tough random symmetric 3-SAT generator, a formula *F* is of n variables with the ratio number α that should have $\alpha * n$ clauses. In this work, we choose the ratio number close to the phase transition number 4.24. Particularly in 3-SAT, since each clause has 3 literals, each variable is expected to appear approximately $3 * \alpha$ times in *F*.

Tough SAT Generator is one of the competitive generators out there for generating tough SAT instances. We would like to compare the toughness of instances generated by our generator and TSG in the following categories: (a) frustrations caused by the generator to the SAT solver and (b) probability of generating instances that are solvable (that is there is at least one solution). The frustration rate can be quantified by the resources used by the solver, such as CPU time, restarts, conflicts and decisions. The probability can be quantified by the ratio between instances with solutions and the total instances generated by the generator.

The contribution of this work is to devise a way to generate harder instances and verify their hardness. We aim at generating those harder instances more efficiently and reliably. The hardness is quantified by the measures given in the solver that the instances require the solver to consume more resources and make more modifications. Our algorithm is more reliable as it generates with a higher probability of instances that have solutions. Our algorithm is also efficient as the generation process is almost linear time. With a verified efficient reliable algorithm that generates harder instances, in a later study we can characterize harder instances in another dimension, in addition to the conventional critical phase transition number.

3.1. Algorithms

In following paragraph, we describe the TSG algorithm (alg 1) and our efficient tough random symmetric 3-SAT generator (ETRSG) algorithm (alg 2). They can both generate SAT instances efficiently in almost linear time.

Algorithm 1 Tough Random K-SAT Generator

Require: k: literals per clause, n: number of variables $(v_1, ..., v_n)$, m clauses
Ensure: Tough random K-SAT formula
Start of algorithm
$F = \emptyset$
for $i = 1, \cdots, m$ **do**
Randomly select k random variables from $[v_1, ..., v_n]$
for $j = 1, \cdots, k$ **do**
For the chosen random variable, randomly assign negation operation
Form clause C_i based on the generated k random literals
$F = F \wedge C_i$
Output F
End of algorithm

The TSG algorithm basically generates m clauses sequentially. In the 3-SAT case, each clause is generated by randomly picking 3 variables from the variable list and with 0.5 probability, the chosen variable is then assigned an negation operation. With the disjunction of the literals, a clause is formed.

The ETRSG algorithm generates m clauses sequentially. But initially it must generate a big sequence s_f that is of 3α subsequences. Each subsequence is a random arrangement of n variables. To avoid adjacent subsequences from forming an invalid clause, that is duplicated variables or literals, we must call the RndGen-Verif subroutine (alg 3) to ensure its validity. If two adjacent sequences are jointly required to produce a particular clause, the ETRSG algorithm checks the adjacent subsequences s_i and $s_{i+1}$to make sure a variable would not appear more than once in that particular clause.

Algorithm 2 Efficient Tough Random Symmetric 3-SAT Generator (ETRSG)

Require: n: number of variables $(v_1, ..., v_n)$, α: desired ratio number number
Ensure: Tough random symmetric 3-SAT formula
Start of algorithm
$F = \emptyset$, $r = \lceil 3 * \alpha \rceil$, $m = \lceil \alpha n \rceil$, s_f an empty string
for $i = 1, \cdots, r$ **do**
Call RndGen-Verif to generate a valid random sequence s_i of n distinct variables
$s_f = \text{Concatenate}(s_f, s_i)$
for $j = 1, \cdots, m$ **do**
Pick 3 variables at position $(j-1) * 3 + 1, (j-1) * 3 + 2, (j-1) * 3 + 3$ from s_f
For the chosen random variables, randomly assign negation operation
Form clause C_i based on the generated 3 random literals
$F = F \wedge C_i$
Output F
End of algorithm

Once s_f , of length $\lceil 3\alpha \rceil n$, is generated, each variable appears $\lceil 3\alpha \rceil$ times and then we can generate m clauses sequentially from position 1 until position $3m$ of s_f . For each position we also randomly assign the negation operation.

Algorithm 3 Random Generation Verification (RndGen-Verif)

Require: s_f: sequence generated so far, n: number of variables
Ensure: a valid sequence s that would avoid invalid 3-SAT clauses
  Start of algorithm
  Generate a random sequence s of n distinct variables
  if $((i-1)*n) \bmod 3 = 0$ **then**
    return s
  else if $((i-1)*n) \bmod 3 = 1$ **then**
    for Repetition of variables at the last position of s_f and positions 1, 2 at s **do**
      Regenerate s
  else if $((i-1)*n) \bmod 3 = 2$ **then**
    for Repetition of variables at the last two positions of s_f and positions 1 at s **do**
      Regenerate s
  Output s
  End of algorithm

3.2. Choice of Recurrence Number

The recurrence number r in ETRSG determines the number of times each variable must appear in the formula. In this paper, r is chosen based on selecting the ratio number α close to the well-known phase transition number. A phase transition [[5], [6]] is a concept utilized in statistical physics but it can also be used to better explain satisfiable and unsatisfiable transitions in 3-SAT problems. In reality, even instances with the critical phase transition number might be easy to solve for a modern solver. The 4.24 phase transition could be where more tough instances exist. In comparison to all possible instances with a critical phase transition number 4.24, this subset of tough instances might be exponentially rare among 3-SAT instances[9]. One of the major goals of this experiment is to figure out some of those exponentially rare instances and characterize them. The critical phase transition number is one of the characters for hard instances. In this experiment, we chose α= 4, 4.24 and 5. The rationale is that SAT instances with a ratio number greater than the critical phase transition number will almost always be rejected as there is no solution. SAT instances with a ratio number smaller than the critical phase transition number will likely have many solutions and therefore the SAT solvers can easily find the solution.

4. TOOLS AND EXPERIMENTS

4.1 Tools

4.1.1 Generators

The baseline generator is the Tough Random K-SAT generator [10] that generates random K-SAT instances, which is built upon latest techniques up to 2017. The other generator is our ETRSG algorithm. Both algorithms are explained in section 3.1.

4.1.2. Solver and Platform

MiniSAT is a minimalistic, open-source SAT solver, developed to help researchers and developers alike get started on SAT. It is released under the MIT license. MiniSAT deploys the Conflict Driven Clause Learning (CDCL) SAT solver with several other features such as clause deletion and dynamic variable ordering [[11], [12]]. A small glimpse into the inner workings of Minisat is provided as a basic introduction to conflict clause learning and to establish a small foothold on the basic idea of SAT solvers.

MiniSAT measures CPU time which, while valuable, is inconsequential as CPU time can change accordingly with better or worse hardware. It also provides other important measures. It stores the number of times the solver was forced to restart, conflicts, decisions, propagations, inspections and conflict literals deleted, which are all machine independent. The mechanism for the MiniSAT solver is as follows. When MiniSAT is given a SAT problem, it solves the problem by choosing a variable to begin propagation of other variables. When a conflict occurs, as in one literal is assigned both a positive and negative value, the solver will store this conflicting clause and begin propagation again from an older assignment but will avoid generating the prior conflicting clause. If the solver moves back to the original chosen variable, it is then restarted with a different variable and propagation begins again. This is redone until a satisfying assignment is found and the problem is deemed satisfiable or until it is shown that no satisfiable solution can be made, deeming the problem unsatisfiable. These are the results on which we will gauge the relative difficulty of the SAT instances.

The ETRSG algorithm was implemented in Python. The testing environment was created in cloud9, which is a cloud based ubuntu IDE. The environment has 512MB of available memory, 2GB of disk space which was more than enough for development and testing. In the case of MiniSAT, the CDCL algorithm used is ultimately machine independent because only CPU time will get better or worse with better or worse hardware respectively. Although, the times between the better and worse hardware can differ the algorithm will function the same way and have similar occurrences for restarts, conflicts, conflict literals, propagations, inspects, decisions and the rate of generating satisfiable instances.

4.2. Experiments

To compare the toughness of instances generated by TSG and ETRSG, we generate 3-SAT instances with test cases where $\alpha = 4$, 4.24 and 5. With each α, the number of variables n is set as 100, 150, 200, 250, 300 and 350. With each (α, n) pair we generate 400 instances for both TSG and ETRSG.

All the test problems were solved using the C instance of MiniSat V 1.4.1 and TSG version 1.1 K-SAT generator was used to generate the control problems.

5. RESULT

The experiment results were summarized in Figure 1 for $\alpha = 4$ case, Figure 2 for $\alpha = 4.24$ case and Figure 3 for $\alpha = 5$ case. What is worth noting is that the performance of TSG and ETRSG are almost similar when $\alpha = 4$. This could be explained that those instances are much easier to solve since there might exist multiple solutions. ETRSG remains a very stable high probability,

almost 1, of generating solvable instances while TSG gradually catches up, from 0.925 to 1, as the number of variables increases. When we compare with the $\alpha = 4.24$ case and $\alpha = 5$ case, it is obvious the hardness measures, such as restart, conflict and decision, increase a couple orders of magnitude as α increases.

The experiment also yielded similar results for the $\alpha = 4.24$ and $\alpha = 5$ cases overall. Simply looking at each α case, we can conclude that *ETRSG* instances are more difficult than the *TSG* instances. The order of magnitude increases as α increases.

The more interesting phenomena we observed was that ETRSG problems retained their difficulty and overall solvability over their randomly generated counterparts. This implies there could exist a different phase transition number for ETRSG problems which can lead to further development of difficult symmetric 3-SAT problems. However, this result leads us to the conclusion that our ETRSG is more efficient in generating more *difficult* problems while maintaining solvability.

6. DISCUSSION

6.1. Critical Zone Exploration for ETRSG

With the speculation that the critical phase transition zone might be different for ETRSG problems, it might be worth discussing the exploration of this new hot and cold zone of satisfiability. Since when $\alpha = 4$, it yielded highly satisfiable problems as seen in Figure 1, we speculate the critical phase transition zone might lie beyond this point. Furthermore, with evidence from Figure 2, we speculate the crucial phase transition zone for ETRSG could be even beyond $\alpha = 4.24$ as the ETRSG problems were all still highly satisfiable. The critical zone must occur before 5 as nearly all symmetric and TSG problems were unsatisfiable. In short, this new number must occur after 4.24 but before 5 and the problem of searching for this number can be approached in a multitude of ways. This could be investigated in another study.

Figure 1: $\alpha = 4$, 400 instances, Red: ETRSG, Blue: TSG. ETRSG problems and the TSG problems began to relate more directly to each other, and the advantageous difficulty of the ETRSG problem was deemed inconsequential.

6.2. Toughness

As pointed out earlier, problems that occur with the typical critical phase transition number 4.24 might turn out to be easy to solve [9]. We might need a finer characterization for harder instances. As shown in this experiment, it is clear that an equal recurrence number for all variables could be one character that can be used to describe this set of harder problems. As described previously when $\alpha = 4.24$ ETRSG still generates with an increasingly high probability (0.75 to 1) solvable hard instances while TSG has a decreasing probability (0.63 to 1). The success rate drops almost to 0 when $\alpha = 5$. As for other measures, such as CPU time, restart, conflict and decision (and so on), are of a higher order of magnitude. A follow up study would focus on scaling α between 4.24 and 5 for ETRSG while keeping solvable probability high and the magnitude of difficulty increasing. Another investigation is needed to determine the cause of success probability dip for only 100 and 150 variables when $\alpha = 4$ transitions to $\alpha = 4.24$. It could be due to numerical fluctuation or some hidden factors to be discovered.

Figure 2: $\alpha = 4.24$, 400 instances, Red: ETRSG, Blue: TSG. When more than 250 variables, ETRSG instances significantly outperform TSG instances in all aspects, except with slight outperformance in restart. ETRSG has a higher probability of generating solvable instances.

7. Conclusion and Future Work

As it shows in the experiment ETRSG 3-SAT problems tend to have a higher level of difficulty. This leads us to believe that the landscape of this type of problem might have many local minimums and only one unique global minimum. With such a landscape, a regular solver using Heuristics might be deceived to believe the local minimum is the global or it would take much more resources (time, space) for the solver to attack. To avoid bias, that is difficulty that has some solver dependency, we should translate the numerically-verified difficult problems into landscape problems.

Studying the landscape problem will allow us to better understand the difficulty of symmetric sat problems when compared to the relative ease of TSG 3-SAT problems. Also, as stated prior in section 5 a new phase transition number might exist for symmetric 3-SAT problems as the 4.24 ratio only applies to general 3-SAT problems. This new phase transition number will also help to shed light on difficulty and satisfiability bounds. Finally, a new partition-based solver that we are developing (for another study) can be used to tackle symmetric problems as it would be blind to the constraints of the problem as they would be broken down into smaller and more manageable problems.

ACKNOWLEDGEMENTS

R. A. and C. C. gratefully acknowledge the support from the State University of New York Polytechnic Institute.

Figure 3: $\alpha = 5$, 400 instances, Red: ETRSG, Blue: TSG. Similar to $\alpha = 4.24$, but more significant in restart. The probability of generating solvable instances drops quickly to 0 for both since 5 is greater than the critical phase transition number.

REFERENCES

[1] S. A. Cook, "The complexity of theorem-proving procedures," in Proceedings of the third annual ACM symposium on Theory of computing, 1971.

[2] R. M. Karp, "Reducibility among combinatorial problems," in Complexity of computer computations, Springer, 1972, pp. 85-103.

[3] C. H. Papadimitriou and M. Yannakakis, "Optimization, approximation, and complexity classes," Journal of computer and system sciences, vol. 43, pp. 425-440, 1991.

[4] R. Marino, G. Parisi and F. Ricci-Tersenghi, "The backtracking survey propagation algorithm for solving random K-SAT problems," Nature communications, vol. 7, p. 12996, 2016.

[5] S. Cocco and R. Monasson, "Statistical physics analysis of the computational complexity of solving random satisfiability problems using backtrack algorithms," The European Physical Journal B-Condensed Matter and Complex Systems, vol. 22, pp. 505-531, 2001.

[6] A. Percus, G. Istrate and C. Moore, Computational complexity and statistical physics, OUP USA, 2006.

[7] B. A. Huberman and T. Hogg, "Phase transitions in artificial intelligence systems," Artificial Intelligence, vol. 33, pp. 155-171, 1987.

[8] M. Mézard, G. Parisi and R. Zecchina, "Analytic and algorithmic solution of random satisfiability problems," Science, vol. 297, pp. 812-815, 2002.

[9] M. Žnidarič, "Scaling of the running time of the quantum adiabatic algorithm for propositional satisfiability," Physical Review A, vol. 71, p. 062305, 2005.

[10] https://toughsat.appspot.com/, "Tough SAT generation," 2017.

[11] N. Een, "MiniSat: A SAT solver with conflict-clause minimization," in Proc. SAT-05: 8th International Conference on Theory and Applications of Satisfiability Testing, 2005.

[12] N. Eén and A. Biere, "Effective preprocessing in SAT through variable and clause elimination," in International conference on theory and applications of satisfiability testing, 2005.

AUTHORS

Robert Amador studies computer and information science and received his master's from SUNY Polytechnic institute. His research interests include artificial intelligence and machine learning.

Dr. Chen-Fu Chiang studies computer science and received his master's from the University of Pennsylvania and his PhD from the university of Central Florida. He is currently an assistant professor in the Computer Science department at the University of New York Polytechnic Institute. His research focus is on quantum computation, theoretical computation and artificial intelligence.

Dr. Chang-Yu Hsieh studies physics. He received his PhD from the University of Ottawa Canada. Upon his graduation, Dr. Hsieh had been conducting research in quantum system as postdocs in University of Toronto and MIT. His research focus is on complexity, near term quantum systems and quantum algorithms.

INTENTIONAL BLANK

DATA ANALYSIS OF WIRELESS NETWORKS USING CLASSIFICATION TECHNIQUES

Daniel Rosa Canêdo[1,2] and Alexandre Ricardo Soares Romariz[1]

[1]Department of Electrical Engineering, University of Brasília, Brasília, Brazil
[2]Federal Institute of Goiás, Luziânia, Brazil

ABSTRACT

In the last decade, there has been a great technological advance in the infrastructure of mobile technologies. The increase in the use of wireless local area networks and the use of satellite services are also noticed. The high utilization rate of mobile devices for various purposes makes clear the need to track wireless networks to ensure the integrity and confidentiality of the information transmitted. Therefore, it is necessary to quickly and efficiently identify the normal and abnormal traffic of such networks, so that administrators can take action. This work aims to analyze classification techniques in relation to data from Wireless Networks, using some classes of anomalies pre-established according to some defined criteria of the MAC layer. For data analysis, WEKA Data mining software (Waikato Environment for Knowledge Analysis) is used. The classification algorithms present a success rate in the classification of viable data, being indicated in the use of intrusion detection systems for wireless networks.

KEYWORDS

Wireless Networks, Classification Techniques, Weka

1. INTRODUCTION

Over the past decade a great technological advance was seen, especially regarding mobile technologies and its infrastructure. The increase in the use of wireless local area networks and also the use of services from satellites, both in organizational and residential environments, is identified. This allows information to be created, transmitted and accessed faster and anywhere at any time by simply having access to the mobile network infrastructure. According to Anatel (Telecommunication National Agency), in January/2016 Brazil registered 257.248 million active lines in mobile telephony, with pre-paid accesses corresponding to 71.45% (183.80 million) of total accesses, while post paid accesses correspond to 28.55% (73.45 million).

The consequence of this scenario is perceived when the use of computational devices used by both individuals and companies are verified. This scenario can be verified through the research conducted by IDC Brasil, which states that in the last quarter of 2014 Brazil had 1,637 million computers, of which 600 thousand are desktops and 1,037 million are notebooks. An unpublished survey by the Brazilian Institute of Geography and Statistics (IBGE) reveals that 57.3% of homes access the internet through cell phones and tablets in 2013.

People are getting used to technologies such as smart phones and tablets with Internet access. Most of these devices are equipped with capabilities based on the IEEE 802.11 standard. Using these wireless networks, users are often able to gain access to the Internet much cheaper than using cellular networks.

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 51-61, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90905

Currently these mobile devices basically act as a small computer, being possible to perform all actions, among others commonly performed on a Personal Computer. Some of these actions are: sending of E-mail to any computational device; use of an operating system; video viewing; execution of Web Systems; content servers; financial transactions; online shopping.

These mobile devices are also part of Wireless Networks as well as wireless actuators offering communication technologies for automation tools built into the Internet of Things in various environments [23].

The high rate of use of mobile devices for various purposes explains the importance of monitoring this infrastructure, since it presents the large-scale transmission of information, which at certain times may be restricted. To the set of this mobile system, determined by both the software and the hardware used, it is relatively fragile with regard to security, mainly due to the characteristic of its transmission medium, but also by the dynamism of access to this system. So there is a need to try to identify the normal and abnormal traffic of these wireless networks so that their administrators can take action.

With increased interconnection between networks, structured and wireless, information security has become a challenge. Networks are subject to various types of attacks that may have internal or external sources, some with the goal of paralyzing services, others with the intention of stealing information and in other cases, just for the amusement of the attackers. In addition, until recently, the networks were restricted to computers, now accept various types of equipment: sensors, smart phones, cell phones, among others. Therefore, security enhancement proposals should consider the technological evolution that is taking place.

The Wireless Networks environment, as well as the environment of Ad Hoc Wireless Networks or Wireless Sensor Networks, has in its characteristic a dynamicity in relation to the composition of the network members, that is, for these types of networks users often enter and leave the network. This feature makes it necessary to manage these environments quickly. This scenario becomes, however, quite vulnerable to attempts to approach the anomalies present in the system as a whole. Anomalies such as *EAPOL Start, Beacon Flood, Deauthentication, RTS Flood* [1][2]. However, the techniques and tools adopted by network managers in the framework of structured computer networks do not always meet these needs in a timely manner. In this sense, the use of intelligent algorithms for classification becomes a great option to minimize these difficulties, in order to identify anomalies more effectively.

The high rate of use of mobile devices for various purposes makes clear the need to monitor this infrastructure, since it presents the large-scale transmission of information, which at certain moments may be confidential. The set of this mobile system, determined by both the software and the hardware used, is relatively fragile regarding security, mainly due to the characteristic of its transmission mean, but also due to dynamic access it. So, there is a need to try to quickly and effectively identify the normal and abnormal traffic of these wireless networks so that administrators can take action. This work aims, from a database of wireless networks [1], to evaluate the classification of these data for some classification techniques. The data is formed by MAC layer information, which will be shown later.

The structure of this article is organized into sections. In section two will be presented some works that have the characteristic of identification of wireless networks traffic using algorithms of learning. In section 3, the theoretical basis for Wireless Networks is presented, while section 4 deals with Classification Techniques. Section 5 will present the methodology of experimentation and results. In Section 6 we present the case studies used to analyze the results. In section 7 will

be performed the quantitative and qualitative analysis of the results. Section 8 presents the conclusion of the work and future work.

2. RELATED WORKS

The large increase in the use of mobile computing resources both in public environments, both in private environment has aroused the great use of Ad Hoc Wireless Networks, mainly due to the ease of deployment of these networks. This, in turn, favors the large-scale development of malicious applications in Wireless Networks. It can be said that the number of attacks on Computer Networks, with wireless and structured architecture, has grown in recent years, with the incidents reported in the Brazil exceed 700,000, according to the Center for Studies and Responses to Security Incidents in Brazil [19]. Thus, there is a need to provide resources capable of guaranteeing the minimum authenticity of the services provided by the Computer Networks.
Intrusion Detection Systems are tools that contribute to guarantee the security in the Computer Networks, and its implementation is based on the policy of security of the environment with the objective of keeping active the services made available by the Computer Networks.

In addition, it is necessary to take into account the characteristics of the Ad Hoc Wireless Networks, which make it difficult to monitor the services and components of the Network, since they are constituted by autonomous nodes with mobility and without centralized management. Ad Hoc Wireless Networks rely on direct peer-to-peer communication, which is established without the need for centralized infrastructure. The Ad Hoc Networks are composed of devices that have the cooperative characteristic, being able to establish a direct communication with the devices that are within their reach. In this network there is centralized administration and each device can have the functionalities of station and router. The communication between the stations is called storage-forwarding, that is, the station that wishes to forward a message accesses the transmission medium and forwards the information to the neighboring station, which stores the information until the optimal time to forward the station other than the destination station. In this way, the formation of a multi-hop link between the information source and the destination of the information is identified, making network services such as routing and access control to the medium performed in a distributed way by all the components belonging to Ad Hoc Wireless Network [20].

There are several proposals of Intrusion Detection System in Wireless Networks [2, 5, 7, 21, 22] where the main obstacle is the durability of the energy of the computational resource, being frequently used in these technical proposals of computational intelligence capable of analyzing, learning and identifying anomalies. These proposals are based on the use of classification techniques, either in a single or joint approach, aiming increasingly to better use the mobile computing resource. The result of the use of classification techniques has contributed with the Computer Networks analysts in the choice of security policies with the purpose of nullifying or minimizing the damages caused by the anomalies in Wireless Networks environments.

It is possible to find in the literature some works of Wireless Networks traffic classification, which can be applied in Intrusion Detection Systems. These proposals make use of supervised and unsupervised learning methods. The proposal [2] provides a general approach to the various classification methods, using high-dimensional data and a variable selection technique aiming to reduce computational time and improving the learning rate.

Govindarajan presents a proposal [3] of two classification methods involving multilayer perceptron and Basis function Networks. This work proposes a hybrid architecture involving both classifiers for intrusion detection systems. Ed Wilson presents a proposal [4] of Hybrid Intrusion

Detection System, in which signal processing is performed using the Wavelet transform and then the classification of the anomalies using Artificial Neural Networks.

Ed Wilson[1] proposes the elaboration of a real database of Wireless Network traffic, which will be used in the evaluation of Intrusion Detection Systems (IDS). This data undergoes a pre-processing to later be classified by techniques of standards recognition, such as Artificial Neural Networks and following formatting rules that must be strictly followed.

The proposal [5] uses a combination of selection methods to classify Denial of Service anomalies in Computer Networks, showing the efficiency of the process selection process for DoS detection. Vo [6] applies supervised and unsupervised machine learning techniques to predict the time series trend by using the K-Means algorithm to group data with similarity and vector machine to train and test the data.

In [7] the most relevant models for the construction of Intrusion Detection Systems are presented, incorporating machine learning in the scenario of Ad Hoc Wireless Networks. Machine learning methods perform classification approach, association rule mining, Artificial Neural Networks and instance-based learning.

Work [21] also uses unsupervised and supervised classification methods to classify a collection of packet data from the Internet.

Gogoi presents the proposal [22] of a multi-level hybrid intrusion detection method that uses a combination of supervised, unsupervised and discrepant-based methods to improve the efficiency of detecting new and old attacks.

3. WIRELESS NETWORKS

The IEEE 802.11 standard defines a structure for the Wireless Local Area Network that covers the physical and link levels present in the reference OSI communication model. For the physical level only, radio frequency (RF) and infrared (IR) transmissions are treated, but other forms of wireless communication such as microwave and visible light can also be considered. For the link level, the access control to the medium is addressed through the definition of the MAC protocol (Medium access Control).

Taking into account the main characteristics of the IEEE 802.11 standard, such as interoperability, low cost, high market demand, reliability of project execution, there is a great growth in the use of Local Area Networks of Wireless Computers, also known as Wireless Networks, in public and private environments. This makes Wireless Networks a priority resource in environments where it is most often possible to access the Internet, whether inside corporations, in homes or in public environments, such as shopping malls, airports and so on [1].
The architecture of Wireless Networks according to the IEEE 802.11 standard is based on the division of the area covered by the Wireless Network into cells, these cells being called BSA (Basic Service Area). The size of the coverage of each BSA will depend exclusively on the characteristics of the environment itself and the power of transmitters and receivers used in the computational devices. The other components of the Wireless Networks architecture are listed below[1]:

I. BSS (*Basic Service Set*): Which is the set of computational devices that communicate by broadcasting (BC) or infrared (IR) within a Basic Service Area;

II. AP (*Access Point*): Specific computational devices, which have the purpose of capturing the transmissions made by computational devices belonging to its BSA (Basic Service Area) and are destined to stations belonging to another Basic Service Area. The Access Point, in turn, will perform the retransmission using a distribution system;
III. Distribution System: Communication infrastructure, which has the purpose of performing the interconnection of several Basic Service Area to allow the construction of networks, which have covers larger than one cell;

IV. ESA (*Extended Service Area*): Service Area that has the purpose of interconnecting several BSAs, through the Distribution System using the Access Point;

V. ESS (*Extended Service Set*): Which is intended to represent a set of computational devices consisting of the union of several BSSs (Basic Service Set) connected by a Distribution System.

The IEEE 802.11 standard also defines a medium access protocol, which is present in a MAC sublayer of the data link level. This protocol is called DFWMAC (*Distributed Foundation Wireless Medium Access Control*), which has two access methods, one of which is a distributed and mandatory feature. The other access method of the DFWMAC protocol is optional, having a centralized feature, and according to the IEEE standard, both the distributed method and the centralized method in the communication system can coexist. The medium access protocol also has the property of treating problems related to computational devices that try to move from one cell to another, a process called roaming. It is also related to the protocol of access to the medium of property to treat problems of lost computational devices, being able to be denominated of hidden node [1].

4. CLASSIFICATION TECHNIQUES

Classification is one of the Data Mining techniques that is mainly used to analyze a given dataset and takes each instance of it and assigns this instance to a particular class, thus granting a low error of classification. It is used to extract models that accurately define important data classes within the given dataset. Classification is a two-step process. During first step the model is created by applying classification algorithm on training data set then in second step the extracted model is tested against a predefined test dataset to measure the model trained performance and accuracy. So classification is the process to assign class label from dataset whose class label is unknown.

The dataset evaluation relied on the following classifiers: Bayesian networks, decision tables, Ibk, J48, MLP and NaiveBayes. The main criteria used were the popularity of such classifiers.
Bayesian networks have been used in many approaches to IDS, as in UMER (2017) [8]. These networks are directed acyclic graphics for representing a probability distribution on a set of random variables. Each vertex represents as random variable and each node represents a correlation among the variables [1] [9].

The decision table classifier works representing a set of conditions needed to determine the occurrence of a group of actions by means of a table format [10]. This technique has also been used in IDS approaches [1][11].

The IBk algorithm refers to a way of implementing the kNN (k-nearest neighbor) clustering method, which is used for classification and regression toward finding the closest neighbors of a

given instance. In the IBk, three neighbors, the ones closest to the search standard neighbors, are used. This is a relatively simple technique that has been used in IDS approaches as well [1][12]. The J48 algorithm relies on decision tree classifications. By this technique, the classification of a new item depends on the prior creation of a decision tree which uses attributes obtained from the training data. By computing the information gain of each of these attributes, J48 can optimize classification mechanisms in IDS [1][13].

The MLP is an artificial neural network that maps input parameters to proper outputs. It consists of many layers of nodes in a directed graphic. Several IDS approaches have used MLP [1][14].

5. METHODOLOGY

This work aims to apply classification techniques to identify anomalies especially in wireless network traffic. As mentioned in the previous section, the techniques adopted for this work are: Bayesian Networks, Decision Tables, Ibk, J48, MLP and NaiveBayes.

In order to achieve the proposed aims, the following activities were performed in accordance with the chronological order of execution.

We use a database with examples of specific anomalies in wireless networks. This base in turn is the final product of the work entitled *A Methodology for building a Dataset to Assess Intrusion Detection Systems in Wireless Networks* [1].

The next step is to perform a pre-processing in the database so that two new databases are obtained. One of the databases is composed of only 10% of the data from the original database and is destined for the test step in the selected algorithms. The other database is composed of 90% of the data from the original database and is destined for the training step of the selected algorithms. Both databases are stored in the Database Manager System named PostgreSQL, and are accessed by the Weka software (*Waikato Environment for Knowledge Analysis*)[15].

Finally, the results of each selected algorithm are analyzed and formatted through tables. In relation to the results, the following information is presented for analysis: Percentage of Classification, relation of correctness and errors.

6. CASE STUDY

The case study chosen to analyze the results of the application of classification techniques presented in previous sections uses data from real wireless networks [1] and the data mining software, Weka [15].

6.1. DATABASE

The database defined for the execution of this case study is a real collection of network traffic captured in the Wireless architecture. This data, in turn, is obtained by the behavior of users to access different information as well as for the use of the Internet. According to the authors [1], the network traffic obtained by students and employees of the institution in which the experiment was performed was used for this database.

The database chosen for the experimentation of this work made use of two different scenarios. The scenarios discussed have their own configuration and topologies, being a scenario of home

environment typical of wireless networks, while the other is a more complex environment, being a corporate environment.

This database is composed of a total of 616,047 records, each record being composed of 16 variables that are characteristics of the wireless network traffic itself. Also in each record of the database is defined a last variable the class to which belongs certain registry, classification is realized taking into account the values of the sixteen variables referring to the obtained wireless network traffic. In this way the data are classified in:

- *Normal*: Acceptable wireless network traffic;
- *EAPOLStart*: Traffic using the Extensible Authentication Protocol (EAP), which aims to perform an authentication method in both the Wired Equivalent Providence (WEP) protocol, both Wi-Fi Protected Access (WPA) protocol, commercial versions for wireless network access;
- *Beacon Flood*: Management type requests, which are intended to transmit millions of invalid Beacons, resulting in the difficulty that a certain Wireless network device will have in identifying a legitimate Access Point [16];
- *Deauthentication*: It also represents management-type requests, which are injected from the Wireless Network. The frames belonging to this anomaly are transmitted as fictitious requests, which requests the deactivation of a device that is authorized in the Wireless Network;
- *RTSFlood*: Also called Request-to-Send Flood is a control-type frame. This anomaly is based on the large-scale transmission of RTS frames or frames for a short period of time [16].

The database for the experimentation process of this work is divided into two distinct bases, in order to meet the requirements of each defined intelligent algorithm. In this way a training database is generated respecting the characteristics of each algorithm, being composed by 554,442 registers, which corresponds to 90% of the complete database. Also, the test database is generated, being composed by 61,604 records that correspond to 10% of the complete database, respecting the characteristic of each algorithm. In order to optimize the experimentation process and to provide better data manipulation, the training and test databases for each defined computational intelligence technique are stored in the PostgreSQL Database Management System.

6.2. DATASET EVALUATION

The data coming from Wireless Network are evaluated through the classification techniques mentioned in the previous section. To evaluate each of the classification techniques, the error parameters, the percentage of classification and the Kappa coefficient are used, which will be explained later.

The Mean Absolute Error (MAE) is defined as the average of the difference between and computed and measured results. The closer to zero the better the classification is. On the other hand, the Root Mean Square Error (RMSE) is computed as the average of the error square root. A minimum MAE does not imply necessarily in a minimal variation. Thus, it is more effective to use both MAE and RMSE in the evaluations [17].

The MAE and RMSE parameters are a simple way of measuring the effectiveness and efficiency of the classification techniques used, thus they are incentive of more advanced techniques.
The Kappa coefficient, in turn, is initially used by observers in the field of psychology as a measure of agreement-induced [18]. This metric shows the degree of acceptance or agreement among a group of judges. Equation 1 shows the agreement of the Kappa coefficient, with the observed agreement *Po* and the coincidence by chance *Pa*.

$$k = \frac{Po - Pa}{1 - Pa} \quad (1)$$

The result of $k = 1$ means that the classification was correct, while $k = 0$ indicates that the classification is entirely by chance. However, the best classifiers are those in which the value of k is close to one.

As previously shown, the classification techniques to be evaluated for the Wireless Networks database are: Bayesian networks, decision tables, Ibk, J48, MLP and NaiveBayes.

6.3. RESULTS AND DISCUSSION

The evaluation of the classifiers is performed using the Weka [15] tool, using the set of data obtained from Wireless Network [1] in which they are classified with the following anomalies: EAPOLStart, Beacon Flood, Deauthentication and RTSFlood. This database is composed of 17 variables per record, 16 MAC layer attributes and an identification attribute of the class to which a particular record belongs.

Experimentation with the chosen classification techniques makes use of 90% of training data and 10% of data for testing. The results of the mean and quadratic errors for the same, during the training are shown in Figure 1. These are relatively small, and it can be deduced that the classifiers have good performance for the data set of Wireless Networks.

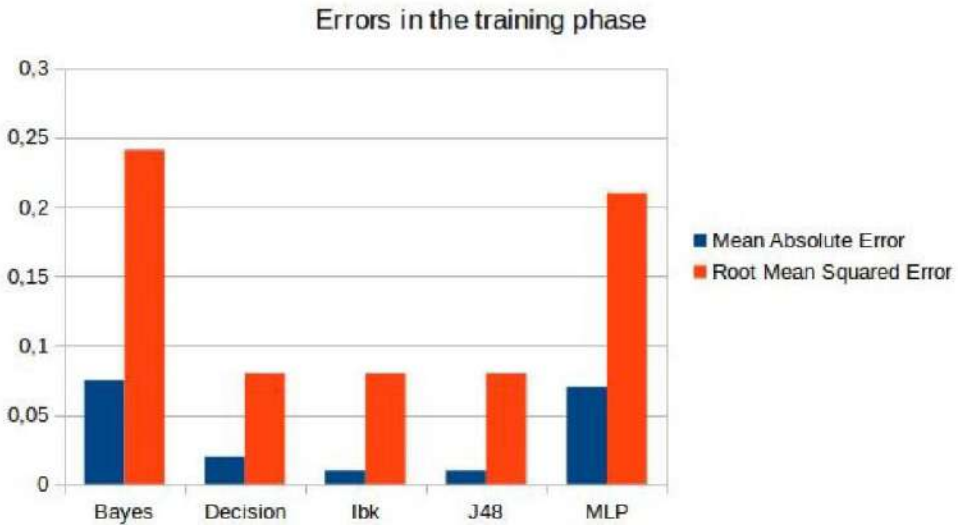


Figure 1. Errors in the training phase

Table 1 presents the simulation results, after the training of the classification techniques in relation to the Wireless Network data. The values obtained in percentage of correctly classified instances are relevant, being superior to some found in literacy. It should be considered that the proposal is to evaluate the performance of the classification techniques for the application of Wireless Networks data, without customizing them.

Table 1.Results for the testing phase of the data set

Classification Techniques	**Correctly Classified Instances (%)**	**Incorrectly Classified Instances (%)**	**Kappa Coefficient**
Bayes Network	76	24	0,42
Decision Tree	98	2	0,91
Ibk	98	2	0,91
J48	98	2	0,91
MLP	75	25	0,4

The evaluation of the data set represents an important research phase in the area of Wireless Networks, as it allows verifying the adequate response of the classification techniques commonly used in Intrusion Detection Systems proposals.

The use of the classification techniques adopted showed good results. The average errors, as shown in Figure 1 are relatively low. It is observed that the absolute mean error as well as the mean square error followed the same trend, proving the actual behavior of the data of Wireless Networks.

Table 1 shows that there is no difference for similar classification algorithms such as Bayes Network and MLP, in which it obtained a rating of 75%, while the other classification algorithms reached 98% of classification with low average errors. Therefore, it is possible to affirm that the use of classification techniques are effective for Wireless Network environments and can be used in Detection and Anomaly Classification Systems for Wireless Networks. It is also noticed that the selection of variables is fundamental for the classification to reach satisfactory levels and optimize the processing of these algorithms.

7. CONCLUSIONS AND FUTURE WORK

The results show that the data used to evaluate the classification techniques are viable and can be components in the evaluation of Intrusion Detection Systems in Wireless Networks. However, despite being preformatted with labels, where each record is identified as normal or with some of the predefined anomalies, it becomes valuable because it is collected directly from a Wireless Network.

The errors found in the training phase of the classification algorithms are low, being below 0.25, confirming that the selected classification techniques are adequate and that the data collected from Ad Hoc Wireless Networks are efficient for the analysis of the same ones.

The Kappa Coefficient results follow the same characteristics of the errors in the training phase of the classification algorithms in relation to the correct and incorrectly classified data, thus confirming their integrity.

Future work can be done in several ways: applying these classification techniques to a wireless network, online detection and classification on the network, and comparing with other existing approaches.

REFERENCES

[1] E. W. T. Ferreira, et al., (2015) "A methodology for building a dataset to assess intrusion detection systems in wireless networks," WSEAS Transactions on Communications, vol.14, pp.113–120, 2015.

[2] G. C. F. Sahin, (2014) "A survey on feature selection methods," Computers Electrical Engineering, 2014, pp. 16–28.

[3] M. Govindarajan & R. M. Chandrasekaran, "Intrusion detection using neural based hybrid classification methods," Computer Networks vol. 55, no. 8, pp. 1662–1671, 2011.

[4] E. W. T. Ferreira, et al., (2011) "Intrusion detection system with wavelet and neural artifical network approach for networks computers," IEEE Latin America Transactions, vol. 9, no.5, pp.832–837, 2011.

[5] S. Bhattacharya & S. Selvakumar, (2016) "Multi-measure multi-weight ranking approach for the identification of the network features for the detection of dos and probe attacks," The Computer Journal, vol. 59, no. 6, pp. 923–943, 2016. [Online]. Available:<http://dx.doi.org/10.1093/comjnl/bxv078>

[6] V. Vo & J. Luo & B. Vo, (2016) "Time series trend analysis based on k-means and support vector machine," Computing and Informatics, vol. 35, p. 11–127, 2016. [Online]. Available: <https://pdfs.semanticscholar.org/fd6d/6d3778f52608f048aa95dd9aaca42fe2871f.pdf>

[7] L. Nishani & M. Biba, "Machine learning for intrusion detection in manet: a state-of-the-art survey," Journal of Intelligent Information Systems, vol. 46, no. 2, pp. 391–407, 2016.

[8] UMER, Muhammad Fahad & SHER, Muhammad & BI, Yaxin. (2017) "Flow-based intrusion detection: Techniques and challenges". Computers & Security, v. 70, p. 238-254, 2017.

[9] N. Friedman & D. Geiger & M. Goldszmidt,(1997) "Bayesian network classifiers," Mach.Learn., vol. 29, no. 2–3, pp. 131–163, 1997.

[10] Wei, W. & Wang, J. & Liang, J. & Mi, X. & Dang, C. (2015). Compacted decision tables based attribute reduction. Knowledge-Based Systems, 86, 261-277.

[11] Rajmahanty, P. H., & Ganapathy, S. (2017). Role of Decision Trees in Intrusion Detection Systems: A Survey. International Journal of Advances in Computer and Electronics Engineering, 2(4), 09-13.

[12] Modi, M. U., & Jain, A. (2015). A survey of IDS classification using KDD CUP 99 dataset in WEKA. Int. J. Sci. Eng. Res, 6(11), 947-954.

[13] Aljawarneh, S., Yassein, M. B., & Aljundi, M. (2017). An enhanced J48 classification algorithm for the anomaly intrusion detection systems. Cluster Computing, 1-17.

[14] S. Haykin, Neural Networks and Learning Machines, 3nd.Ontario Canada: Pearson, 2009.

[15] Modi, M. U., & Jain, A. (2015). A survey of IDS classification using KDD CUP 99 dataset in WEKA. Int. J. Sci. Eng. Res, 6(11), 947-954.

[16] R. F. de Moraes & N. V. D. S. A. C. Maciel, "Avaliação de um conjunto de dados quanto á sua qualidade na especificação de perfis de ataque e não-ataque numa rede IEEE 802.11w," Anais da VI

Escola Regional de Informática da Sociedade Brasileira da Computação(SBC) - Regional de Mato Grosso, 2015, pp. 145–1508.

[17] Terziyska, M. & Todorov, Y. & Dobreva, M. (2018). Efficient Error Based Metrics for Fuzzy-Neural Network Performance Evaluation. In Advanced Computing in Industrial Mathematics (pp. 185-201). Springer, Cham.

[18] J. Cohen, "A Coefficient of Agreement for Nominal Scales," Educ. Psychol. Meas., vol. 20, no.1, pp. 37–46, Apr. 1960.

[19] CERT-BR, "Estatísticas dos incidentes reportados ao cert.br,"<https://www.cert.br/stats/incidentes/>, accessed: 2018-06-01.

[20] J. Loo, J. L. Mauri, and J. H. Ortiz, Mobile ad hoc networks: current status and future trends.Press, 2016.

[21] A. Vlăduţu, D. Comăneci, and C. Dobre, "Internet traffic classification based on flows' statistical properties with machine learning," International Journal of Network Management, vol. 27, no. 3,p.1929, 2017.

[22] P. Gogoi, D. Bhattacharyya, B. Borah, and J. K. Kalita, "Mlh-ids: A multi-level hybrid intrusion detection method," The Computer Journal, vol. 57, no. 4, pp. 602–623, 2014. [Online].Available: <http://dx.doi.org/10.1093/comjnl/bxt044>

[23] M. Sha, D. Gunatilaka, C. Wu, and C. Lu, "Empirical study and enhancements of industrial wireless sensor–actuator network protocols," IEEE Internet of Things Journal, vol. 4, no. 3, pp. 696–704, 2017.

AUTHORS

Daniel R. Canêdo has a degree in Computer Engineering from Pontifícia Universidade Católica de Goiás (2003) and a Master's degree in Electrical Engineering from the University of Brasília (2006). He is currently an exclusive professor at Federal Institute of Goiás - Campus Luziânia. He is currently a PhD student in the Post-Graduate Program in Electronic Systems and Automation Engineering of the Department of Electrical Engineering of the University of Brasília (UnB).

Alexandre R. Romariz holds a BS in Electrical Engineering from the University of Brasília (1992), a Master's degree in Electrical Engineering from the State University of Campinas (1995) and a PhD in Electrical Engineering from the University of Colorado at Boulder (2003). He is currently "Professor Associado" at University of Brasilia. He has experience in Computational Intelligence, Integrated Circuits, Optoelectronics and Digital Signal Processing.

INTENTIONAL BLANK

A SURVEY OF STATE-OF-THE-ART GAN-BASED APPROACHES TO IMAGE SYNTHESIS

Shirin Nasr Esfahani[1]and Shahram Latifi[2]

[1]Department of Computer Science, UNLV, Las Vegas, USA
[2]Department of Electrical & Computer Eng., UNLV, Las Vegas, USA

ABSTRACT

In the past few years, Generative Adversarial Networks (GANs) have received immense attention by researchers in a variety of application domains. This new field of deep learning has been growing rapidly and has provided a way to learn deep representations without extensive use of annotated training data. Their achievements may be used in a variety of applications, including speech synthesis, image and video generation, semantic image editing, and style transfer. Image synthesis is an important component of expert systems and it attracted much attention since the introduction of GANs. However, GANs are known to be difficult to train especially when they try to generate high resolution images. This paper gives a thorough overview of the state-of-the-art GANs-based approaches in four applicable areas of image generation including Text-to-Image-Synthesis, Image-to-Image-Translation, Face Aging, and 3D Image Synthesis. Experimental results show state-of-the-art performance using GANs compared to traditional approaches in the fields of image processing and machine vision.

KEYWORDS

Conditional generative adversarial networks (cGANs), image synthesis, image-to-image translation, text-to-image synthesis, 3D GANs.

1. INTRODUCTION

The task of image synthesis is central in many fields like image processing, graphics, and machine learning. This is done by computing the correct color value for each pixel in an image with desired resolution. Although various approaches have been proposed, image synthesis remains a challenging problem. Generative Adversarial Networks (GANs), one of the most interesting ideas in recent years, have made a breakthrough in Machine Learning applications. Due to the power of the competitive training manner as well as deep networks, GANs are capable of producing realistic images, and have shown great advances in many image generations and editing models.

Generative adversarial networks (GANs) were proposed by I. Goodfellow et al. (2014) [1] is a novel way to train a generative model. GANs are an advanced method for both semi-supervised and unsupervised learning. They consist of two adversarial models: a generative model *G* that captures the data distribution, and a discriminative model *D* that estimates the probability that a sample came from the training data rather than *G*. The only way *G* learns is through interaction with *D* (*G* has no direct access to real images). In contrast, *D* has access to both the synthetic samples and real samples. Unlike FVBNs (Fully Visible Belief Networks) [2] and VAE (Variational Autoencoder) [3], they do not explicitly model the probability distribution that generates the training data. In fact, *G* maps a noise vector *z* in the latent space to an image and *D*

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 63-76, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90906

is defined as classifying an input as a real image (close to 1) or as a fake image (close to 0). The loss function is defined as:

$$\min_{G} \max_{D} E_{x \in X} [\log D(x)] + E_{x \in X} \left[\log\left(1 - D\left(G(z)\right)\right)\right] \quad (1)$$

Images generated by GANs are usually less blurred and more realistic than ones produced with other previous generative models. In an unconditioned generative model, there is no control on modes of the data being generated. Conditioning the model on additional information will direct the data generation process. This makes it possible to engage the learned generative model in different "modes" by providing it with different contextual information. Conditional Generative Adversarial Networks (cGANs) was introduced by M. Mirza and S. Osindero [4]. In cGANs, both *G* and *D* are conditioning on some extra information (*c*) that can be class labels, text or sketches. Providing additional controls on the type of data being generated, makes cGANs popular for almost all image generating applications. The structure of GANs and cGANs are illustrated as Figure 1.

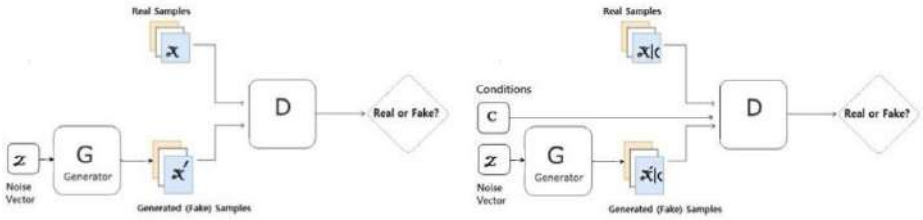


Figure 1. Structure of GANs (left) and cGANs (right)

In this survey, we discuss the ideas, contributions and drawbacks of state-of-the art models in four fields of image synthesis by using GANs. So, it is not intended to be a comprehensive review of all image generation fields of GANs; many excellent papers are not described here, simply because they were not relevant to our chosen subjects. This survey is structured as follows: Sections2 and 3 provide state-of-the-art GAN-based techniques in text-to-image and image-to-image translation fields, respectively, then section 4 is related to Face Aging. Finally, Section 5 is relevant materials to 3D generative adversarial networks (3GANs).

2. TEXT-TO-IMAGE SYNTHESIS

Synthesizing high-quality images from text descriptions, is one of the exciting and challenging problems in Computer Vision which has many applications, including photo editing and computer-aided content creation. The task of text to image generation usually means translating text in the form of single-sentence descriptions directly into prediction of image pixels. This can be done by different approaches.

One of difficult problems is the distribution of images conditioned on a text description is highly multimodal. In other words, there are many plausible configurations of pixels that correctly illustrate the description. For example, more than one suitable image would be found with "this small bird has a short, pointy orange beak and white belly" in a bird dataset. S. Reed et al. [5] were the first to propose a CGAN-based model (GAN-CLS), which successfully generated realistic images (64 × 64) for birds and flowers that are described by natural language descriptions. By conditioning both generator and discriminator on side information (also used before by Mirza et al. [4]), they were able to naturally model multimodal issue since the discriminator plays as a "smart" adaptive loss function. Their approach was to train a deep

convolutional generative adversarial network (DCGAN) conditioned on text features encoded by a hybrid character-level convolutional recurrent neural network. The network architecture follows the guidelines of DCGAN [6]. Both the generator *G* and the discriminator *D* performed feed-forward inference conditioned on the text feature. The architecture can be seen in Figure 2.

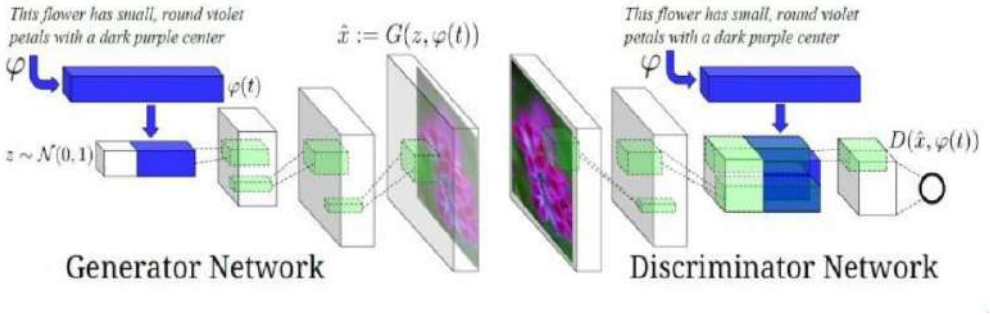


Figure 2. DCGANs architecture: Text encoding φ(t) is used by both *G* and *D*. It is projected to a lower-dimension and depth concatenated with image feature maps for further stages of convolutional processing [5]

They improved their model to generate 128 × 128 images by utilizing the locations of the content to draw (GAWWN) [7]. Their methods are not directly suitable for cross-media retrieval, but their ideas and models are valuable because they use *ten* single-sentence descriptions for each bird image. In addition, each image marked the bird location with a bounding box, or key point's coordinates for each bird's parts as well as an extra bit used in each part to show whether or not the part can be visible in the each. Both *G* and *D* are conditioned on the bounding box and the text vector (represents text description). The model has two branches for *G*: a global stage that apply on full image and local stage which only operates on the inside of bounding box. Several new approaches have been developed based on GAN-CLS. In a similar way, S. Zhu et al. [8] presented a novel approach for generating new clothing on a wearer based on textual descriptions. S. Sharma et al. [9] improved the inception scores of synthesis images with several objects by adding a dialogue describing the scene (ChatPainter). However, a large text input is not desirable for users. Z. Zhang et al.'s model [10](HDGAN) was a multi-purpose adversarial loss for generating more effective images. Furthermore, they defined a new visual-semantic similarity measure to evaluate the semantic consistency of output images. M. Cha et al. [11] extended the model by improving perceptual quality of generated images. H. Dong at al. [12] defined a new condition (the given images) in the image generation process to reduce the searching space of synthesized images. H. Zhang et al. [13] followed Reed's [5] approach to decompose the challenging problem of generating realistic high-resolution images into more manageable sub-problems by proposing StackGAN-v1 and StackGAN-v2. S. Hong [14] designed a model to generate complicated images which preserve semantic details and highly relevant to the text expression by generating a semantic layout of the objects in the image and then conditioning on the map and the caption. Y. Li et al. [15]did similar work to generate video from text. J. Chen et al. [16] designed a Language-Based Image Editing (LBIE) system to create an output image automatically by editing the input image based on the language instructions that users provide. Another text-to-image generation model (TAC-GAN) was proposed by A. Dash et al. [17]. It is designed based on Auxiliary Classifier GAN[18] but uses a text description condition instead of a class label condition. Comparisons between different text-to-image GAN-based models are given in Table 1.

Although, the application of Conditional GAN is very promising in generating realistic nature images, training GAN to synthesize high-resolution images using descriptors is a very difficult task. S. Reed et al. [5] succeeded to generate reasonable 64 × 64 images which didn't have much

details. Later, [7] they were able to synthesize higher resolution (128 × 128) only with additional annotations of objects. Additionally, the training of their CGANs was unstable and highly related to the choices of hyper-parameters [19]. T. Xu et al. [20] proposed an attention-driven model (AttnGAN) to improve fine-grained detail. It uses a word-level visual-semantic that fundamentally relies on a sentence vector to generate images.

TABLE 1. Different text-to image models.

Model	Input	Output	Characteristics	Resolution
GAN-INT-CLS [5]	text	image	---------	64 × 64
GAWWM [7]	text + location	image	location-controllable	128 × 128
StackGAN [13]	text	image	high quality	256 × 256
TAC-GAN [17]	text	image	diversity	128 × 128
ChatPainter [9]	text + dialogue	image	high inception score	256 × 256
HDGAN [10]	text	image	high quality and resolution	512 × 512
AttnGAN [20]	text	image	high quality and the highest inception score	256 × 256
Hong et al. [14]	text	image	Second highest inception score and complicated images	128 × 128

T. Salimans et al. [21] defined Inception Scores as a metric for automatically evaluating the quality of image generative models. This metric was shown to correlate well with human judgment of image quality. In fact, inception score tries to formalize the concept of realism for a generated set of images. The inception scores of generated images on the MS COCO data set for some different models is provided in Table 2. [9]

TABLE 2. Inception scores of different models.

Model	Inception Score
GAN-INT-CLS [5]	7.88 ± 0.07
StackGAN [13]	8.45 ± 0.03
Hong et al. [14]	11.46 + 0.09
ChatPainter (non–current) [9]	9.43 ± 0.04
ChatPainter (recurrent) [9]	9.74 ± 0.02
AttnGAN [20]	25.89 ± 0.47

3. IMAGE-TO-IMAGE-TRANSLATION

Many visual techniques including in painting missing image regions (predicting missing parts in a damaged image in such a way that the improved region cannot be detected by observer), adding color to grayscale images and generate photorealistic images from sketches, involve translating one visual representation of an image into another. Application-specific algorithms are usually used to solve these problems with the same setting (map pixels to pixels). However, applying generative modeling to train the model is essential because some translating processes may have more than one correct output for each input image. Many researchers of image processing and computer graphic area have tried to design powerful translation models with supervised learning when they can have training image pairs (input, output), but producing paired images can be difficult and expensive. Moreover, these approaches are suffering from the fact that they usually formulated as per-pixel classification or regression which means that each output pixel is conditionally independent from all others in the input image.

P. Isola et al. [22] designed a general-purpose image-to-image-translation model using conditional adversarial networks. The new model (Pix2Pix), not only learned a mapping function, but also constructed a loss function to train this mapping. In particular, a high-resolution source grid is mapped to a high-resolution target grid. (The input and output differ in surface appearance, but both are renderings of the same underlying structure). In Pix2Pix model, *D*learns to classify between fake (synthesized by the generator) and real {input map, photo} tuples. *G* learns to fool *D*. *G* and *D* can access to the input map. (Figure. 3)

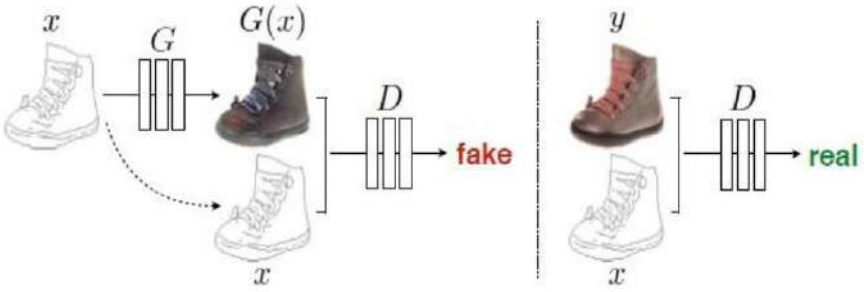


Figure 3. Training a cGANs to map edges to the photo. (Here, input map is map edges) [22]

The Pix2Pix model has some important advantages: (1) it is a general-purpose model which means it is a common framework for all automatic problems defining as the approach of translating one possible instance of an image into another(predicting pixels from pixels) by giving sufficient training data; and (2) instead of hand designing the loss function, the networks learn a loss function sensitive to data and task, to train the mapping. Finally (3), by using the fact that there is a lot of information sharing between input and output, Pix2Pix model takes advantages of them more directly by skipping connections between corresponding layers in the encoder following the general shape of a "U-Net" to create much higher quality results. The main drawback of Pix2Pix model is that it requires significant number of labeled image pairs, which is generally not available in domain adaptation problems. Later, they improved their method and designed a new model (CycleGAN) to overcome to this issue by translating an image from a source domain to a target domain in the absence of paired examples using combination of adversarial and cycle-consistent losses. [23]. A comparison against other baselines (CoGAN) [24], BiGAN [25]/ALI [26], SimGAN [9] and CycleGAN for mapping aerial photos can be seen in Figure 4. To measure the performance of photo↔ *l*abels, the standard metrics of the Cityscapes benchmark is used that includes per-pixel accuracy, per-class accuracy, and mean class Intersection-Over-Union (Class IOU) [27]. Comparison results are provided in Table 3 [10].

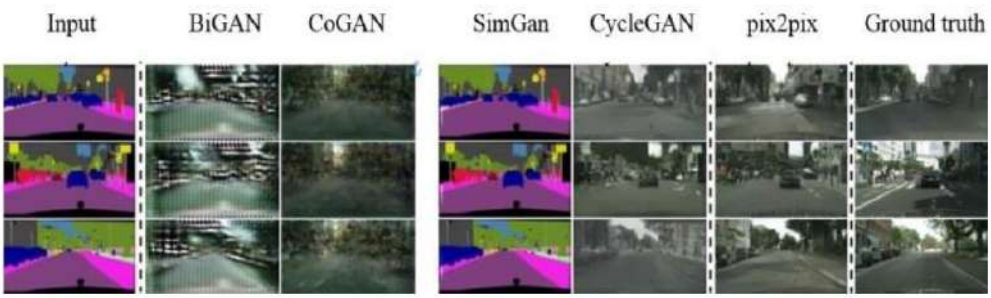


Figure 4. Different methods for mapping labels ↔ photo on Cityscapes images. From left to right: input, BiGAN/ALI, CoGAN, SimGAN, CycleGAN, Pix2Pix trained on paired data, and ground truth. [23]

TABLE 3. Classification performance for different models on images of the Cityscapes dataset.

Model	Per-pixel Accuracy	Per-class Accuracy	Class IOU
CoGAN [24]	0.45	image	0.08
BiGAN/ALI [25, 26]	0.41	image	0.07
SimGAN [9]	0.47	image	0.07
CycleGAN [23]	0.58	image	0.16
Pix2Pix [22]	0.85	image	0.32

Later, Q. Chen and V. Koltun [28] suggest that because of the training instability and optimization issues of CGANs, it is hard and prone to failure to generate images with high resolution. Instead, they used a direct regression objective based on a perceptual loss and produced the first model that can generate 2048 × 1024 images. However, their results often don't have fine details and realistic textures [29]. Following the Pixt2Pix model's architecture, Lample et al. [30] designed *Fader Networks*, with *G* and *D* competing in the latent space to generates realistic images of high resolution without needing to apply a GAN to the decoder output. Their model provided a new direction towards robust adversarial feature learning. D. Michelsanti and Z.-H Tan [31] used Pix2Pix to create a new framework for speech enhancement. Their model learned a mapping between noisy and clean speech spectrograms as well as to learn a loss function for training the mapping.

4. FACE AGING

Face aging, age synthesis or age progression (refers to future looks) and regression (refers to previous looks), are different names for a simple concept that is rendering of facial images with different ages with the same facial recognition features. It has many applications such as finding lost children and wanted person or entertainment. There have been two main traditional face aging methods: prototyping and modeling [32]. Prototyping methods transform an input face image into target age group by computing the average faces within age groups and using them as the aging patterns. They are simple and fast, but mostly unable to create realistic face images. On the other hand, molding techniques simulate the age effects on muscles and skin by employing parametric models. Both need to have variant images of a same person in different ages that is a very difficult and nearly impossible task. The first GAN–based architecture for automatic face aging (Age-cGAN) was introduced by G. Antipov et al. [32] Since the introduction of GAN networks, many GAN- based methods have been proposed to do modifications on human faces (changing the hair's colour, adding sunglasses, designing younger or older faces). These methods' results are more plausible and realistic than previous ones, but most of their generating results suffer from the fact that original person's identity is lost in the modified image. The Age-cGAN had the ability to preserve the identity information. Moreover, the model was able to generate high quality and incredibly realistic results. Age-cGAN is consisted of cGANs networks combined with an encoder. After training cGAN networks, mapping an input face image to a latent vector is done by the encoder, then generator maps the latent vector conditioned on age number to produce new face image. (An optimal latent vector is approximated by using an input image and a specific age). Finally, a reconstructed face image is generated. In the next step, the resulting face image is generated by providing the age at the input of generator (Figure 5).

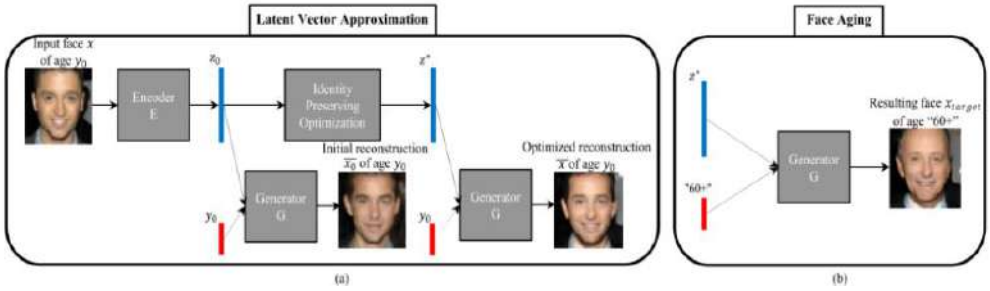


Figure 5. (a): Approximation of the latent vector to reconstruct the input image,
(b): Switching the age condition at the input of the generator to perform face aging [32]

Even with promising results that Age-cGAN provides, there are still some problems. In term of time efficiency because it must apply L-BFGS-B optimization algorithm [33] for each image, the performance is not reasonable [34]. Besides, the model cannot preserve the original identities in age's faces perfectly that makes it unsuitable for cross-age verification. Later, to improve the model, they proposed a Local Manifold Adaptation approach [35]. Combined with Age-cGAN model to design a new model Age-cGAN+LMA to boost the accuracy of cross-age face verification via age normalization. A comparison between two models is shown in Figure 6 and based on Face Verification (FV) score on the LFW dataset [36] measured with an open-source face verification software [37] in Table 4.

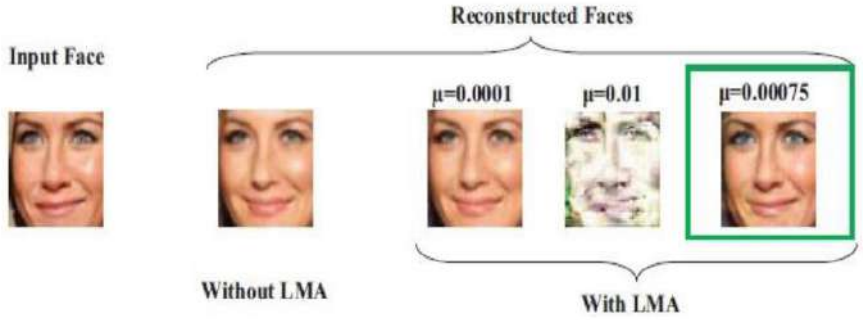


Figure 6. Face reconstruction with and without Local Manifold Adaptation (LMA)
For LMA-enhanced reconstructions, the impact of the learning rate μ is illustrated. [35]

TABLE 4. FV scores calculation on the LFW dataset by using open-face software [32].

Tested Pairs	FV Scores on LFW dataset
Original	89.4%
Age-cGAN [32]	82.0%
Age-cGAn + LMA [35]	88.7%

Another important age modeling approach was introduced by Z. Zhang et al. [38] by using a conditional adversarial auto-encoder (CAAE) .At first, the encoder mapped a face image to a vector *z* (personal features), then the output vector (the new latent vector) and a label *l* (new age) were concatenated to be used as an input of the generator to synthesis new face image. The success of their model is related to the availability of a large database with different ages, so for a small amount of training data, the model's performance is not reasonable. Age-cGAn and CAAE independently model the distribution of each age group, so they are unable to capture the transition patterns (the gradual shape and texture changes between adjacent age groups). S. Liu et al. proposed a novel Contextual Generative Adversarial Nets (C-GANs) to specifically take it into

consideration [39]. The C-GAN model is consisted of a conditional transformation network and two discriminative networks (an age discriminative network and a transition pattern discriminative network) which are collaboratively contributing to generates promising results. Another main problem of both Age-cGAN and CAAE is that they first map the face image into a latent vector and then project to the face manifold model conditioned on age, while the effect of conditioned on the generated face image is not always guaranteed. In other words, in the training step, the face images are constructed with the same age condition as the input, however in the testing step, face images are generated by combining an input face image with different age conditions that in the worst case, if the age doesn't have any effect on the synthesized face images, so it is impossible to generate face aging changing the age condition of the trained network. To solve this problem, J. Song et al. [40] designed, a dual conditional GANs (Dual cGANs) which had the ability that face aging and rejuvenation were trained from multiple sets of unlabelled face images with different ages. In this model, the cGAN transforms a face image to other ages based on the age condition, while the dual conditional GAN learns to invert the task.

Preserving the personal identity is done with definition of loss function that is the reconstruction error of images. On the other hand, the discriminators can learn the transition patterns (the shape and texture changes between different age groups) from generated images, so the final outputs are age-specific photo-realistic faces. Another GAN- based model with pyramid architecture is designed by H. Yang et al. [39]. Their model is benefited from most of the image generation ability of GAN, by using a multi-pathway discriminator to refine detailed aging process. This model has stronger ability to handling the identity performance and aging accuracy, comparing with previous models. Although aging is usually reflected in local facial parts (wrinkles and the eye corner), face aging models usually ignore them. To address this issues, P. Li et al. [42] proposed a Global and Local Consistent Age Generative Adversarial Network (GLCA-GAN) for age progression and regression. The generator is consisted of one global network and three local networks to learn the whole facial structure and imitate subtle changes of crucial facial subregions simultaneously. Instead of the learning the whole face, the generator uses the residual face to preserve most of the details and increases the speed of learning. Later, they extended their model to a Wavelet domain Global and Local Consistent Age Generative Adversarial Network (WaveletGLCA-GAN) [43] that one global specific network and three local specific networks are integrated together to capture both global topology information and local texture details of human faces. New model can generate higher-resolution age synthesis with more accuracy. WaveletGLCA-GAN's performance comparison with three of previous models is shown in Table 5. (Faces under 30 years old called $AG_0$are chosen as the input test images to synthesize faces in 31-40 years old (AG_1), 41-50 years old (AG_2) and 51-77 years old (AG_3), then the average age are calculated).

TABLE 5. The Age estimation results of different methods on CACD2000 (Cross- Age Celebrity Dataset) and Morph datasets [32].

	CACD2000			**Morph**		
Methods	**AG_1**	**AG_2**	**AG_3**	**AG_1**	**AG_2**	**AG_3**
CAAE [38]	31.32	34.94	36.91	28.13	32.50	36.83
Yang et.al [39]	44.29	48.34	52.02	42.84	50.78	59.91
GLCA-GAN [42]	37.09	44.92	48.03	43.00	49.03	54.60
WaveletGLCA-GAN [43]	37.56	48.13	54.17	38.36	46.90	59.14
Real Data	39.15	47.14	53.87	38.59	48.24	58.28

5. 3D IMAGE SYNTHESIS

3D object reconstruction of 2D images has always been a challenging task that try to define any object's 3D profile, as well as the 3D coordinate of every pixel. It is generally a scientific problem which has a wide variety of applications such as Computer Aided Geometric Design (CAGD), Computer Graphics, Computer Animation, Computer Vision, medical imaging etc. Researchers have done impressive works on 3D object synthesis, mostly based on meshes or skeletons. Using parts from objects in existing CAD model libraries, they have succeeded to generate new objects. Although the output objects look realistic, but they are not conceptually novel. J. Wu et al. [44] were the first that introduced 3D generative adversarial networks (3D GANs). Their state-of-the-art framework was proposed to model volumetric objects from a probabilistic domain (usually Gaussian or uniform distribution) by using recent progresses in volumetric convolutional networks and generative adversarial networks. They generated novel objects such as chairs, table and cars. Besides, they proposed a model which mapped 2D images to images having 3D versions of objects. 3DGAN is an all-convolutional neural network, showing in Figure 7.

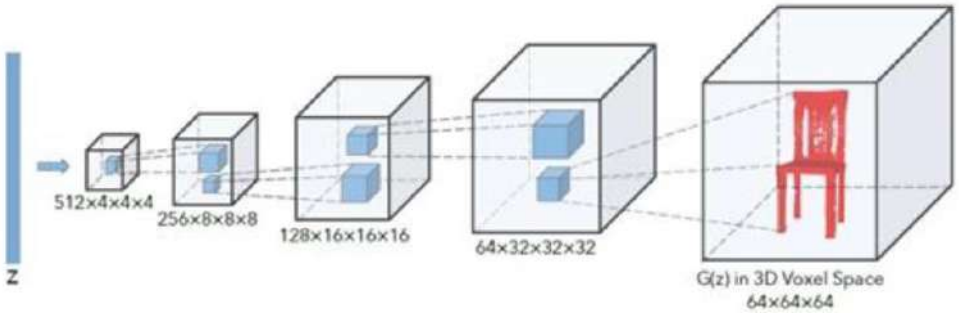


Figure 7. 3DGAN generator. The Discriminator mostly mirrors the generator

The *G* has five volumetric fully convolutional layers with kernel sizes of 4 × 4 × 4 and strides 2. Between the layers, batch normalization and ReLU layers have been added with a Sigmoid layer at the end. Instead of ReLU layers, The *D* uses Leaky ReLU while it is basically like the *G*. Neither pooling nor linear layers are used in the network. The 3DGAN model has some important achieving results comparing with previous 3D models: (1) It samples objects without using a reference image or CAD model; (2) It has provided a powerful 3D shape descriptor that can be learned without supervision that makes it widely applicable in many 3D object recognition algorithms; (3) Having comparable performance against recent surprised methods, and outperforms other unsupervised methods by a large margin; (4) They have the capability to apply for different purposes including 3D object classification and 3D object recognition. However, there are significant limitations in using 3DGANs: (1) Their using memory and the computational costs grow cubically as the voxel resolution increases which make them un usable in generating high resolution 3D image as well as in interactive 3D modelling (2) They are largely restricted to partial (single) view reconstruction and rendered images. There is a noticeable drop in performance when applied to natural (non-rendered) images. Later, they proposed a new 3D model called MarrNet by improving the previous model (3DGANs) [45]. They enhanced the model's performance by using 2.5D sketches for single image 3D shape reconstruction. Besides, in order to have consistency between 3D shape and 2.5D sketches, they defined differentiable loss functions, so MarrNet is an end-to-end fine-tuned on real images without annotations. At first, it returns objects from an RGB image to their normal, depth, and silhouette image, then from the 2.5D sketches, regresses the 3D shape. It also applies an encoding-decoding nets as well as

reprojection consistency loss function to ensure the estimated 3D shape aligns with the 2.5D sketches precisely. The whole architecture can be trained end-to-end. (Figure 8)

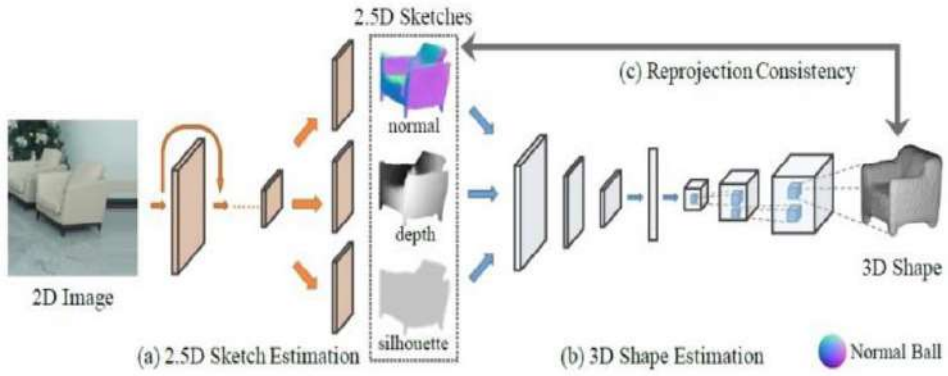


Figure 8. Components of MarrNet: (a) 2.5D sketch estimation, (b) 3D shape estimation, and (c) Loss function for reprojection consistency [45]

There are other 3D models that have been designed based on the 3DGAN architecture. Combining a 3D Encoder-Decoder GAN(3D-ED-GAN) with a Long term Recurrent Convolutional Network (LRCN), W. Wang et al. [46] proposed a hybrid framework. The model's purpose is in painting corrupted 3D objects and completing high-resolution 3D volumetric data. It gets significant advantage of completing complex 3D scene with higher resolution such as indoor area, since it is easily fit into GPU memory. E. J. Smith and D. Meger [47] improved 3DGAN and introduced a new model called 3D-IWGAN (Improved Wasserstein Generative Adversarial Network) to reconstruct 3D shape from 2D images and perform shape completion from occluded 2.5D range scans. Leaving the object of interest still and rotating the camera around it, they were able to extract partial 2.5D views, instead of enforcing it to be similar to a known distribution. P. Achlioptas et al. [48] explored AAE variant by using a specially-designed encoder network for learning a compressed representation of point clouds before training GAN on the latent space. However, their decoder is restricted to be MLP that generates m pre-defined and fixed number of points. On the other hand, the output of decoder is 3m (fixed)for 3D point clouds, while the output of the proposed G_x is only 3 dimensional and it can generate arbitrarily many points by sampling different random noise z as input. The new model (MarrNet) has the ability to jointly estimates intrinsic images and full 3D shape from a color image and generates reasonable results on standard datasets [49]. It has the ability to recover more details compared to 3D GAN (Figure 9). A comparison between different 3D models can be shown in Table 6.

Figure 9. 3D construction of chairs on IKEA dataset. From left to right: input, ground truth, 3D estimation by 3DGAN and two view of MarrNet. [45]

Table 6. Classification results on ModelNet dataset [46].

Model	ModelNet40	ModelNet10
3DGAN [44]	83.3%	91.0%
3D-ED-GAN [46]	87.3%	92.6%
VoxNet [50]	92.0%	83.0%
DeepPano [51]	88.66%	82.54%
VRN [52]	91.0%	93.6%

6. CONCLUSION

In this study, we presented an overview of state-of-art approaches in four common fields of GANs-based image generation including text-to-image synthesis, image-to-image translation, face aging and 3D image generation. We have reviewed pioneering models in each mentioned field with all advantages and disadvantages. Moreover, we have discussed some improved models which are designed based on predecessor model's architecture with their applications. Among mentioned fields, 3D image synthesis approaches face several limitations even despite the advancements. Face aging filed has been the most attractive area due to their promising results. While as text-to-image synthesis and image-to-image translation have been the fields with most different proposed models and still have potential for improvement and expansion improved.

REFERENCES

[1] Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., &Bengio, Y. (2014) "Generative adversarial nets" Advances in Neural InformationProcessing Systems 27 (NIPS 2014),Montreal, Canada.

[2] Frey, B. J. (1998) "Graphical models for machine learning and digital communication", MIT press.

[3] Doersch, C. (2016)"Tutorial on variational autoencoders", arXiv preprint arXiv:1606.05908,

[4] M. Mirza & S. Osindero (2014) "Conditional generative adversarial nets", arXiv:1411.1784v1.

[5] S. Reed, Z. Akata, X. Yan, L. Logeswaran, B. Schiele & H. Lee (2016) "Generative adversarial text to image synthesis", International Conference on Machine Learning, New York, USA, pp. 1060-1069.

[6] A. Radford, L. Metz & S. Chintala (2016) "Unsupervised representation learning with deep convolutional generative adversarial networks", 4th International Conference of Learning Representations (ICLR 2016), San Juan, Puerto Rico.

[7] S. Reed, Z. Akata, S. Mohan, S. Tenka, B. Schiele & H. Lee (2016) "Learning what and where to draw", Advances in Neural Information Processing Systems, pp. 217–225.

[8] S. Zhu, S. Fidler, R. Urtasun, D. Lin & C. L. Chen (2017) "Be your own prada: Fashion synthesis with structural coherence", International Conference on Computer Vision (ICCV 2017), Venice, Italy,pp. 1680-1688.

[9] S. Sharma, D. Suhubdy, V. Michalski, S. E. Kahou& Y. Bengio (2018) "ChatPainter: Improving text to image generation using dialogue", 6th International Conference on Learning Representations (ICLR 2018 Workshop), Vancouver, Canada.

[10] Z. Zhang, Y. Xie& L. Yang (2018) "Photographic text-to-image synthesis with a hierarchically-nested adversarial network", Conference on Computer Vision and PatternRecognition (CVPR 2018), Salt Lake City, USA,pp. 6199-6208.

[11] M. Cha, Y. Gwon& H. T. Kung (2017) "Adversarial nets with perceptual losses for text-to-image synthesis", International Workshop on Machine Learning for Signal Processing (MLSP 2017), Tokyo, Japan,pp. 1- 6.

[12] H. Dong, S. Yu, C. Wu & Y. Guo (2017) "Semantic image synthesis via adversarial learning", International Conference on Computer Vision (ICCV 2017), Venice, Italy,pp. 5706-5714.

[13] H. Zhang, T. Xu, H. Li, S. Zhang, X. Wang, X. Huang, and D. Metaxas (2017) "Stackgan: Text to photo-realistic image synthesis with stacked generative adversarial networks", International Conference on Computer Vision (ICCV 2017), Venice, Italy,pp. 5907-5915.

[14] S. Hong, D. Yang, J. Choi & H. Lee (2018) "Inferring semantic layout for hierarchical text-to-image synthesis", Conference on Computer Vision and PatternRecognition (CVPR 2018), Salt Lake City, USA,pp. 7986-7994.

[15] Y. Li, M. R. Min, Di. Shen, D. Carlson, and L. Carin (2018) "Video generation from text", 14th Artificial Intelligence and Interactive Digital Entertainment Conference (AIIDE 2018), Edmonton, Canada.

[16] J. Chen, Y. Shen, J. Gao, J. Liu & X. Liu (2017) "Language-based image editing with recurrent attentive models", The IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2018), Salt Lake City, USA, pp. 8721-8729.

[17] A. Dash, J. C. B. Gamboa, S. Ahmed, M. Liwicki& M. Z. Afzal (2017) "TAC-GAN-Text conditioned auxiliary classifier", arXiv preprint arXiv: 1703.06412, 2017.

[18] A. Odena, C. Olah& J. Shlens (2017) "Conditional image synthesis with auxiliary classifier GANs," Proceeding of 34th International Conference on Machine Learning (ICML 2017), Sydney, Australia.

[19] H. Zhang, I. Goodfellow, D. Metaxas & A. Odena (2018) "Self-attention, generative adversarial networks", arXiv preprint arXiv:1805.08318, 2018.

[20] T. Xu, P. Zhang, Q. Huang, H. Zhang, Z.Gan, X. Huang & X. He (2018) "AttnGAN: Fine-grained text to image generation with attentional generative adversarial networks", The IEEE Conference on Computer Vision and PatternRecognition (CVPR 2018), Salt Lake City, USA,pp. 1316-1324.

[21] T. Salimans, I. J. Goodfellow, W. Zaremba, V. Cheung, A. Radford & X. Chen (2016) "Improved techniques for training GANs", Advances in Neural Information Processing Systems 29 (NIPS 2016), Barcelona, Spain.

[22] P. Isola, J.-Y. Zhu, T. Park & A. A. Efros (2017) "Image-to-image translation with conditional adversarial networks",The IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2017), Honolulu, Hawai, USA, pp. 1125-1134.

[23] J.-Y. Zhu, T. Park, P. Isola & A. A. Efros (2017) "Unpaired Image-to-Image Translation using Cycle-Consistent", The IEEE International Conference on Computer Vision (ICCV2017), Venice, Italy, pp. 2223-2232.

[24] M.-Y. Liu & O. Tuzel (2016) "Coupled generative adversarial networks", 2016 Conference on Neural Information Processing Systems (NIPS 2016), Barcelona, Spain, pp. 469–477.

[25] J. Donahue, P. Kr¨ahenb¨uhl& T. Darrell (2016) "Adversarial feature learning", 4th International Conference on Learning Representations (ICLR 2016),San Juan, Puerto Rico.

[26] V. Dumoulin, I. Belghazi, B. Poole, A. Lamb, M. Arjovsky, O. Mastropietro& A. Courville (2017) "Adversarially learned inference", 5th International Conference on Learning Representations(ICLR 2017), Toulon, France.

[27] M. Cordts, M. Omran, S. Ramos, T. Rehfeld, M. Enzweiler, R. Benenson, U. Franke, S. Roth, & B. Schiele (2016) "The cityscapes dataset for semantic urban scene understanding", The IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2016), Las Vegas, USA, pp. 3213-3223.

[28] Q. Chen & V. Koltun (2017) "Photographic image synthesis with cascaded refinement networks",IEEE International Conference on Computer Vision (ICCV 2107), Venice, Italy, pp. 1520–1529.

[29] T.-C. Wang, M.-Y. Liu, J.-Y. Zhu, A. Tao, J. Kautz & B. Catanzaro (2018) "High-resolution image synthesis and semantic manipulation with conditional GANs", The IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2018), Salt Lake City, USA, pp. 8798-8807.

[30] G. Lample, N. Zeghidour, N. Usunier, A. Bordes, L. Denoyer& M. Ranzato (2017) "Fader networks: Manipulating images by sliding attributes", Advances in Neural Information Processing Systems 30 (NIPS 2017), Long Beach, USA.

[31] D. Michelsanti & Z.-H. Tan (2017) "Conditional generative adversarial networks for speech enhancement and noise-robust speaker verification", Proceeding of Interspeech, pp. 2008–2012.

[32] G. Antipov, M. Baccouche &J.-L. Dugelay(2017)"Face aging with conditional generative adversarial networks", IEEE International Conference on Image Processing (ICIP 2017), pp.2089 – 2093.

[33] R. H. Byrd, P. Lu, J. Nocedal& C. Zhu (1995) "A limited memory algorithm for bound constrained optimization", SIAM Journal on Scientific Computing, vol. 16, no. 5, pp. 1190–1208, 1995.

[34] Z. Wang, X. Tang, W. Luo & S. Gao (2018) "Face aging with identity preserved conditional generative adversarial networks", Proceeding IEEE Conference Computer Vision and Pattern Recognition, CVPR 2018), Salt Lake City, USA, pp. 7939–7947.

[35] G. Antipov, M. Baccouche& J.-L. Dugelay (2017)" Boosting cross-age face verification via generative age normalization", International Joint Conference on Biometrics (IJCB 2017), Denver, USA, pp. 17.

[36] E. L.-Miller, Gary B. Huang, A. R. Chowdhury, H. Li &G.Hua (2016) "Labeled Faces in the Wild: A Survey",Advances in Face Detection and Facial Image Analysis, Springer,2016, pp.189-248.

[37] B. Amos, B. Ludwiczuk, & M. Satyanarayanan. Openface (2016) "A general-purpose face recognition library with mobile applications", Technical report, CMU-CS-16-118, CMU School of Computer Science.

[38] Z. Zhang, Y. Song & H. Qi (2017) "Age progression/regression by conditional adversarial auto encoder", IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2017), Honolulu, USA, pp. 4352 – 4360.

[39] S. Liu, Y. Sun, D. Zhu, R. Bao, W. Wang, X. Shu & S. Yan (2017) "Face Aging with Contextual Generative Adversarial Nets", Proceedings of the 25th ACM international conference on Multimedia, Mountain View, USA, pp. 82 -90.

[40] J. Song, J. Zhang, L. Gao, X. Liu & H. T. Shen (2018) "Dual Conditional GANs for Face Aging and Rejuvenation", Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence (IJCAI-18), Stockholm, Sweden, pp. 899-905.

[41] H. Yang, D. Huang, Y. Wang & A. K. Jain (2018)" Learning face age progression: A pyramid architecture of GANs", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2018), Salt Lake City, USA, pp. 31– 39.

[42] P. Li, Y. Hu, Q. Li, R. He & Z. Sun (2018) “Global and local consistent age generative adversarial networks”, IEEE International Conference on Pattern Recognition, Beijing, China.

[43] P. Li, Y. Hu, R. He & Z. Sun (2018) “Global and Local Consistent Wavelet-domain Age Synthesis”, arXiv:1809.07764.

[44] J. Wu, C. Zhang, T. Xue, W. T. Freeman & J. B. Tenenbaum (2016) “Learning a probabilistic latent space of object shapes via 3d generative-adversarial modeling,” In Advances in Neural Information Processing Systems 29 (NIPS 2016), Barcelona, Spain.

[45] J. Wu, Y. Wang, T. Xue, X. Sun, B. Freeman & J. Tenenbaum (2017) “Marrnet: 3d shape reconstruction via 2.5 d sketches”, Advances in Neural Information Processing Systems,Long Beach, USA, pp. 540–550.

[46] W. Wang, Q. Huang, S. You, C. Yang & U. Neumann (2017) “Shape inpainting using 3d generative adversarial network and recurrent convolutional networks”, The IEEE International Conference on Computer Vision (ICCV 2017),Venice, Italy, pp. 2298-2306.

[47] E. J. Smith & D. Meger (2017) “Improved adversarial systems for 3d object generation and reconstruction”, first Annual Conference on Robot Learning,Mountain View, USA, pp. 87–96.

[48] P. Achlioptas, O. Diamanti, I. Mitliagkas& L. Guibas (2018) “Learning representations and generative models for 3d point clouds”, 6th International Conference on Learning Representations, Vancouver, Canada.

[49] X. Sun, J. Wu, X. Zhang, Z. Zhang, C. Zhang, T. Xue, J. B. Tenenbaum & W. T. Freeman (2018) “Pix3d: Dataset and methods for single-image 3d shape modeling”, IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2018), Salt Lake City, USA, pp. 2974-2983.

[50] D. Maturana &S. Scherer (2015) “VoxNet: A 3D Convolutional Neural Network for real-time object recognition”, 2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS),Hamburg, Germany, pp. 922 – 928.

[51] B. Shi, S. Bai, Z. Zhou & X. Bai (2015) “DeepPano: Deep Panoramic Representation for 3-D Shape Recognition”, IEEE Signal Processing Letters ,Vol. 22(12), pp. 2339 – 2343.

[52] A. Brock, T. Lim, J. Ritchie & N. Weston (2016) “Generative and discriminative voxel modeling with convolutional neural networks”, arXiv:1608.04236.

AUTHORS

Shirin Nasr Esfahani received her M.S. degree in computer science – scientific computation from Sharif University of technology, Tehran- Iran. She is currently a Ph.D. candidate in computer science, University of Nevada, Las Vegas (UNLV). Her fields of interest include, hyper spectral image processing, neural networks, deep learning and data mining.

Shahram Latifireceived the Master of Science and the PhD degrees both in Electrical and Computer Engineering from Louisiana State University, Baton Rouge, in 1986 and 1989, respectively. He is currently a Professor of Electrical Engineering at the University of Nevada, Las Vegas.

IoT -Based Approach To Monitor Parking Space In Cities

Fatin Farhan Haque[1], Weijia Zhou[2], Jun-Shuo Ng[3], Ahmed Abdelgawad[4], Kumar Yelamarthi[5] and Frank Walsh[6]

[1,2,4,5]College of Science and Engineering, Central Michigan University, Michigan, USA

[3,6]Department of Computing and Mathematics, Waterford, Ireland

ABSTRACT

Internet of Things is the next big thing, as almost everything developed now has an extensive use of data which is then used to get the daily statistics and usage of every individual. The work mainly consists of constructing a screen where the parking space will be shown, and a camera module will be set up, and PIR (Passive Infrared Sensor) will be at the entrance to detect the entrance of a car or any vehicle eligible to park at the lot. The vehicle will be scanned for its registration number in to provide a check whether the vehicle is registered to park or not. This also acts as the security of the parking lot. Moreover, a viable sensor will be placed at each parking slot through which the vacancy of each parking slot will be shown to determine the exact spot available to the user. In order to surpass the project completion, we will be using Raspberry Pi 3 with camera module mounted on it and by using Tensorflow, Node-Red we would be able to identify the car and the license number and also infrared sensor to detect the parking availability which would be displayed on the screen.

KEYWORDS

IoT, Node-Red, Tensor Flow, smart, parking

1. INTRODUCTION

The project proposal is initiated due to the current issues that are being faced by some regular people every day, i.e., to find a parking spot. The idea is mainly to create a device with a camera module mounted on it which will help to scan only the cars entering and exiting a parking lot and will display the appropriate space remaining in the lot. As it has been known that 20% of the drivers are getting irritated by driving the whole block to look for vacancy spot to park the car [12]. People are getting dependent upon the app which can help them get proper information about the parking lot occupancy, but inevitable due to the improper implication of GPS and other sensors [1]. The micro-controllers are used since they are battery-operated platform and costs very less with quite big life expectancy and also has numerous numbers of configuration options with a deployable architecture to run any application [2]. Another approach will show if the system is working according to the setup, if there are sufficient sensor network with whom the system is going to interact and process data that will help in showing the status i.e. occupied/vacancy of the parking lot [11]. If applied through IoT devices all the technological limitations can be portrayed as storage, processing and energy and the cloud will be able to deal with all the computation and real applications [7].

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 77-84, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90907

Some extra features have been added, and that is, the camera module will also scan the vehicle license number in order to determine whether the vehicle is registered for that space or not, this will help the authority to track down unregistered vehicle taking up space in the lot. Every system is not properly designed, as in terms of real-time detection some incorrect parking might lead to costly parking charges [3]. Through this system, time consumption will be minimized to find an available parking slot. The system can be applied in a different way, one is to create an algorithm and recognize the difference in walk-in state and drive state through which the state change will trigger the detection [4]. Another feature that can be added is with a viable sensor on each parking space, which will basically feed information to the cloud whether that space is empty in the lot or not and hence, a display of all the available space will be provided through which the vehicle entering can easily track down the space without wasting any time. As, it is known that the range of the sensor, for example, infrared lies from 20 to 4000 mm which will help us deduce the actual vacancy of the parking area [10].

Some previous work entitles as to use the visual sensor network in order to determine the parking space automatically and in order to do that encrypting of images or videos are being sent to the central controller which deals with all the decrypting and analyzing the contents that have been sent over. Implementing few techniques like detecting character recognition by OpenCV which stands for Optical Character Recognition and reading out the number plate number [8]. Using machine learning has been the next thing in today's world, which implies to unusual pattern in recognizing the parking spaces being allocated and dynamically checking out the vacancy in the parking lot area [9]. The sensors that can be used to achieve the task and get back with the information on the parking lot area are, ultrasonic, inductive loops, infrared sensors as the sensors tend to be very reliable but for huge parking lots the cost can be huge and hence using convolutional neural network can be an option to get the desired output [13]. The process and other related measures take enough power and capacity, but this can be resolute by connecting the network in the hub which in here acts in the cloud [14]. Another work relates to real-time detection of a vehicle entering and an automatic collection of parking fees which somehow gets declined if the real-time feature is not being focused on, as there have been already several literature reviews on the smart-parking system, hence other features are mostly being focused in.

2. METHODOLOGY

Two ways will be applied to make the work successful:

- Vehicle Recognition via Cameras: Multiple cameras will be installed in the parking lot to monitor all parking space and then accumulate their conditions.

- Viable Sensor: Each parking space is equipped with a viable sensor, which will basically feed information to the cloud whether space is empty or not.

- Provide any kind of warning or notification when any car is about to reserve the spot. Ultimately, a device with data receiver inside will be installed in the entrance to properly convert the information and present it to users in a straightforward way.

  The challenges that can be faced while doing the project would be, mounting the cameras and getting proper feeds in the cloud and making a detection about vehicle's registration is also another challenge that needs to get overcome.

3. RELATED WORKS

The paper [5] illustrates the use of a smart parking facility with a few standard methods that are also IoT related and also for the ease of people in everyday life. Through an app, the registration

and issuing of parking slip and vacancy are denoted and will be updated in the app through cloud mechanism. The sensors are used in an appropriate spot for the collection of data as per needed for the system to make necessary actions. It only deals with the space being empty and issuing the ticket as applicable.

The paper [6] discusses comparing two different paradigms: Compress-Then-Analyze (CTA) and Analyze-Then-Compress (ATC) when using a visual sensor system to analyze parking lot occupancy. CTA paradigm is to capture an image in real time and sending it to a processing unit to obtain information; ATC paradigm requires the visual content to be processed locally on the camera module itself before sending it off to be processed. The comparison is done to mainly compare energy consumption, bandwidth usage and, the accuracy of data of both paradigms. ATC method was much more effective on that when deploying in the real-world examples.

4. IMPLEMENTATION

A list of supplies that are needed for the smart parking lot are, Raspberry Pi 3 to convolute the results as per required, the Camera to scan the license plate number and recognizing the vehicle, OpenALPR to help in getting the correct the license plate number by using it's set of libraries, set of Wires for sensor connectivity, Toy Cars for the purpose of the real-time scenarios, Infrared Sensors for detecting the incoming vehicle approaching, LCD Screen for showing the exact spot to park the vehicle, PIR Sensor for detecting the motion of approaching car and working along the proposed way and lastly the LED to show that the oncoming vehicle is allowed to park in the available spot as it is registered in the system.

A Raspberry Pi 3 with camera module is mounted on the Pi (shown in Fig: 1) and connected with a display to helps us configure the related software and build-ups required in order to process the object identification with TensorFlow and the color of the object and also the model of the car will be identified. The Node-Red platform has been deployed which will focus on the checking of the license plate number and extracting the whole license number and then the number will be passed on to the cloud server which then will be used to check for the registration of the vehicle and through the check, if the license plate number matches up then the entrance gate will open up to let the vehicle in otherwise, it will stay close. In Fig 2, it has been shown how the Node-Red dashboard looks like after deployment. On another note, an offline process has also been applied which has been done by using the OpenALPR (open Automatic License Plate Recognition) which will in thus help to not rely on the internet as sometimes there might be delay or loss of connection. The code has been done on the Python platform and will help us determine the license plate number by using machine learning coding. The whole set up makes the work a pretty drastic since it takes a lot of time to configure the set of libraries and other related operations to make the Raspberry Pi suitable to detect the objects as per described in the tensorflow terminologies. There were few challenges that were faced while doing this, and it has been listed at a later stage in the paper.

The first step was to set up the tensorflow in the Pi and make it detect objects which later on we are going to focus on making it restricted to focus on only one object which is known as the single object detection. Fig 3 shows pictures of the data that we have collected, and which also shows a percentage of assumption of the object that the Pi was able to detect. In Fig 3, it can be seen that at the top-left corner of the detection frame, the accuracy of the object being detected and the object itself is illustrated.

Fig 1: Raspberry Pi with the camera module

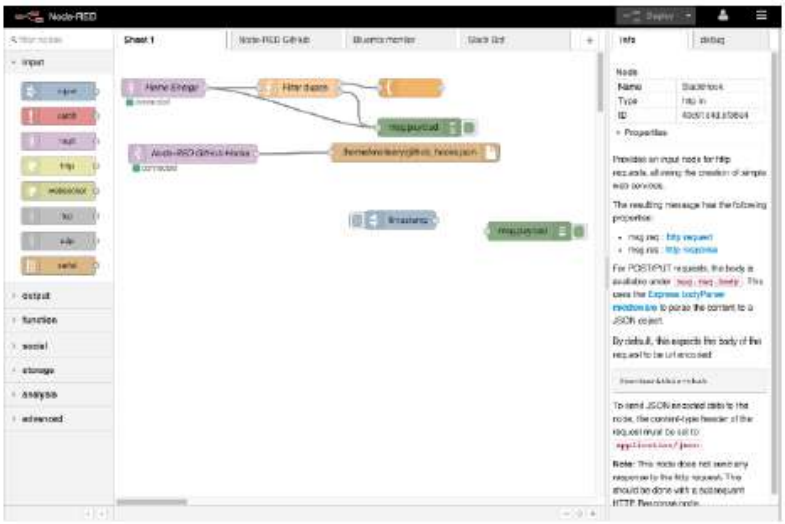


Fig 2: The Node-Red terminal where the action has been shown and the results received are displayed on the right-hand side.

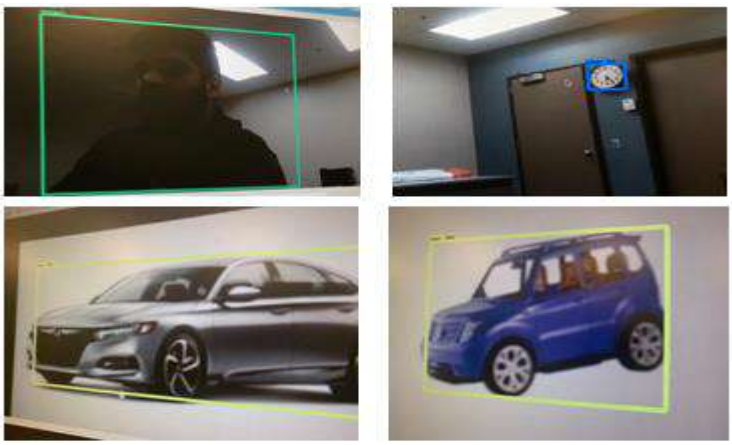


Fig 3: (a) a person with 95% accuracy. (b) A clock with 95% accuracy. (c) A car with 97% accuracy. (d) A toy car with 98% accuracy.

Fig 4 evaluates the flow of the process through multiple scanning and sensor reading and thus the results will be displayed on the screen as a vehicle approaches and try to get in the parking area.

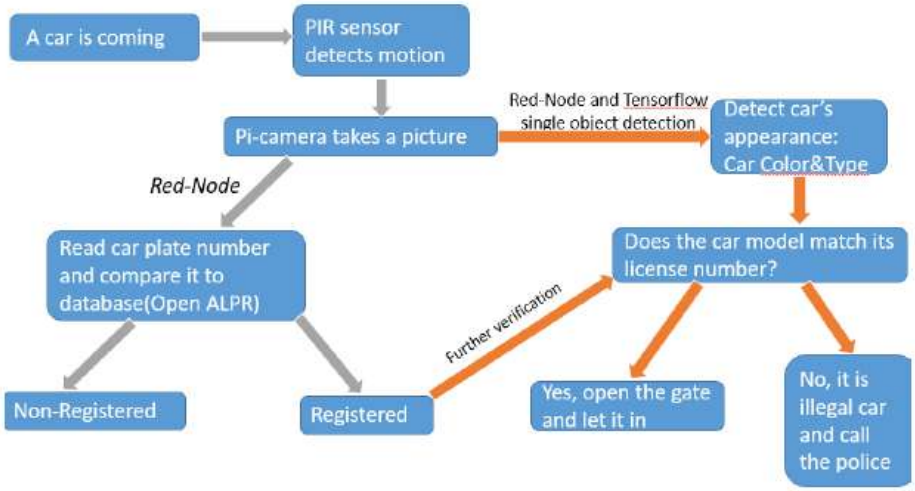


Fig 4: The flowchart describing te overall process.

Fig 5, shows the overall schematic diagram which had been hooked up on the breadboard using the sensor mentioned previously. This will be set up at the front gate in a box which in thus helps to resonate the program being deployed.

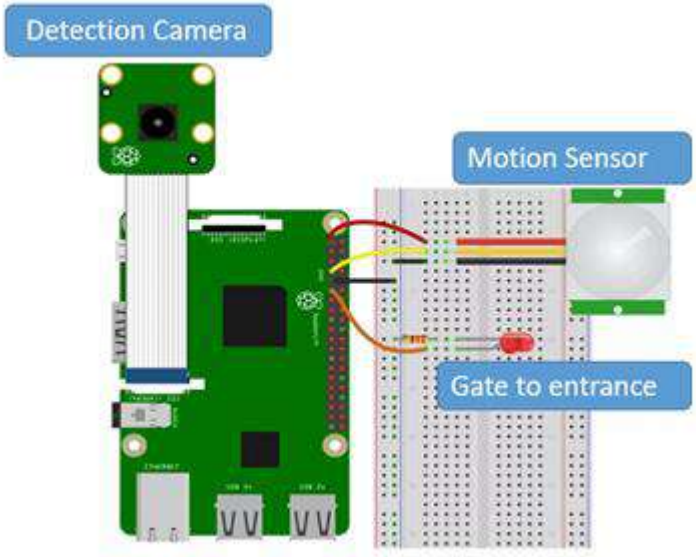


Fig 5: The schematic hook-up of the process.

In Fig 6, the flowchart depicts the use of the parking lot assignment and the screen demonstrates which parking area is vacant and where the vehicle can go and park, which is also in turns can be set as reserved for that vehicle.

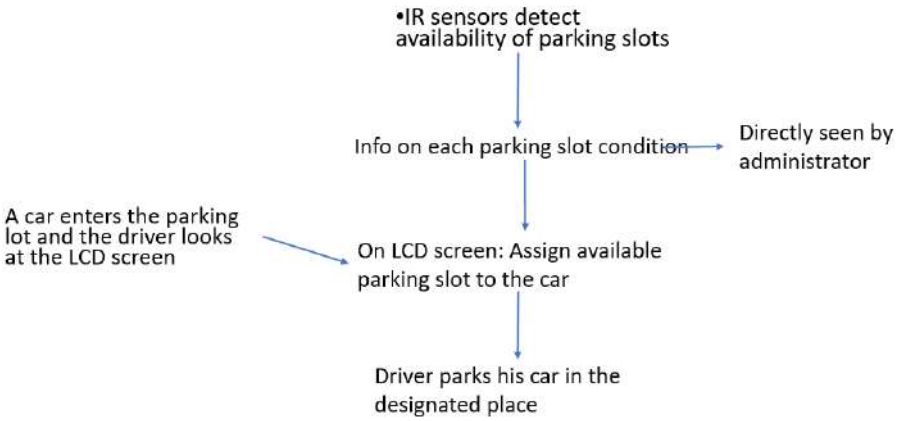


Fig 6: The flowchart representing the parking lot assignment.

5. RESULTS

As the process has been deployed, we started to get data from the system. At first, we tried the license plate detection, and the results are shown in Fig 7, which portrays both the registered and unregistered car after reading the license plate number through the raspberry pi camera.

Fig 7: The picture illustrated the car license number detection and the license being recognized.

Fig 8: The picture shows the license of a different car and the license being recognized as unregistered.

The hookup diagram and the LCD screen has been shown in Fig 8, which will save the user time to look for parking as it will automatically display which parking area to go in to since each parking slot is equipped with an infrared sensor and feeds information to the LCD.

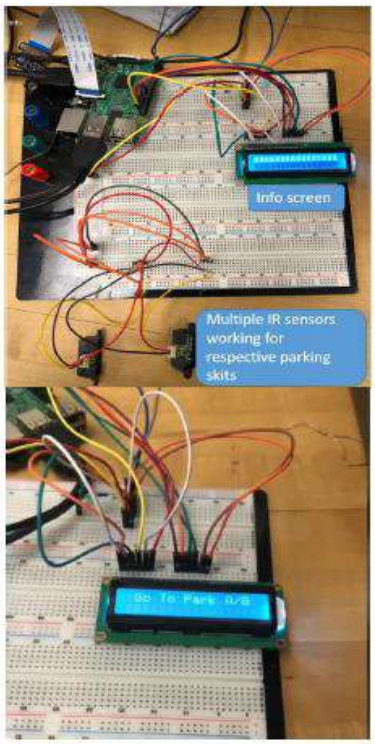


Fig 9: The hookup diagram and the anticipated output to be displayed.

6. CONCLUSION AND FUTURE WORK

The parking lot assignment has been the new thing which automatically tells users which parking slot to place their vehicle, as it has been one of the many concerns that everyone has nowadays, and everyone wants to park their vehicle more effectively and efficiently. The setup and everything else were done to ensure the ease of set up each parking lot equipment. The introduction of machine learning will help in determining the collection of vehicles coming in and will take less time in the future to detect the objects coming in.

Our future work lies in applying this to the real parking lot as this is just a prototype and there would be latency and power consumption, which we need to focus on making this embedded system further proceed.

ACKNOWLEDGEMENTS

The authors would like to thank K. Yelamarthi, F. Walsh and A. Abdelgawad for their constant feedback of the work and making it more keen and precise for the acquired data to make it more compatible in the real-world applications.

REFERENCES

[1] A. Nandugudi, T. Ki, C. Nuessle & G. Challen, 2014. PocketParker: pocketsourcing parking lot availability. In International Joint Conference on Pervasive and Ubiquitous Computing. Seattle, 2014, ACM.

[2] J. A. Propst, K. M. Poole & J. O. Hallstrom, 2012. An embedded sensing approach to monitoring parking lot occupancy. In 50th Annual Southeast Regional Conference. Tuscaloosa, 2012. ACM.

[3] P. Sadhukhan, 2017. An IoT-based E-parking system for smart cities. In International Conference on Advances in Computing, Communications, and Informatics (ICACCI). Udupi, 2017. IEEE.

[4] S. Soubam, D. Banerjee, V. Naik, & D. Chakraborty, 2016. BluePark: tracking parking and un-parking events in indoor garanges. In International Conference on Distributed Computing and Networking. Singapore, 2016. ACM.

[5] V. Hans, P. S. Seithi, J. Kinra, 2015. An approach to IoT based car parking and reservation system on cloud. In International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE.

[6] L. Baroffio, L. Bondi, M. Cesana, A. E. Redondi, M. Tagliasacchi, 2015, "A Visual Sensor Network for Parking Lot Occupancy Detection in Smart Cities". In IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE.

[7] A. Khanna, R. Anand, 2016." IoT Based Smart Parking System". In 2016 International Conference on Internet of Things and Applications (IOTA). IEEE.

[8] S. Rane, A. Dubey, T. Parida, 2017. "Design of IoT based intelligent parking system using image processing algorithms". In IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC).

[9] X. Ling, J. Sheng, O. Baiocchi, X. Liu, M. E. Tolentino, 2017. "Identifying Parking Spaces & Detecting Occupancy Using Vision-based IoT Devices". In 2017 Global Internet of Things Summit (GIoTS).

[10] K. Laubhan, M. Trent, B. Root, A. Abdelgawad, K. Yelamarthi. "A Wearable Portable Electronic Travel Aid for Blind". In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)

[11] S. Shinde, A. Patil, S. Chavan, S. Deshmukh, S. Ingleshwar. "IoT Based Parking System Using Google". In 2017 International Conference on I-SMAC (IoT in Socail, Mobile, Analytics and Cloud).

[12] S. Mendiratta, D. Debopam, D. R. Sona. "Automatic Car Parking System with Visual Indicator along with IoT".In 2017 International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS).

[13] S. Valipour, M. Siam, E. Stroulia, M. Jagersand. "Parking-Stall Vacancy Indicator System, Based on Deep Convolutional Neural Networks". In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT).

[14] K. Laubbhan, K. Talaat, S. Riehl, M. S. Aman, A. Abdelgawad, K. Yelamarthi. "A Low-Power IoT Framework: From Sensors to the Cloud". In 2016 IEEE International Conference on Electro Information Technology (EIT).

QUERY PERFORMANCE OPTIMIZATION IN DATABASES FOR BIG DATA

Manoj Muniswamaiah[1], Dr. Tilak Agerwala[2] and Dr. Charles Tappert[3]

[1]Seidenberg School of CSIS, Pace University, White Plains, New York

ABSTRACT

Organizations maintain different databases to store and process big data which is huge in volume and have different data models. Querying and analysing big data for insight is critical for business. The data warehouses built should be able to meet the ever growing demand of data. With new requirements it is important to have near real times response from the big data gathered. All the data cannot be fit in to one particular database "One Size Does Not Fit All" since data originating from sources have different formats. The main focus of our research is to find an adequate solution using optimized data created by data engineers to improve the performance of query execution in a big data ecosystem.

KEYWORDS

Databases, Big data, Optimization, Analytical Query, Data Analysts and Data Scientists.

1. INTRODUCTION

Big data enables organizations to analyze data which is immense in volume, variety and velocity for decision making and take appropriate actions. There are different databases with varied data models to store and query big data: Columnar databases are used for read heavy analytical queries; online transactional processing databases are used for quicker writes and consistency; NoSQL data stores are used to process large volume of data and for horizontal scaling; HTAP databases are hybrid of both OLTP and columnar databases [1].

There are various data stores been designed and developed for specific needs and for optimal performances. Relational databases can store and process structured data efficiently but its performance decreases with read heavy queries. Similarly columnar databases are used for analytical query processing and NoSQL data stores are specialized to handle unstructured data. The processed data is stored in different databases to be used by analysts [1].

Performance optimization and different data models are important for data intensive applications. The main challenge is to build data pipelines that are scalable and efficient. Data engineers optimize and maintain these data pipelines which are crucial for the performance of the applications. Data pipelines process, transform and load the data in to the data warehouse which are used by data analysts and data scientists for research. Big data platforms which use different databases continue to be challenging with regard to improvement of query performance and also added complexity due to different data models used in these databases.

Data engineers primary job is to partition, normalize, index the base tables in order to improve the performance of the queries which are used for dashboards and reports. These optimized copies would be stored in different databases based on their data models for querying and quicker response. In this research we want to automate this process where if data analysts or data

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 85-90, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90908

scientists issues a query against any desired database the query framework should be able to detect the optimized copies created and stored by data engineers and execute the query against optimized copy rather than the base table which would improve the performance of the query response.

2. BACKGROUND

There are several techniques to improve query performance and response time like partitioning the base table, indexing on required columns, materialization and creating OLAP cubes. Indexing helps in faster reads and retrieval of data. It is similar to dictionary data lookup, B-tree indexing keeps the data sorted and allows for sequential access of the data [2]. Consistency and freshness of the optimized copies is maintained by updating them whenever the base table changes.

BigDAWG is a polystore framework implemented to support multiple databases. The main feature of BigDAWG is to provide location independence which routes the queries to the desired databases and semantic completeness which lets the queries to make use of the native database features effectively. Location independence is implemented using island concept where databases with similar data models are grouped together. Shim component is used to translate the incoming query into their respective native database queries to take the advantages of the database features. One of the important features provided by BigDAWG is casting where data from one format is been converted in to another and queried [3].

Apache Kylin is an open source distributed analytical engine that supports SQL interface and multi-dimensional analytics on Hadoop for large datasets originally been developed by eBay inc. OLAP cubes are built offline using map reduce process. Recently Apache Spark is been used to speed up the cube build process which is stored in HBase data store. When users issue a query they are routed to be executed against the prebuilt cubes for quicker response, if the desired cube does not exists then the query would be executed against the Hadoop data [4].

Myria is an academia analytical engine been developed and provided as a cloud service. MyriaX is the analytical engine which efficiently executes the queries. MyriaL is the query language supported by Myria for querying [5].

Apache Hive is used for batch processing of big data. It coverts SQL-like queries in to map reduce jobs and executes the queries. HiveQL is the query language used for processing of the data [6].

Kodiak is an analytical distributed data platform which uses materialized views to process analytical queries. Various levels of materialized views are created and stored over petabytes of data. Kodiak platform can maintain these views efficiently and update them automatically. It shows that query execution was three times faster and also used less resources [7].

Apache Lens is another open source framework which tries to provide a unified analytical layer of Hadoop and databases ecosystem using a REST server and query language CubeQL to store and process data cubes [8].

Analytical queries whose aggregates have been stored as OLAP cubes are used in reports and dashboards. These cubes often need to be updated with latest aggregates. Multiple databases are used within an organization for various tasks to store and retrieve the data. Data engineers implement data pipelines to optimize datasets which would be later used by data analysts and data scientists for research. Creating optimized copies involves partitioning and indexing of the base tables. These optimized copies would later be stored in different databases for querying.

Our research focus and solution is to implement a query framework that routes the data analysts and data scientists queries to the optimized copies created by data engineers which are stored, maintained, updated automatically to achieve better query performance and reduce response time.

3. QUERY OPTIMIZER

Apache calcite framework is an open source database querying framework which uses relational algebra for query processing. It parses the incoming coming query and converts them to logical plans and later various transformations would be applied to convert this logical plan into optimized plan which has low cost in execution. This optimized logical plan would be converted in to physical plan to be executed against the databases by using traits. Query optimizer eliminates logical plans which increase cost of the query execution based on cost model been defined. Apache Calcite Schema contains details about the data formats present in the model which is used by schema factory to create schema [9].

The query optimizer applies the planner rules to the relational node and generates different plans with reduced cost by retaining the original semantics of the query. When a rule matches a pattern query optimizer executes the transformations by substituting the sub tree in to the relation expression and also preserves the semantics of it. These transformations are specific to each databases. The metadata component provides the query optimizer with details of the overall cost of the execution of the relational expression and also the degree of parallelism that can be achieved during execution [9].

The query optimizer uses cost-based dynamic programming algorithm which fires rules in order to reduce the cost of the relational expression. This process continues until the cost of the relational expression is not improved subsequently. The query optimizer takes in to consideration CPU cycles, memory been used and IO resource utilization cost to execute the relational expression [9].

One of the techniques which is used to improve query processing is to use the optimized copies been created by data engineers in big data analytics. The query optimizer needs to have the ability to make use of these optimized copies to rewrite the incoming queries to make use of them. Optimizer does this by substituting part of the relational expression tree with optimized copies which it uses to execute query and return the response.

Algorithm

Optimization of relational expression R:

1. Register the relational expression R.
   a. Check for existence of appropriate optimized copy which can be used to substitute relational expression R.
   b. If optimized copy exists, then register the new relational expression R1 of the optimized copy.
   c. Trigger the transformation rules on relational expression R1 for cost optimization.
   d. Obtain the best relational expression R1 based on cost and execute it against the database.
2. If the relational expression R cannot be substituted with an existing optimized copy
   a. Trigger the transformation rules on relational expression R.
   b. Obtain the best relational expression based on cost and execute it against the database.

4. ARCHITECTURE

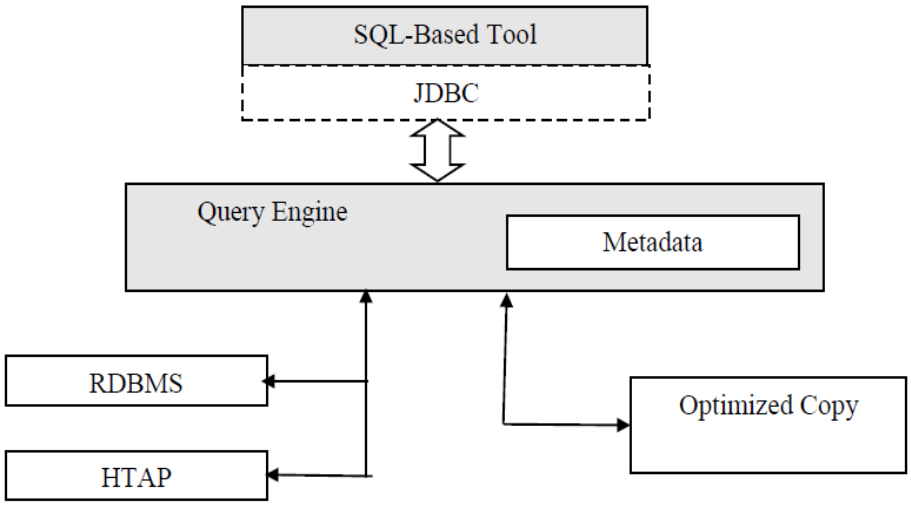


Figure 1. Architecture of the SQL Framework

The analytical queries been executed would be parsed and different logical plans would be generated. The query parser determines if the parsed relational expression can be substituted with the registered optimized copies been created by data engineers automatically. It executes various rules to obtain relational expression with minimal cost. The query would then be rewritten to be executed against the optimized copy and the results would be returned.

SQL-Tool: Includes any tool which can be integrated using JDBC connection and execute SQL analytical queries.

Query Engine: Apache Calcite open source framework that includes query optimizer been extended to include optimized copies.

Metadata: Contains information about the schema and the features of the native databases.
Optimized copy: Optimized tables created by the data engineers.

RDBMS: Includes any relational database to store structured data.
HTAP: Hybrid database which has the scalability of NoSQL data stores.

5. EVALUATION

Analytical queries helps in data driven decision making. In this paper we used NYC Taxi and Limousine Commission (TLC) datasets provided under the authorization of Taxicab & Livery Passenger Enhancement Programs consisting of the green and yellow taxi data [10].

These datasets help in answering questions regarding the passenger drop-pick, drop-off, how Uber ride sharing affect taxi services, do passengers use ridesharing or taxi services to reach common public places, the average time taken to reach the destination, the payment mode used by passengers and other such queries.

The following experimentation setup was made to benchmark and evaluate the query optimizer performance to find the optimized copy of the data and substitute it in the query plan during run time and execute it against the optimized copy Data engineers usually store these optimized copies in the columnar database for faster read access. The tables and data used for the query evaluation was obtained from NYC taxi dataset [10]. Data was stored in Mysql [11], Splice Machine [12] and Vertica database [13].

Evaluation was obtained based on the following setup

a.) Base tables had rows ranging from ~10,000,000 to ~20,000,000
b.) Optimized copy tables had rows ranging from ~1,000 to ~4,000,000
c.) Mysql, Splice Machine and Vertica database were running on single node instance with 2X Intel Quad Core Xeon 3.33GHz, 24 GB RAM and 1TB HDD.
d.) Base table data been stored in HDFS [14].
e.) Optimized copies been stored in Vertica database.
f.) SQL query optimizer used cost based dynamic algorithm to substitute optimized in the query plan.

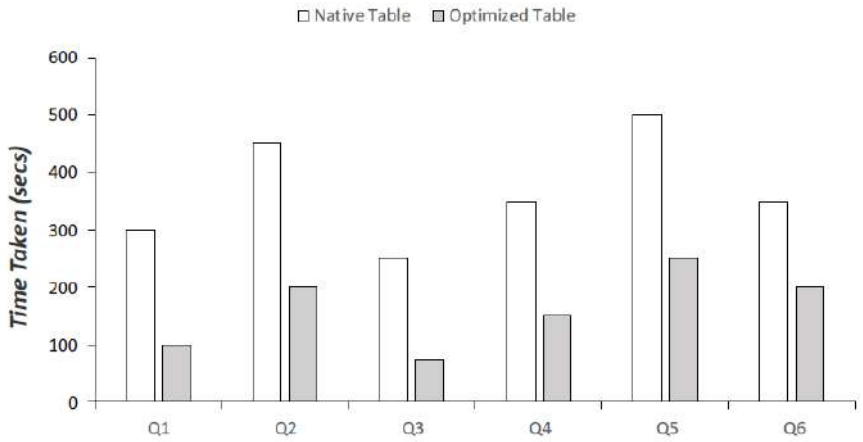


Figure 2. Query Response Time

The two bar graphs show the analytical queries been executed by the query optimizer against the base table and the optimized copy. The query optimizer was successfully able to substitute the optimized copy in the query plan when it existed and improve the performance of the query and its response time.

6. CONCLUSION

In this research we were able to make extensions to cost based query optimizer to make use of the optimized copies to obtain an improved query response time and performance. Various analytical queries were executed to measure the results obtained. The query optimizer was successfully able to substitute the optimized copies when existed during the runtime and modify the incoming query to execute against it. Part of the future work is to extend this query optimizer to the cloud databases.

REFERENCES

[1] Duggan, J., Elmore, A. J., Stonebraker, M., Balazinska, M., Howe, B., Kepner, J., et al. (2015). The BigDAWG Polystore System. ACM Sigmod Record, 44(3)

[2] V. Srinivasan and M. Carey. Performance of B-Tree Concurrency Control Algorithms. In Proc.ACM SIGMOD Conf., pages 416–425, 1991

[3] A. Elmore, J. Duggan, M. Stonebraker, M. Balazinska, U. Cetintemel,V. Gadepally, J. Heer, B. Howe, J. Kepner, T. Kraskaet al., "A demonstration of the bigdawg polystore system,"Proceedings of theVLDB Endowment, vol. 8, no. 12, pp. 1908–1911, 2015

[4] http://kylin.apache.org

[5] D. Halperin et al. Demonstration of the myria big data management service. In SIGMOD, pages 881–884, 2014.

[6] Fuad, A., Erwin, A. and Ipung, H.P., 2014, September. Processing performance on Apache Pig, Apache Hive and MySQL cluster. In Information, Communication Technology and System (ICTS), 2014 International Conference on (pp. 297-302). IEEE.

[7] Liu, Shaosu, et al. "Kodiak: leveraging materialized views for very low-latency analytics over high-dimensional web-scale data." Proceedings of the VLDB Endowment9.13 (2016): 1269-1280

[8] https://lens.apache.org/

[9] https://calcite.apache.org/

[10] https://www1.nyc.gov/site/tlc/about/tlc-trip-record-data.page

[11] Luke Welling, Laura Thomson, PHP and MySQL Web Development, Sams, Indianapolis, IN, 2001

[12] https://www.splicemachine.com/

[13] C. Bear, A. Lamb, and N. Tran. The vertica database: Sql rdbms for managing big data. In Proceedings of the 2012 workshop on Management of big data systems, pages 37–38.ACM, 2012

[14] Cong Jin, Shuang Ran, "The research for storage scheme based on Hadoop", Computer and Communications (ICCC) 2015 IEEE International Conference on, pp. 62-66, 2015.

MAXIMIZING THE TOTAL NUMBER OF ON TIME JOBS ON IDENTICAL MACHINES

Hairong Zhao

Department of Mathematics, Computer Science & Statistics
Purdue University, Northwest

ABSTRACT

This paper studies the job-scheduling problem on $m \geq 2$ parallel/identical machines.There are n jobs, denoted by $J_{i,,}1 \leq i \leq n$. Each job J_i, has a due date d_i. A job has one or more tasks, each with a specific processing time. The tasks can't be preempted, i.e., once scheduled, a task cannot be interrupted and resumed later. Different tasks of the same job can be scheduled concurrently on different machines. A job is on time if all of its tasks finish before its due date; otherwise, it is tardy. A schedule of the jobs specifies which task is scheduled on which machine at what time. The problem is to find a schedule of these jobs so that the number of on time jobs is maximized; or equivalently, the number of tardy jobs is minimized. We consider two cases: the case when each job has only a single task and the case where a job can have one or more tasks. For the first case, if all jobs have common due date we design a simple algorithm and show that the algorithm can generate a schedule whose number of on time jobs is at most (m-1) less than that of the optimal schedule. We also show that the modified algorithm works for the second case with common due date and has same performance. Finally, we design an algorithm when jobs have different due dates for the second case. We conduct computation experiment and show that the algorithm has very good performance.

KEYWORDS

On time job, identical machines, order scheduling

1. INTRODUCTION

This paper studies the job-scheduling problem on $m \geq 2$ parallel/identical machines. There are n jobs, denoted by $J_{i,,}1 \leq i \leq n$. Each job J_i, has a due date d_i. A job has one or more tasks, each with a specific processing time. The tasks can't be preempted, i.e., once scheduled, a task cannot be interrupted and resume later. Different tasks of the same job can be scheduled concurrently on different machines. A job is on time if all of its tasks finish before its due date; otherwise, it is tardy. A schedule of the jobs specifies which task is processed on which machine at what time. The problem is to find a schedule of these jobs so that the number of on time jobs is maximized; or equivalently, the number of tardy jobs is minimized. The number of on time/tardy jobs is a very important criterion since, in many cases, the cost penalty incurred by a tardy job does not depend on how late it is, but the fact that it is late. In such cases, an appropriate objective would be to minimize the number of tardy jobs. For example, a late job may cause a customer to switch to another supplier, especially in the just-in-time production environment.

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 91-97, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90909

This problem has been studied in many literatures. In the classic model each job has a single task. When there is a single machine, i.e., m=1, Moore ([2]) gave an O(n log n) algorithm (sometimes known as Hudgson's Algorithm) that solves the problem optimally. When $m \geq 2$, the problem becomes NP hard even if all jobs have the same due date. When m = 2, Leung & Yu [1] gave a heuristic, based on Moore's algorithm, for the multiprocessor case. It is shown that the performance ratio of the heuristic is 4/3 for two identical processors, where the performance ratio is defined to be the least upper bound of the ratio of the number of on-time jobs in an optimal schedule versus that in the schedule generated by the heuristic. Ho and Chang [3] conducted extensive simulation experiment to test the effectiveness of the heuristic on multiple machines. The simulation results showed that this heuristic is quite effective in most cases. The paper also proposed two other heuristics.

The scheduling model where a job can have multiple tasks is called order scheduling in literature (see [4] and the references therein). In general order scheduling, a machine may be dedicated and can only process one type of tasks; or be flexible and can process multiple types of tasks. In this paper, all machines are identical and fully flexible, i.e. every machine is able to process all types of tasks and different tasks of an order/job can be processed concurrently. If there is one machine, the problem minimizing the number of tardy jobs under this model is reduced to the classics model where each job has only a single task. If there are multiple machines, however, the classical model is a special case of order scheduling. Some work has been done for this model with the objective of total completion time. When the jobs are unweighted, Blocher and Chhajed ([5]) show that the problem is ordinary NP-hard for any fixed $m \geq 2$ and strongly NP-hard when m is arbitrary. Then the authors presented six heuristics and performed empirical analysis of the heuristics. Two classes of nine heuristics with proven worst-case performance bounds were studied by Leung, L_i and Pinedo in [6]. To the best of our knowledge, no past work has ever been done for the number of on time jobs objective.

In this paper, we are interested in the performance of simple heuristics for both the classical model and the order-scheduling model. We first consider the case with common due date, then we consider the general case where jobs can have arbitrary due date. For the general case, we evaluate the performance of the heuristics by some experimental results.

Note that for the optimal solution, the problem of minimizing the number of tardy jobs is the same as maximizing the number of on time jobs. However, all our problems are NP-hard so there is no hope to find an optimal schedule in polynomial time. We can only design effective and efficient heuristics for large size problems. To evaluate the effectiveness of a heuristic, we could use the absolute error, i.e. the difference between the optimal solution and the solution found by the heuristic; we may also use relative error, i.e the ratio of the absolute error and the optimal solution. In this case, if we use the number of tardy jobs, it is possible that the optimal schedule has 0 tardy jobs, and consequently the relative error becomes infinity. It is for this reason; we consider the number of on time jobs, instead of tardy jobs in this paper.

2. CLASSICAL MODEL WITH COMMON DUE DATE

In this section, we assume that each job has a single task and all jobs have the same common due date. Using the three field notation, the problem of minimizing the number of tardy jobs can be denoted as $P_m|d_j=d|\Sigma U_j$ where $U_j=1$ if J_j is tardy.

Algorithm1:

Input:

- J= { J_1, J_2 …, J_n}, a set of n jobs, job Ji in has processing time pi and due date d
- m machines, M_1, M_2, …, M_m

Output:

A non-preemptive schedule of a subset of J where all jobs are on time.

Method: Schedule the jobs in SPT order (Shortest Processing Time first) on M1 before d, if no more jobs can be scheduled on M1, and then schedule the jobs on M2 before d, and keep repeating this procedure until all jobs have been scheduled or no more jobs can be scheduled on M_m before d.

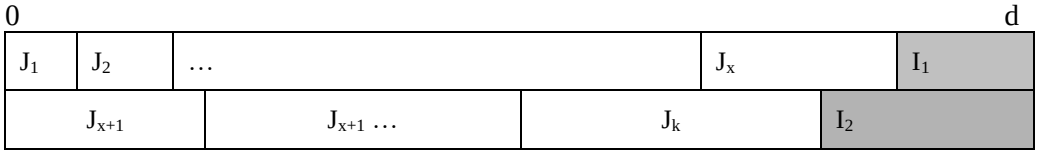
Algorithm1 certainly is not optimal. Consider the example of four jobs and two machines such that the processing times are, 1, 2, 3, 4 and the common due date 5. Algorithm1 will schedule the first two jobs on M_1, and the third job on M_2, and the last job is tardy. However, the optimal schedule will schedule the first job and the last job on M_1, and the second and the third job on M_2. The absolute error is one. It turns out this is not a coincident. We have the following Lemma.

Theorem1. For two machines, the number of on time jobs of the schedule that is generated byAlgorithm1 is at most one less than that of the optimal schedule, i.e. the absolute error of is at most 1.

Proof. For convenience, suppose the jobs are numbered in the SPT order. Suppose there are k on time jobs in the schedule generated by Algorithm1, then it must be the first k shorted jobs. Suppose that the schedule is not optimal. Let I_1 and I_2 be the length of idle interval on M1 and M2, respectively. Then we must have that $I_1 < p_{k+1}$ and $I_2 < p_{k+1}$. Thus, the total processing time of on time jobs before d in any schedule is at most

$$p_1 + p_2 + .. + p_k + I_1 + I_2 < p_1 + p_2 + .. + p_k + 2\ p_{k+1.}$$

Since we schedule the jobs in SPT order, in any other schedule, at most k+1 jobs can be scheduled before d.



Using similar argument, we can prove the following theorem.

Theorem2. For m machines, the number of on time jobs of the schedule that is generated by Algorithm1 is at most (m-1) less than that of the optimal schedule, i.e. the absolute error of is at most (m-1).

3. ORDER SCHEDULING MODEL

In this section, we consider the case that a job may have one or more tasks. For job J_i, we use, $J_{i,1,}$ $J_{i,2,}$ … to represent its tasks, and we use $p_{i,1}$, $p_{i,2}$, … to represent the length of these tasks. We still use pi to represent the total length of the job. Different tasks of the same job can be scheduled concurrently on different machines. We consider 2 cases, the jobs have common due date and the case each job has their own due date. Without loss of generality, we assume that for each job, $p_j \leq d_j$.

3.1. Common Due Date

Modified Algorithm1: We still consider the jobs one by one in SPT order, and for each job, schedule the tasks in arbitrary order; for a particular task, first check if it can be scheduled on the first machine before the due date, if not, then check if it can be scheduled on the second machine, and so on. If the task can't be scheduled to any machine before the due date, then this job and remaining jobs will be the tardy jobs. Otherwise, we repeat this procedure until all jobsare scheduled before the due date or until no more jobs can be scheduled on time.

Using similar argument as the proof of theorem1, we can prove the following theorem.Theorem3. For m machines, the number of on time jobs of the schedule that is generated by Modified Algorithm1 is at most (m-1) less than that of the optimal schedule.

3.2. Different Due Date

Algorithm2: Consider the jobs EDD (Earliest Due Date First) order. For each job, schedule the tasks one by one in arbitrary order; to schedule a task $J_{i,x}$, choose the machine with the latest finishing time such that $J_{i,x}$ can finish before its due date d_j. If there is no such machine, it means J_i or one of the jobs that have been scheduled on time has to be tardy.

To find out which one is a better choice for the tardy job, we do the following:

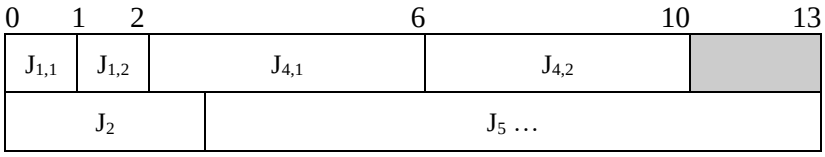
- Restore the schedule by deleting those tasks of J_i that have been scheduled. Let S be the schedule, and f_{max} be the maximum finishing time of the jobs that have been scheduled in S.
- Find the job J_k with the largest processing time from those jobs that have been scheduled.
- Deleting job J_k from the schedule, try to schedule job J_i.
- If some of the tasks of J_i can't be scheduled on time, Ji will be chosen as a tardy job. Otherwise, let S' be schedule obtained, and let f'_{max} be the maximum finishing time of the tasks of J_i in S'. If $f_{max} \leqslant f'_{max}$, J_i will also be chosen as the tardy job, else J_k will be chosen as the tardy job.

After we choose J_k or J_i as the tardy job, continue to schedule the remaining jobs to S' if J_k is tardy or S if J_i is on time. We terminate the process until all jobs have been scheduled on time or chosen as a tardy job.

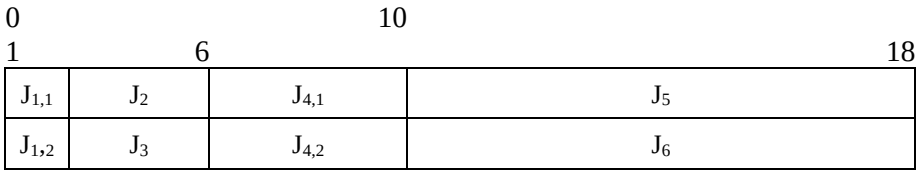
Following is an example of applying Algoirhtm2. Suppose there are 2 machines, 6 jobs.

J_1 has 2 tasks of length 1, 1, and due date 4. J_2 and J_3 have both single task of length 3, and due date 4. J_4 has 2 tasks of length 4, 4, and due date 10. J_5 and J_6 have both single task of length 10, and due date 18.

Algorithm 2 schedules J_1 J_2, J_4 and J_5 before their due dates, and two other jobs are tardy, as in the following figure.



In the optimal schedule, however, all 6 jobs are on time.



One can generalize the above example to more jobs, so that the optimal schedule has all jobs on time, but the schedule generated by Algorithm 2 has 2/3 of the jobs on time. Thus the absolution error can be quite large.

4. COMPUTATIONAL RESULTS

In this section, we want to design experiments to find the performance of Algorithm2 for randomly generated large instances.

We choose the number of jobs n = 500, and the number of machines m = 20. Problem instances of varying hardness are generated according to different characteristics of the due dates. First of all, for each job, the number of tasks is randomly generated from the uniform distribution [1,10m]. Then, the length of each task is generated from the uniform distribution [1,100]. Finally, after all jobs are generated, for each job, its due date is generated from the following uniform distribution: $P/m[(1- \delta 2 - \delta 1/2), (1- \delta 2 + \delta 1/2)]$ where P is the total processing time of all the tasks, $\delta 1$ and $\delta 2$ determines the range in which the due dates lie and adjusts the tightness of the due dates, respectively. We set $\delta 1$ = 0.2, 0.4, 0.6, 0.8, 1.0 and $\delta 2$ = 0.6, 0.8, 1.0. For each combination of $\delta 1$ and $\delta 2$, 100 instances are generated. Thus, there are 2500 instances in total. The algorithms are implemented in Java.

To evaluate the algorithm, for each generated instance Ii (i = 1, 2, . . . , 100), we construct the corresponding single-machine instance I'_i as described follows:

For each job j, construct a job j for I' i with processing time $p'_j = p_j/m$ and due date $d' = d$. The instance I'_i can be solved optimally by Moore's algorithm, and one can show that the number of on time jobs of I'_i, denoted by $UB(I'_i)$, is an upper bound of the number of on time jobs of the original instance I_i. We compare the number of on time jobs of the schedule found by Algorithm2 with its corresponding upper bound.

Our result shows that the absolute error in most cases is less than one, i.e. Algorithm 2 finds optimal schedule in most cases. We also calculated the average relative error with respect to the upper bound, and the result is summarized as follows.

(δ1, δ2)	(0.2,0.2)	(0.2,0.4)	(0.2,0.6)	(0.2,0.8)	(0.2,1.0)
relative error	0.10%	0.10%	0.20%	0.20%	0.10%
(δ1, δ2)	(0.4,0.2)	(0.4,0.4)	(0.4,0.6)	(0.4,0.8)	(0.4,1.0)
relative error	0.10%	0.10%	0.10%	0.20%	0.10%
(δ1, δ2)	(0.6,0.2)	(0.6,0.4)	(0.6,0.6)	(0.6,0.8)	(0.6,1.0)
relative error	0%	0.10%	0.10%	0.10%	0.10%
(δ1, δ2)	(0.8,0.2)	(0.8,0.4)	(0.8,0.6)	(0.8,0.8)	(0.8,1.0)
relative error	0.00%	0.10%	0.10%	0.10%	0.10%
(δ1, δ2)	(1.0,0.2)	(1.0,0.4)	(1.0,0.6)	(1.0,0.8)	(1.0,1.0)
relative error	0%	0%	0.10%	0.30%	0.60%

5. CONCLUSIONS

This paper studies the problem of scheduling n jobs to m identical machines with the objective of maximizing the number of on time jobs. Each job J_i, has a due date d_i. A job has one or more tasks and the tasks can't be preempted, but different tasks of the same job can be scheduled concurrently on different machines. We considered two cases: the case when each job has only a single task and the case where a job can have one or more tasks. We designed a simple and effective algorithm when all jobs have common due date. We also designed an algorithm when jobs have different due dates for the second case. We conducted computation experiment and showed that the algorithm has very good performance.

REFERENCES

[1] J Y-T, Leung and V. K.M. Yu, Heuristic for minimizing the number of late jobs on two processors, International Journal of Foundations of Computer Science, Vol 5, Nos 3 & 4 (1994), pp. 261-279.

[2] J. M. Moore, An n job, one machine sequencing algorithm for minimizing the number of late jobs, Management Science, 15 (1968), 102–109.

[3] J. C. Ho and Y. L. Chang, Minimizing the number of tardy jobs for m parallel machines, European Journal of Operational Research, 8(2), 1995, 343-355.

[4] J.-T. Leung, H. Li, M. Pinedo, Order scheduling models: an overview, in: G. Kendall, E. K. Burke, S. Petrovic, M. Gendreau (Eds.), Multidisciplinary Scheduling: Theory and Applications, Springer, 2005, pp. 37–53.

[5] J. Blocher, D. Chhajed, The customer order lead-time problem on parallel machines, Naval Research Logistics 43 (1996) 629-654.

[6] J.-T. Leung, H. Li, M. Pinedo, Approximation algorithms for minimizing total weighted completion time of orders on identical machines in parallel, Naval Research Logistics 53~(4) (2006) 243--260.

INTENTIONAL BLANK

SERVICE LEVEL DRIVEN JOB SCHEDULING IN MULTI-TIER CLOUD COMPUTING: A BIOLOGICALLY INSPIRED APPROACH

Husam Suleiman and Otman Basir
Department of Electrical and Computer Engineering, University of Waterloo
hsuleima@uwaterloo.ca, obasir@uwaterloo.ca

ABSTRACT

Cloud computing environments often have to deal with random-arrival computational workloads that vary in resource requirements and demand high Quality of Service (QoS) obligations. It is typical that a Service-Level-Agreement (SLA) is employed to govern the QoS obligations of the cloud computing service provider to the client. A typical challenge service-providers face every day is maintaining a balance between the limited resources available for computing and the high QoS requirements of varying random demands. Any imbalance in managing these conflicting objectives may result in either dissatisfied clients and potentially significant commercial penalties, or an over-resourced cloud computing environment that can be significantly costly to acquire and operate. Thus, scheduling the clients' workloads as they arrive at the environment to ensure their timely execution has been a central issue in cloud computing. Various approaches have been reported in the literature to address this problem: Shortest-Queue, Join-Idle-Queue, Round Robin, MinMin, MaxMin, and Least Connection, to name a few. However, optimization strategies of such approaches fail to capture QoS obligations and their associated commercial penalties. This paper presents an approach for service-level driven load scheduling and balancing in multi-tier environments. Joint scheduling and balancing operations are employed to distribute and schedule jobs among the resources, such that the total waiting time of client jobs is minimized, and thus the potential of a penalty to be incurred by the service provider is mitigated. A penalty model is used to quantify the penalty the service provider incurs as a function of the jobs' total waiting time. A Virtual-Queue abstraction is proposed to facilitate optimal job scheduling at the tier level. This problem is NP-complete, thus, a genetic algorithm is proposed as a tool for computing job schedules that minimize potential QoS penalties and hence minimize the likelihood of dissatisfied clients.

KEYWORDS

Heuristic Optimization,JobScheduling,JobAllocation,LoadBalancing,Multi-TierCloudComputing

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 99-118, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90910

1. INTRODUCTION

The cloud computing is gaining momentum as the computing environment of choice that leverages a set of existing technologies to deliver better service and meet varying demands of clients. Cloud services are provided to clients as software-as-a-service, platforms, and infrastructures. Such services are accessed over the Internet using broad network connections. The success of cloud computing, in all cases, hinges largely on the proper management of the cloud resources to achieve cost-efficient job execution and high client satisfaction. The virtualization of computing resources is an important concept for achieving this goal [1, 2].

Generally speaking, cloud computing jobs vary in computational needs and QoS requirements. They can be can be periodic, aperiodic, or sporadic [3]. Each job has a prescribed execution time and tardiness allowance. Typically, an SLA is employed to govern the QoS expectations of the client, as well as a model to compute penalties in cases of QoS violation [4, 5]. A major challenge cloud computing service providers face is maintaining a maximum resource utilization while ensuring adequate resource availability to meet the QoS expectation in executing jobs of varying computational demands. Failing to meet its clients QoS demands may result into harsh financial penalties and dissatisfaction of customers. On the other hand, procuring large assets of computational resources can be prohibitively costly. Thus, it is imperative that jobs are allocated to resources and scheduled for processing so as to minimize their waiting time in the environment. The goodness of any scheduling strategy hinges on its ability to achieve high computing performance and maximum system throughput.

There are two job scheduling categories, namely, preemptive scheduling and non-preemptive scheduling. Under preemptive scheduling, a running job can be taken away from the server or interrupted to accommodate a higher priority job. Furthermore, non-preemptive scheduling, in general, is simpler to implement, no synchronization overhead, minimum stack memory needs. Under non-preemptive scheduling, a running job cannot be taken away from the CPU or interrupted. While non-preemptive scheduling allows for a predictable system response time, preemptive scheduling, on the other hand, emphasizes real-time response time at the job level.

In this paper, we are concerned with the issue of job scheduling in multi-tier cloud computing environments. Given a set of client jobs with different computational demands/constraints, to be executed on a multi-tier cloud computing environment, it is desirable that these jobs are scheduled for execution in this environment such that the penalty to be incurred by the service provider is minimized. It is assumed that the environment consists of a set of cascaded tiers of identical computing resources.

Emphasizing the notion of penalty in scheduling the jobs allows us to imply job priority of treatment that is based on economic considerations. As such, the service provider is able to leverage available job tardiness allowances and QoS penalty considerations to compute schedules that yield minimum total penalty. This strategy is particularly useful in situations of excessive volume of demands or lack of an adequate resource availability that will make it impossible to meet the QoS requirements.

2. BACKGROUND AND RELATED WORK

The issue of job scheduling has been an active area of research since the early days of computing. A large body of work exists in the literature about scheduling approaches in cloud computing environments [6–8]. Such approaches, generally speaking, aim at minimizing the average response time of jobs and maximizing resource utilization. Schroeder *et al*. [9] evaluate the Least-Work-Left, Random, and Size-Interval based Task Assignment (SITA-E) scheduling approaches on a single-tier environment that consists of distributed resources with one dispatcher. They propose an approach that purposely unbalances the load between resources. The mean response time and slowdown metrics are used to assess each approach. The primary drawback in their work is that they don't consider migrating jobs between resource queues and as a result fail to produce optimal schedules.

Liu *et al*. [10] report a Min-Min algorithm for task scheduling that makes jobs with long times execute at reasonable times. Li *et al*. [11] present a Max-Min scheduling approach that estimates the total workload and completion time of jobs in each resource, so as to allocate jobs on resources to reduce their average response time. In both approaches, the scheduling decisions dedicate powerful resources to execute specific jobs without accurately considering the different QoS expectations of jobs. For instance, a Max-Min approach assigns the job with the maximum execution time to the resource that provides the minimum completion time for the job, yet does not account for the different job constraints and the impacts of their violations on the QoS. However, states of resource queues are not considered when the decisions are taken, and accordingly ineffective distribution of workloads among the resource queues is expected to occur. Furthermore, such approaches tackle jobs that mainly arrive in batches. When jobs of different constraints and requirements arrive in a consecutive/dynamic manner to a multi-tier cloud computing environment, the scheduling decisions of such approaches would fail to accurately capture the QoS obligations and economical impacts of these jobs on the service provider and client.

Some approaches take advantage of the knowledge obtained about the system state to make

scheduling decisions. Examples of these approaches are: Least Connect (LC), Join-Shortest-Queue (JSQ), Weighted Round Robin (WRR), and Join-Idle-Queue (JIQ). Gupta *et al*. [12] present and analyze the JSQ approach in a farm of servers, that is similar in architecture to a single-tier cloud environment. JSQ assumes the resource of the least number of jobs is the least loaded resource. In contrast, the weighted algorithms (e.g., WRR and WLC) are commonly used in balancing the load among resources in cloud environments [13, 14]. Wang *et al*. [14] effectively apply the WRR algorithm, by determining weights for resources based on their computational capabilities, then allocating and balancing the workloads among these resources. Though, powerful resources would receive extra workloads of jobs. However, the states of the resource queues are not accurately measured, and thus scheduling decisions taken based on only weights of resources often lead to load unbalance among the resource queues.

Lu *et al*. [15] present a JIQ algorithm for large-scale load balancing problems to minimize the communication overhead incurred between resources and multiple distributed dispatchers at the time of job arrivals. In the JIQ algorithm, each dispatcher has a separate idle queue to maintain IDs of idle resources of the tier. An idle resource informs specific dispatcher(s) of its availability to receive jobs. The primary drawback is that an idle resource might experience significant queuing bottlenecks when it requests jobs from many dispatchers at the same time. Also, an idle resource might run the risk of not receiving jobs and thus get under-utilized if its associated/informed dispatchers are empty of jobs, while at the same time other uninformed dispatchers of the tier might be holding jobs waiting to get idle resources. Sometimes, low priority jobs might get a dispatcher that has IDs of idle resources, whilst high priority jobs might be assigned to a dispatcher that has not yet held signals of idle resources. In this case, the low priority jobs would get scheduled and executed in idle resources while the high priority jobs are still waiting.

The Round Robin algorithm, which has been popular in process scheduling, has been adopted in cloud computing to tackle the job scheduling problem. The Round Robin algorithm aims at distributing the load equally to all resources [16]. Using this algorithm, one Virtual Machine (VM) is allocated to a node in a cyclic manner. However, the Round Robin algorithms are based on a simple cyclic scheduling scenario, thus lead to unbalancing the traffic and incur more load on resources. In general, Round Robin algorithms have shown improved response times and load balancing.

Some researchers have adopted Bio-inspired meta-heuristic approaches to tackle the scheduling problem in cloud environments [17–19]. For instance, Nouiri *et al*. [20] present a particle swarm optimization algorithm to minimize the maximum makespan. Nevertheless, their bio-inspired job scheduling formulation makes scheduling decisions to benefit specific jobs at the expense of other

jobs. Such approaches disregard economical penalties that may result from scheduling decisions. Instead, they focus on optimizing system-level metrics. Job response time, resource utilization, maximum tardiness, and completion time are typically used metrics.

Mateos *et al*. [21] propose an Ant Colony Optimization (ACO) approach to implement a scheduler for cloud computing applications, which aims at minimizing the weighted flow-time and Makespan of jobs. The load is calculated on each resource, taking into consideration CPU utilization of all the VMs that are executing on each host. CPU utilization is used as a metric that allows Ant to choose the least loaded host to allocate its VM. Pandey *et al*. [22] report a Particle Swarm Optimization (PSO) algorithm for minimizing the computational cost of application workflow in cloud computing environments. Job execution time is used as a performance metric. The PSO based resource mapping demonstrated superior performance when compared to Best Resource Selection (BRS) based mapping. Furthermore, the PSO based algorithm achieved optimal load balance among the computing resources.

As a general observation, current cloud computing approaches contemplate single tier environments and fail to exploit resource queue dynamics to migrate jobs between the resources of a given tier so as to achieve the optimal job scheduling. Furthermore, schedule optimality is defined based on job response time metrics. The reality is, the scheduling problem is an NP problem and there are situations where finding schedules that satisfy the target response times of all jobs is an impossible task due to resource limitations, even if we are to put the problem complexity aside. Cloud computing clients are not the same with respect to their QoS expectations.

Furthermore, the impact of the job execution violation on the QoS differs from job to another. There are computing jobs that can tolerate some degree of execution violation, however, there are other jobs that are tightly coupled with mission-critical obligations or user experience. These jobs tend to be intolerant to execution delays. SLAs tend to provide a context based on which differential job treatment regimes can be devised. The impact of job violation on QoS tends to be captured in a penalty model. In this work we propose to leverage this model to influence scheduling in a multi-tier cloud computing environment so as to minimize penalty payable by the service provider and as a result attain a pragmatic QoS.

3. SLA DRIVEN JOB SCHEDULING

We consider a multi-tier cloud computing environment consisting of N sequential tiers:

$$T = \{T_1, T_2, T_3, ..., T_N\} \tag{1}$$

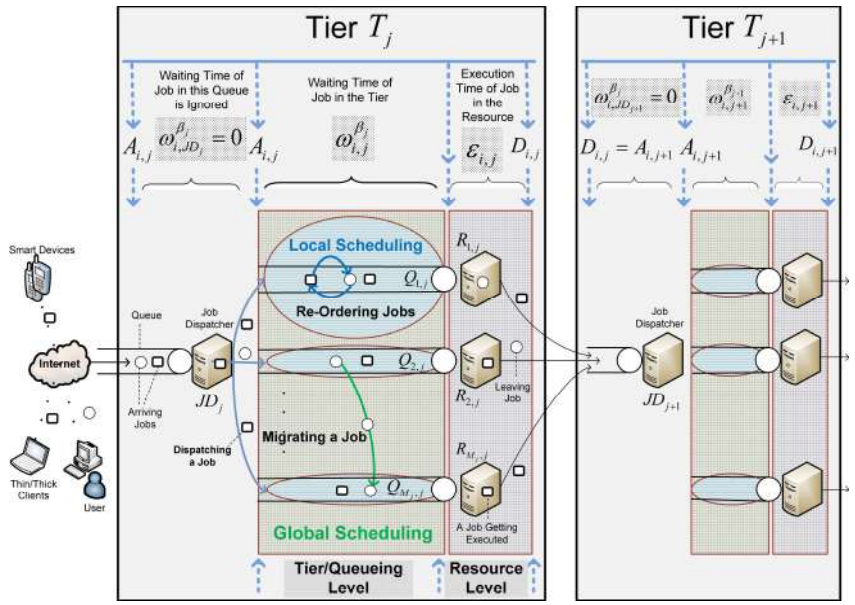


Figure 1. System Model of the Multi-Tier Environment

Each tier T_j employs a set of identical computing resources R_j:

$$R_j = \{R_{1,j}, R_{2,j}, R_{3,j}, ..., R_{M_j,j}\} \tag{2}$$

Each resource $R_{k,j}$ employs a queue $Q_{k,j}$ to hold jobs waiting for execution by the resource. Jobs with different computational requirements are submitted to the environment. It is assumed that these jobs are submitted by different clients and hence are governed by various SLA's. Jobs arrive at the environment in streams. Job J_i arrives at the environment before job J_{i+1}. Jobs arrive in a random manner. $A_{i,j}$ is the arrival time of Job J_i at tier T_j; $\mathcal{E}_{i,j}$ is its prescribed execution time at this tier.

Jobs arriving at tier T_j are queued for execution based on an ordering β_j. As shown in Figures 1 and 2, each tier T_j of the environment consists of a set of resources. Each resource has a queue to hold jobs assigned to it. For instance, resource $R_{1,j}$ of tier T_j is associated with queue $Q_{1,j}$, which consists of 4 jobs (J_6, J_7, J_8, and J_{10}) waiting for execution. A virtual-queue is a cascade of all queues of a given tier. The total execution time E_i of job J_i is defined as

$$E_i = \sum_{j=1}^{N} \mathcal{E}_{i,j} \tag{3}$$

Job J_i's response time Z_i is a function of its total execution time E_i and waiting time W_i, which in turn is dependent on its position in the queues as it progresses from one tier to the next:

$$Z_i = \sum_{j=1}^{N} (\mathcal{E}_{i,j} + \omega_{i,j}^{\beta_j}) = E_i + W_i \tag{4}$$

where $\omega_{i,j}^{\beta_j}$ represents the waiting time of job J_i at tier T_j; β_j is the ordering that governs the order of execution of jobs at tier T_j. W_i is the total time job J_i waits at all tiers. Job J_i departs T_j at time $D_{i,j}$.

We assume a service level agreement that stipulates a penalty amount as an exponential function of the difference between the prescribed response time and the actual response time.

$$\begin{aligned} \varrho_i &= \chi * (1 - \mathrm{e}^{-\nu(Z_i - E_i)}) \\ &= \chi * (1 - \mathrm{e}^{-\nu(W_i)}) \\ &= \chi * (1 - \mathrm{e}^{-\nu \sum_{j=1}^{N} \omega_{i,j}^{\beta_j}}) \end{aligned} \tag{5}$$

where χ is a monitory cost factor and ν is an arbitrary scaling factor. The total penalty cost associated with a set of jobs $J_1 \ldots J_l$, across all tiers is defined as:

$$\varphi = \sum_{i=1}^{l} \varrho_i \tag{6}$$

The objective is to find optimal set of orderings $\beta = (\beta_1, \beta_2, \beta_3, \ldots, \beta_N)$ such that the total penalty cost φ is minimum:

$$\underset{\beta}{\text{minimize}}(\varphi) \equiv \underset{\beta}{\text{minimize}}(\sum_{i=1}^{l} \sum_{j=1}^{N} \omega_{i,j}^{\beta_j}) \tag{7}$$

β_j is an ordering of the jobs waiting at the virtual queue of tier T_j.

4. MINIMUM PENALTY JOB SCHEDULING: A GENETIC ALGORITHM FORMULATION

The paper is concerned with scheduling the client jobs for execution on the computing resources. A job is first submitted to tier-1 for execution by one of the resources of the tier. It is desired that the jobs are scheduled in such a way that minimizes the total waiting time. Finding a job scheduling that yields minimum total waiting time is an NP problem. Given the volume of cloud jobs to be scheduled and the computational complexity of the job scheduling problem, it is prohibitive to seek an optimal solution for the job scheduling problem using exhaustive search techniques. Thus, a meta-heuristic search strategy, such as Permutations Genetic Algorithms (PGA), is a viable option for exploring and exploiting the large space of scheduling permutations [23]. Genetic algorithms have been successfully adopted in various problem domains [24]. They have undisputed success in yielding near optimal solutions for large scale problems, in reasonable time [20].

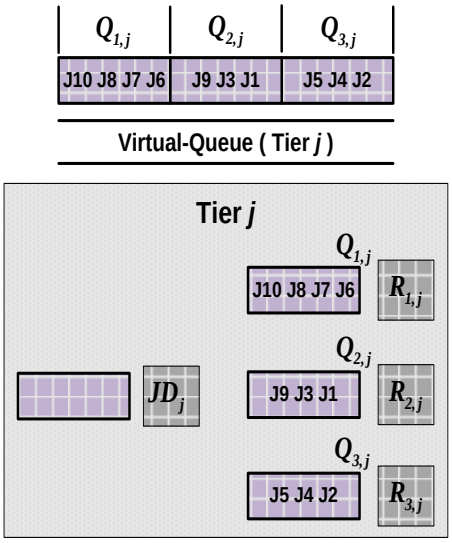


Figure 2. The Virtual-Queue of a Tier j

Scheduling cloud jobs entails two steps: 1) allocating/distributing the jobs among the different tier resources. Jobs that are allocated to a given resource are queued in the queue of that resource; 2) ordering the jobs in the queue of the resource such that their total waiting time is minimum. What makes the problem increasingly harder is the fact that jobs continue to arrive at the tier, while the prior jobs are waiting in their respective queues for execution. Thus, the scheduling process needs to respond to the job arrival dynamics to ensure that job execution at all tiers remains waiting-time optimal. To achieve this, job ordering in each queue should be treated as a continuous process. Furthermore, jobs should be migrated from one queue to another so as to ensure balanced job allocation and maximum resource utilization. Thus, we introduce two operators for constructing optimal job schedules at the tier level:

- The *reorder* operator is used to change the ordering of jobs in a given queue so as to find an ordering that minimizes the total waiting time of all jobs in the queue.
- The *migrate* operator, on the other hand, is used to exploit the benefits of moving jobs between the different resources of the tier so as to reduce the total waiting time at the tier level. This process is adopted at each tier of the environment.

However, implementing the *reorder/migrate* operators in a PGA search strategy is not a trivial task. This implementation complexity can be relaxed by virtualizing the queues of each tier into one virtual queue. The virtual queue is simply a cascade of the queues of the resources of the tier. In this way we converge the two operators into simply a reorder operator. Furthermore, this simplifies the PGA solution formulation. A consequence of this abstraction is the length of the

permutation chromosome and the associated computational cost. This virtual queue will serve as the chromosome of the solution. An index of a job in this queue represents a gene. The ordering of jobs in a virtual queue signifies the order at which the jobs in this queue are to be executed by the resource associated with that queue. Solution populations are created by permuting the entries of the virtual queue, using the *order* and *migrate* operators. The virtual-queue in Figures 2 and 3 of the j^{th} tier has three queues ($Q_{1,j}$, $Q_{2,j}$, and $Q_{3,j}$) cascaded to construct one virtual queue.

4.1. Evaluation of Schedules

A fitness evaluation function is used to assess the quality of each virtual-queue realization (chromosome). The fitness value of the chromosome captures the cost of a potential schedule. The fitness value $f_{r,G}$ of a chromosome r in generation G is represented by the total waiting time of jobs that remain in the virtual queue.

$$f_{r,G} = \sum_{i=1}^{l} (\omega_{i,j}^{\beta_j}) \tag{8}$$

The waiting time $\omega_{i,j}^{\beta_j}$ of the i^{th} job waiting in the virtual queue of the j^{th} tier should be calculated based on its order in the queue, as per the ordering β_j.

The normalized fitness value of each schedule candidate is computed as follows:

$$f_r = \frac{f_{r,G}}{\sum_{C=1}^{n} (f_{C,G})}, \quad r \in C \tag{9}$$

Based on the normalized fitness values of the candidates, the Russian Roulette is used to select a set of schedule candidates to produce the next generation population, using the combination and mutation operators.

4.2. Evolving the Scheduling Process

To evolve a new population that holds new scheduling options for jobs in resource queues of the tier, the crossover and mutation genetic operators are both applied on randomly selected schedules (virtual queues) of the current generation. The crossover operator produces a new generation of virtual-queues from the current generation. The mutation operator applies random changes on a selected set of virtual-queues of the new generation to produce altered virtual-queues. These operators diversify the search direction into new search spaces to avoid getting stuck in a locally

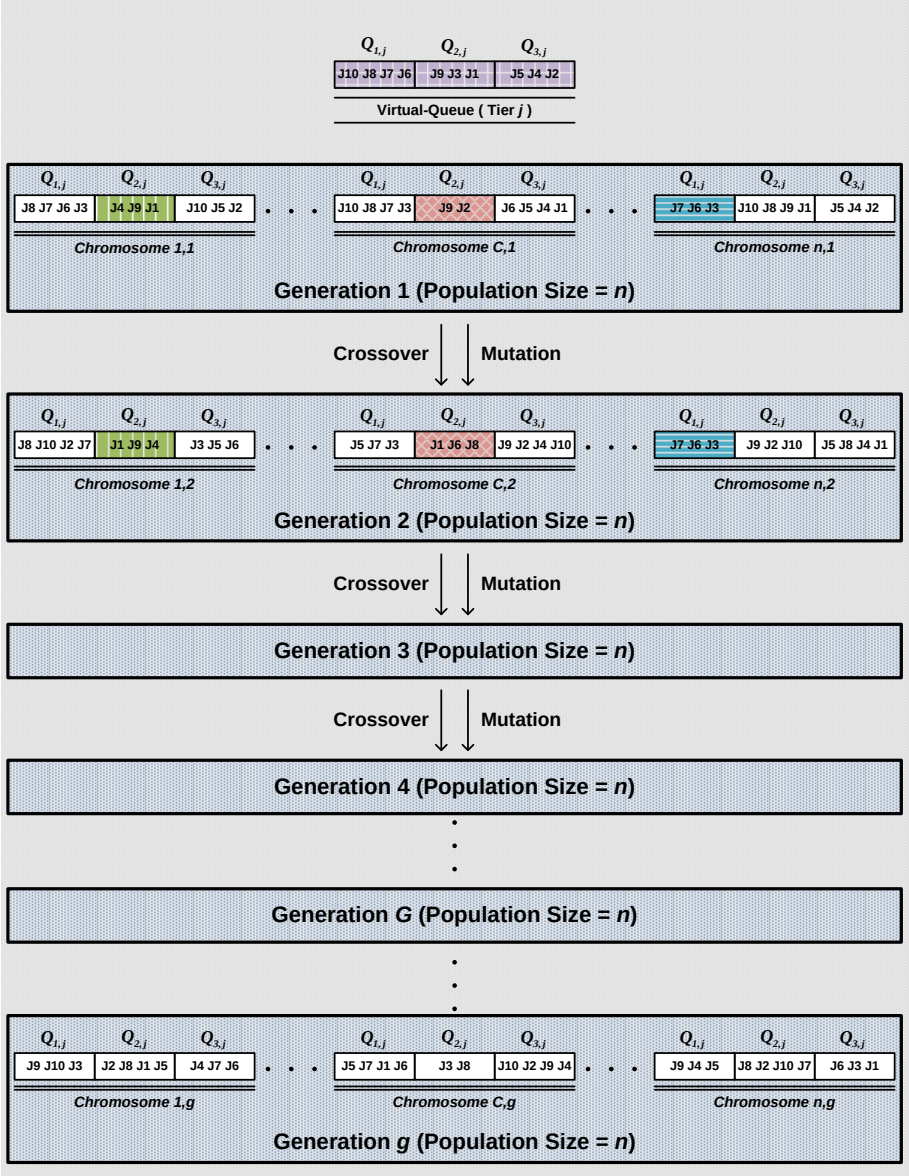


Figure 3. A Tier-based Genetic Approach on the Virtual-Queue

optimum solution. Overall, the *Single-Point* crossover and *Insert* mutation genetic operators are used in this paper. The rates of crossover and mutation operators are both set to be 0.1 of the population size in each generation.

Figure 3 explains how each virtual-queue in a given generation are evolved to create a new virtual-queue of the next generation, using the crossover and mutation operators. Each chromosome (virtual-queue) represents a new scheduling of jobs. The jobs and their order of execution on the resource will be reflected by the segment of the virtual queue corresponding to the actual queue associated with the resource. As a result of the evolutionary process, each segment of the virtual queue corresponding to an actual queue will be in one of the following states:

- Maintain the same set and the same ordering of jobs as in the previous generation.
- A new ordering for the same set of jobs as in the previous generation.
- A different set of jobs and their associated ordering.

For instance, queue $Q_{1,j}$ of *Chromosome* (n,1) in the first generation maintains exactly the same set and order of jobs in the second generation shown in queue $Q_{1,j}$ of *Chromosome* (n,2). In contrast, queue $Q_{2,j}$ of *Chromosome* (1,1) in the first generation maintains the same set of jobs in the second generation, yet has got a new order of jobs as shown in queue $Q_{2,j}$ of *Chromosome* (1,2). Finally, queue $Q_{2,j}$ of a random *Chromosome* (C,1) in the first generation has neither maintained the same set nor got the same order of jobs in the second generation shown in queue $Q_{2,j}$ of *Chromosome* (C,2), which in turn would yield a new scheduling of jobs in the queue of resource $R_{2,j}$ if *Chromosome* (C,2) is later selected as the best chromosome of the tier-based genetic solution.

5. EXPERIMENTAL WORK AND DISCUSSIONS ON RESULTS

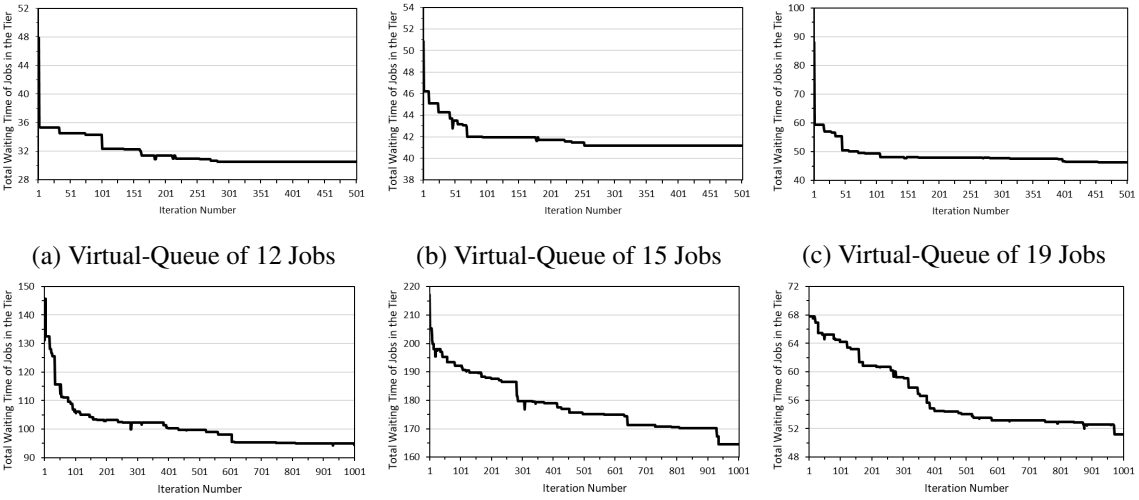
The cloud environment adopted in this paper consists of two tiers, each of which has 3 computing resources. The jobs generated into the cloud environment are atomic and independent of each other. A job is first executed on one of the computing resources of the first tier and then moves for execution on one of the resources of the second tier. Each job is served by only one resource at a time, the scheduling strategy is non-preemptive.

Jobs arrive to the environment at the first tier and are queued in the arrival queue (tier dispatcher) of the environment. The arrival behaviour is modeled as a Poisson process. The running time of each job in a computing resource is assumed to be known in advance, generated with a rate $\mu = 1$ from the exponential distribution function exp($\mu = 1$) [25]. In each tier T_j, job migrations from a queue to another queue are permitted.

Two experiments are conducted. In the first experiment, we take advantage of the virtualized queue, and seek optimal schedules that produce minimum total waiting time among all jobs. Thus, the proposed genetic algorithm operates on all queues of the tier simultaneously. In the second experiment we apply the genetic algorithm on the individual queues of the tier. The penalty exponential scaling parameter ν is set to be $\nu = 0.01$, it is an arbitrary number used to visualize the penalty under different scheduling scenarios. In both experiments, we employ 10 chromosomes populations.

5.1. Virtualized Queue Experiment

The tier-based genetic solution is applied on the *virtualized-queue*. The virtual-queue starts with an initial state that represents an initial scheduling β_j of jobs in the tier (initial tier-state), which in turn yields an initial fitness and penalty of the virtual-queue. The initial fitness of the virtual-queue represents the total waiting time of jobs in the tier according to their initial scheduling in the virtual-queue. The tier-based genetic solution shown in Figure 3 is then applied on the virtual-queue (*globally* at the tier level of the environment), which after some iterations finds a new enhanced scheduling of jobs in the virtual-queue (enhanced tier-state) that optimizes the objective function. The new enhanced tier-state yields a new improved fitness and penalty of the virtual-queue, which in turn is translated into a new enhanced scheduling of jobs in the resource queues of the tier that reduces the total waiting time and penalty of jobs *globally* at the tier level of the environment.



(a) Virtual-Queue of 12 Jobs (b) Virtual-Queue of 15 Jobs (c) Virtual-Queue of 19 Jobs

(d) Virtual-Queue of 31 Jobs (e) Virtual-Queue of 32 Jobs (f) Virtual-Queue of 27 Jobs

Figure 4. Tier-based Scheduling

The results shown in Table 1 and Figure 4 demonstrate the effectiveness of using the queue virtualization along with the tier-based genetic solution to reduce the total waiting time and thus the QoS violation penalty. The results of applying the tier-based genetic solution are reported in 6 different instances. Figures 4a-4c are mapped to their corresponding first 3 instances of Table 1. For the virtual-queue of 19 jobs shown in Table 1, the results show that the tier-based genetic solution has improved the fitness of the tier-state by 47.39%, reducing the total waiting time of jobs at each tier of the environment from 88.0743 time units for the initial tier-state to 46.3381 time units for the enhanced tier-state. The penalty amount has also been improved by 36.66%, reducing it from 0.586 for the initial tier-state to 0.371 for the enhanced tier-state.

Table 1. Tier-based Scheduling

	Virtual-Queue[1]	Initial[2]		Enhanced[3]		Improvement	
	Length	Waiting	Penalty	Waiting	Penalty	Waiting %	Penalty %
Figure4a	12	47.8462	0.380	30.4821	0.263	36.29%	30.90%
Figure4b	15	50.8813	0.399	41.1748	0.338	19.08%	15.37%
Figure4c	19	88.0743	0.586	46.3381	0.371	47.39%	36.66%
Figure4d	31	126.4679	0.718	94.0426	0.610	25.64%	15.07%
Figure4e	32	217.1755	0.886	164.4844	0.807	24.26%	8.92%
Figure4f	27	63.0545	0.468	51.2031	0.401	18.80%	14.32%

[1] **Virtual-Queue Length** represents the total number of jobs in queues of the tier. For instance, the first entry of the table (12) means that the 3 queues of the tier all together contain 12 jobs.

[2] **Initial Waiting** represents the total waiting time of jobs in the virtual-queue according to the initial scheduling of jobs before using the tier-based genetic solution.

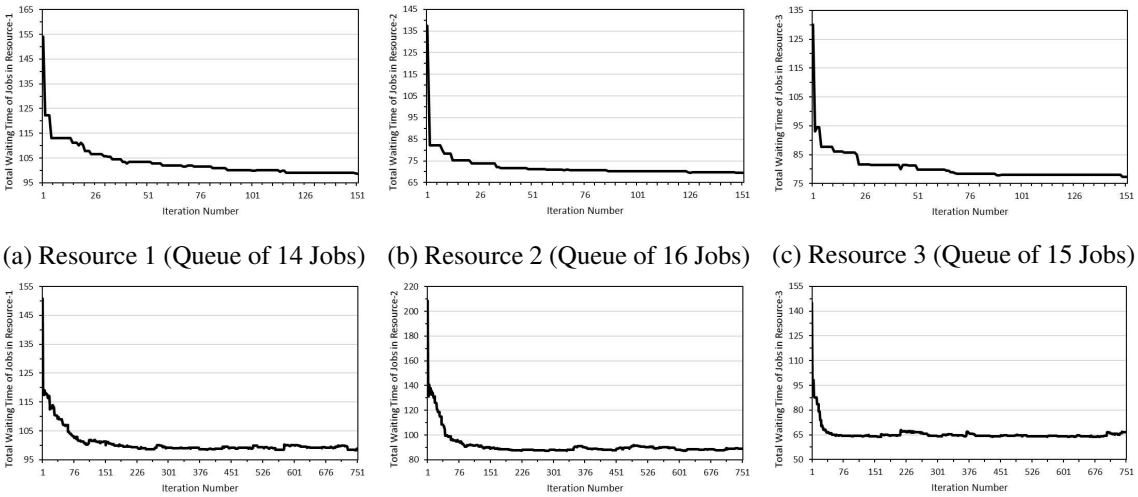
[3] **Enhanced Waiting** represents the total waiting time of jobs in the virtual-queue according to the final/enhanced scheduling of jobs found after using the tier-based genetic solution.

Figure 4c demonstrates the effectiveness of the tier-based genetic solution in reducing the total waiting time of jobs in the virtual-queue of 19 jobs. The tier-based genetic solution has required 500 iterations, each of which contains 10 chromosomes, to achieve the reported enhancement on the tier-state. A total of only 5000 *global* scheduling options for jobs in the tier is effectively explored in the search space of 19! (approximately 1.22×10^{17}) different *global* scheduling options at the tier level of the environment to improve the fitness and penalty of the tier-state by 47.39% and 36.66%, respectively. Similarly, improvements are achieved with respect to the other 2 instances of the virtual-queue (12 and 15 jobs) shown in Table 1. Figures 4a and 4b, respectively, depict such improvement.

In contrast, Figures 4d-4f are mapped to the second and third instances reported in Table 1. The tier-based genetic solution has required 1000 iterations, each of which contains 10 chromosomes, to obtain the enhancement on the tier-state of each event. In this case, a virtual-queue of a large number of jobs has required more iterations so as to explore more *global* scheduling options of the jobs at the tier level of the environment. For the virtual-queue of 31 jobs shown in Table 1, the tier-based genetic solution has improved the performance of the tier by 25.64% and 15.07%, respectively. Figure 4d shows that a total of only 10,000 out of 31! (approximately 8.22×10^{33}) possible *global* scheduling options for jobs at the tier level of the environment are effectively explored to achieve the latter enhancements. Similarly, performance improvements are achieved with respect to the other 2 instances of the virtual-queue (32 and 27 jobs) shown in Table 1, and their corresponding performance are depicted in Figures 4e and 4f, respectively.

5.2. Segmented Queue Experiment

The genetic solution is applied at *each individual queue* level. Each one of the three queues holds an initial set of jobs to be executed on the resource associated with that queue. The waiting time of each job is calculated based on its position in the queue. The proposed genetic algorithm is then used to seek an optimal ordering of the jobs that are queued for execution by the resource associated with that queue, such that the total waiting time of these jobs is minimized. The genetic algorithm in this case seeks an optimal schedule in a reduced search space, since the optimal ordering is sought on each queue individually. In other words, a genetic search strategy is performed on each queue. The total waiting time, of all jobs in the three queues, are computed.



(a) Resource 1 (Queue of 14 Jobs) (b) Resource 2 (Queue of 16 Jobs) (c) Resource 3 (Queue of 15 Jobs)

(d) Resource 1 (Queue of 19 Jobs) (e) Resource 2 (Queue of 23 Jobs) (f) Resource 3 (Queue of 14 Jobs)

Figure 5. Queue-based Scheduling

Table 2 shows the results of applying the genetic algorithm on the three resource queues, in two different instances. The first instance represents a job allocation whereby resource-1 is allocated 14 jobs, resource-2 16 jobs, and resource-3 15 jobs. The second instance represents a job allocation whereby resource-1 is allocated 19 jobs, resource-2 23 jobs, and resource-3 14 jobs. Table 2 enumerates the total number of *local* orderings (schedules) for the first instance. There are $14!$ possible orderings for queue-1, $16!$ for queue-2, and $15!$ for queue-3.

The table shows a 36.04% improvement from the initial ordering for queue-1, a reduction from 154.1339 time units of total waiting time to 98.5818 time units of total waiting time. The QoS violation penalty has improved by 20.24%, from 0.786 due to the initial ordering, to 0.627 due to the improved ordering computed by the genetic search strategy.

Figure 5a depicts the total waiting time of jobs allocated to resource-1 during the search process.

Table 2. Queue-based Scheduling

	Queue[4]	Initial[5]		Enhanced[6]		Improvement	
	Length	Waiting	Penalty	Waiting	Penalty	Waiting %	Penalty %
Resource 1 Figure5a	14	154.1339	0.786	98.5818	0.627	36.04%	20.24%
Resource 2 Figure5b	16	137.3684	0.747	69.4641	0.501	49.43%	32.95%
Resource 3 Figure5c	15	130.0566	0.728	77.3358	0.539	40.54%	25.99%
Resource 1 Figure5d	19	150.8208	0.779	98.1834	0.625	34.90%	19.69%
Resource 2 Figure5e	23	208.596	0.876	87.2667	0.582	58.16%	33.53%
Resource 3 Figure5f	14	145.0253	0.765	63.8502	0.472	55.97%	38.35%

[4] **Queue Length** represents the number of jobs in the queue of a resource.

[5] **Initial Waiting** represents the total waiting time of jobs in the queue according to the initial scheduling of jobs before using the queue-based genetic solution.

[6] **Enhanced Waiting** represents the total waiting time of jobs in the queue according to the final/enhnaced scheduling of jobs found after using the queue-based genetic solution.

After 150 genetic iterations, an optimal solution was found. Each iteration 10 chromosomes are used to evolve the optimal schedule. Thus, 1500 orderings are constructed and genetically manipulated throughout the search process, as apposed to 14!, if we were to employ a brute-force search strategy. Similar observations are in order with respect to resource-2 and resource-3, as can be seen in the figure.

Table 2 reveals the magnitude of search space growth as a result of increasing the number of jobs allocated a given resource. For example, if we consider the impact of increasing the number of jobs allocated to resource-1 from 14 jobs to 23 jobs. In a brute-force search strategy, the search space will increase from 14! to 23!. In contrast, the genetic search strategy needed to expand the search space from 1500 populations to 7500 populations. After 7500 genetic iterations the waiting time was improved by 58.16% from the initial ordering. The total waiting time of jobs was reduced from 208.596 waiting time units due to the initial job ordering to 87.2667 waiting time units due to the genetically improved ordering. Figures 5d-5f demonstrate the effectiveness of using the queue-based genetic solution to decrease the total waiting time of jobs in the three resources: resource-1, resource-2, and resource-3, respectively.

5.3. Comparison

Figure 6 and Table 3 contrast the performance of both genetic strategies, i.e, the virtualized queue search strategy and the individualized queue strategy. The initial orderings of the three queues,

Table 3. Total Waiting Time of Jobs in each Approach

Virtualized Queue	Segmented Queue	WLC	WRR
1961.34	2464.61	3001.82	3617.95

and by implication, that of the virtualized queue are the same. WRR's based ordering entailed 3617 units of total waiting time. WLC's based ordering entailed 3001 units of total waiting time. The individualized queue genetic search strategy was produced an ordering that entails 2464 units of waiting time, a 32% reduction compared to the WRR strategy and 18% reduction compared to the WLC strategy. The virtualized queue genetic search strategy produced an ordering that entails 1961 units of waiting time. That is a reduction of 46% compared to he WRR strategy and 35% reduction compared to the WLC strategy.

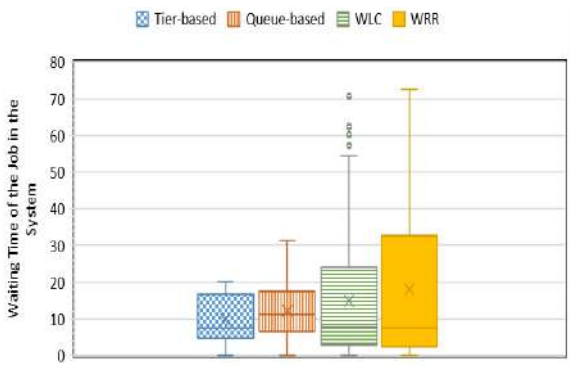


Figure 6. Maximum Waiting Time Performance Comparison

Figure 6 depicts the average waiting performance of the four scheduling strategies. The virtualized queue genetic strategy has produced the shortest average waiting time per job, with an average waiting time of 10 time units. The individualized queue search strategy produced an average waiting time of 13 time units. The WRR and WLC job ordering strategies delivered inferior performance.

On the other hand, the individualized queue strategy has yielded a maximum job waiting time of 19 time units. The WRR produced a maximum job waiting time of 32 time units, while in the WLC produced a maximum job waiting time of 24. The virtualized queue scheduling strategy delivered a maximum job waiting time of 16 time units. Overall, the virtualized queue scheduling strategy delivered the best performance in minimizing the total waiting time and thus the lowest QoS penalty.

6. CONCLUSION

This paper presents a genetic algorithm for tackling the job scheduling problem in a multi-tier cloud computing environment. The paper makes the connection between penalties payable due to QoS violations and job waiting time. This connection establishes a framework for facilitating penalty management and mitigation that service providers can utilize in high demand/limited resources situations. It is assumed that each tier of the environment consists of a set of identical computing resources. A queue is associated with each one of these resources. To achieve maximum resource utilization and minimum waiting time, a virtualized queue abstraction is proposed. Each virtual queue realization represents an execution ordering of jobs. This virtualized queue abstraction collapses the search spaces of all queues into one search space of orderings, and thus allowing the genetic algorithm to seek optimal schedules at the tier level. The paper presented experimental work to investigate the performance of the proposed biologically inspired strategy to WRR and WLC, as well as an individualized queue strategy. It is concluded that the proposed job scheduling strategy delivers performance that is superior to that of both WRR and WLC. The genetic search strategy when applied at the individual queue delivers performance also superior to that of WRR and WLC. However, the genetic search strategy applied at the virtual queue still delivered the best performance compared to all the other search strategies.

7. FUTURE WORK

The proposed scheduling strategy does not contemplate the impact of schedules optimized in a given tier on the performance of schedules on the subsequent tiers. Therefore, it is the intent of the authors to expand the work reported in this paper to investigate such impact and to extend the algorithms proposed in this paper so as to mitigate the impact of tier dependency. Furthermore, the formulation presented in this paper treats the penalty factor of each job as a function of time to be identical. Typically, cloud computing jobs tend to vary with respect to the QoS violation penalties. Therefore, it is imperative to modify the penalty model so as to reflect such sensitivity so as to force the scheduling process to produce minimum penalty schedules, and not necessarily minimum total waiting time schedules.

REFERENCES

[1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications*, vol. 1, no. 1, pp. 7–18, 2010.

[2] Y. Jadeja and K. Modi, "Cloud computing - concepts, architecture and challenges," in *Proceedings of the International Conference on Computing, Electronics and Electrical Technologies*, March 2012, pp. 877–880.

[3] K. Aida, "Effect of job size characteristics on job scheduling performance," in *Proceedings of the Workshop on Job Scheduling Strategies for Parallel Processing*, May 2000, pp. 1–17.

[4] H. J. Moon, Y. Chi, and H. Hacigumus, "Performance evaluation of scheduling algorithms for database services with soft and hard SLAs," in *Proceedings of the Second International Workshop on Data Intensive Computing in the Clouds*, November 2011, pp. 81–90.

[5] G. Stavrinides and H. Karatza, "The effect of workload computational demand variability on the performance of a SaaS cloud with a multi-tier SLA," in *Proceedings of the Fivth IEEE International Conference on Future Internet of Things and Cloud*, August 2017, pp. 10–17.

[6] H. Shoja, H. Nahid, and R. Azizi, "A comparative survey on load balancing algorithms in cloud computing," in *Proceedings of the International Conference on Computing, Communication and Networking Technologies*, July 2014, pp. 1–5.

[7] E. Ghomi, A. Rahmani, and N. Qader, "Load-balancing algorithms in cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 50–71, 2017.

[8] A. Arunarani, D. Manjula, and V. Sugumaran, "Task scheduling techniques in cloud computing: A literature survey," *Future Generation Computer Systems*, vol. 91, pp. 407–415, 2019.

[9] B. Schroeder and M. Harchol-Balter, "Evaluation of task assignment policies for supercomputing servers: The case for load unbalancing and fairness," *Journal of Cluster Computing*, vol. 7, no. 2, pp. 151–161, 2004.

[10] G. Liu, J. Li, and J. Xu, "An improved Min-Min algorithm in cloud computing," in *Proceedings of the International Conference of Modern Computer Science and Applications*, May 2013, pp. 47–52.

[11] X. Li, Y. Mao, X. Xiao, and Y. Zhuang, "An improved Max-Min task-scheduling algorithm for elastic cloud," in *Proceedings of the International Symposium on Computer, Consumer and Control*, June 2014, pp. 340–343.

[12] V. Gupta, M. Harchol-Balter, K. Sigman, and W. Whitt, "Analysis of join-the-shortest-queue routing for web server farms," *Performance Evaluation*, vol. 64, no. 9–12, pp. 1062–1081, 2007.

[13] L. Kang and X. Ting, "Application of adaptive load balancing algorithm based on minimum traffic in cloud computing architecture," in *Proceedings of the International Conference on Logistics, Informatics and Service Sciences*, July 2015, pp. 1–5.

[14] W. Wang and G. Casale, "Evaluating weighted round robin load balancing for cloud web services," in *Proceedings of the International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, September 2014, pp. 393–400.

[15] Y. Lu, Q. Xie, G. Kliot, A. Geller, J. Larus, and A. Greenberg, "Join-Idle-Queue: A novel load balancing algorithm for dynamically scalable web services," *Performance Evaluation*, vol. 68, no. 11, pp. 1056–1071, 2011.

[16] P. Samal and P. Mishra, "Analysis of variants in round robin algorithms for load balancing in cloud computing," *International Journal of Computer Science and Information Technologies*, vol. 4, no. 3, pp. 416–419, 2013.

[17] K. Boloor, R. Chirkova, T. Salo, and Y. Viniotis, "Heuristic-based request scheduling subject to a percentile response time SLA in a distributed cloud," in *Proceedings of the IEEE Global Telecommunications Conference*, December 2010, pp. 1–6.

[18] N. Ghumman and R. Kaur, "Dynamic combination of improved max-min and ant colony algorithm for load balancing in cloud system," in *Proceedings of the International Conference on Computing, Communication and Networking Technologies*, July 2015, pp. 1–5.

[19] F. Ramezani, J. Lu, and F. Hussain, "Task-based system load balancing in cloud computing using particle swarm optimization," *International Journal of Parallel Programming*, vol. 42, no. 5, pp. 739–754, 2014.

[20] M. Nouiri, A. Bekrar, A. Jemai, S. Niar, and A. Ammari, "An effective and distributed particle swarm optimization algorithm for flexible job-shop scheduling problem," *Journal of Intelligent Manufacturing*, vol. 29, no. 3, pp. 603–615, 2018.

[21] C. Mateos, E. Pacini, and C. Garino, "An ACO-inspired algorithm for minimizing weighted flowtime in cloud-based parameter sweep experiments," *Advances in Engineering Software*, vol. 56, pp. 38–50, 2013.

[22] S. Pandey, L. Wu, S. Guru, and R. Buyya, "A particle swarm optimization-based heuristic for scheduling workflow applications in cloud computing environments," *Proceedings of the IEEE International Conference on Advanced Information Networking and Applications*, pp. 400–407, 2010.

[23] Y. Xiaomei, Z. Jianchao, L. Jiye, and L. Jiahua, "A genetic algorithm for job shop scheduling problem using co-evolution and competition mechanism," in *Proceedings of the International Conference on Artificial Intelligence and Computational Intelligence*, October 2010, pp. 133–136.

[24] X. Li and L. Gao, "An effective hybrid genetic algorithm and tabu search for flexible job shop scheduling problem," *International Journal of Production Economics*, vol. 174, no. 4, pp. 93–110, 2016.

[25] T. Atmaca, T. Begin, A. Brandwajn, and H. Castel-Taleb, "Performance evaluation of cloud computing centers with general arrivals and service," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 8, pp. 2341–2348, 2016.

THREAT MODELLING FOR THE VIRTUAL MACHINE IMAGE IN CLOUD COMPUTING

Raid Khalid Hussein and Vladimiro Sassone

Department of Electronics and Computer Science,
University of Southampton, Southampton, The UK

ABSTRACT

Cloud computing is one of the most smart technology in the era of computing as its capability to decrease the cost of data processing while increasing flexibility and scalability for computer processes. Security is one of the core concerns related to the cloud computing as it hinders the organizations to adopt this technology. Infrastructure as a service (IaaS) is one of the main services of cloud computing which uses virtualization to supply virtualized computing resources to its users through the internet. Virtual Machine Image is the key component in the cloud as it is used to run an instance. There are security issues related to the virtual machine image that need to be analysed as being an essential component related to the cloud computing. Some studies were conducted to provide countermeasure for the identify security threats. However, there is no study has attempted to synthesize security threats and corresponding vulnerabilities. In addition, these studies did not model and classified security threats to find their effect on the Virtual Machine Image. Therefore, this paper provides a threat modelling approach to identify threats that affect the virtual machine image. Furthermore, threat classification is carried out to each individual threat to find out their effects on the cloud computing. Potential attack was drawn to show how an adversary might exploit the weakness in the system to attack the Virtual Machine Image.

KEYWORDS

Cloud Security, Virtualization, Virtual Machine Image, Security Threats.

1. INTRODUCTION

Cloud computing is a paradigm that enable its users to access infrastructure, platform and software resources as services without owning, managing or maintaining the resources. Infrastructure as a service (IaaS) delivers hardware services to users' applications such as OpenStack, Amazon web services and google cloud platform using virtualization. IaaS provides and maintain a catalog that list the available virtual machines images (VMI). The VMI may include operating system like windows, Linux or Fedora and might contains other resources like applications that are created by organization such as database management system or application server[1]. There are some security issues associated with VMI in cloud computing that has harmful impact on the security of the cloud and might affect confidentiality, integrity or availability[2]. Threat modelling is conducted to identify security threats and draw possible routes threats might follow to attack the VMI. Furthermore, threat modelling distinguishes the area where the VMI is stored, classify threats based on their unwanted effect and detect the agent of the threats which is the objective of this paper.

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 119-132, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90911

Threat modelling process involves three high-level steps: Firstly, characterizing the system which represents cloud computing platform that was used to achieve the threat modelling. Secondly identifying threats, which represent threats that identified in the academic literature related to VMI. Finally, identifying assets and access point that represent the area threat modelling was achieved in the cloud platform. The identified threats were classified based on their effect on security. STRIDE model is used to classify the identified threats developed by Microsoft for threat modelling [3]. Beside threat modelling, it is essential to take into consideration who is conducting the attack and what type of skills is needed to achieve the attack on the identified assets. Therefore, threat agent was identified for the context of VMI. Potential attacks was drawn to show the possible attacks that an adversary might follow to attack the VMI by exploiting the system vulnerabilities.

2. RELATED WORK

There are a number of studies were conducted to detect security threats and draw countermeasures to secure the VMI. An image management system (IMS) was designed to control the access to the VMI , track its provenance, provides image filters and scanners for both users and administrators to detect threats and repair security issues. The drawback of this system is that image filters for detecting and fixing security violation was not accurate 100% to remove private information like password or illegal software like pirated software from the image before publishing it. In addition, the virus scanner does not assure to detect all the malicious software in the image. This study identified unauthorized access, leak of sensitive information, malware and non-compliance as security threats that need to be considered[4].

Kazim, Masood and Shibli (2013) suggested Encrypted Virtual Disk Images in Cloud (EVDIC) to secure the VMI. Their idea was to encrypt the VMI whenever it is terminated to avoid security threats that might attack the VMI when it is dormant. EVDIC could provide security from malicious software or malwares. The proposed system EVDIC could identify compromised disk image, unauthorized access and data leakage as security threat.

Schwarzkopf et al. (2012) demonstrated a technique to detect outdated software in VMIs and to scan for security vulnerabilities. It includes two components: the Updates checker and online penetration suite. The Update checker is used to find out Linux based virtual machine who in need of update their software. The update checker copy the information about installed packages and save them in the database. The checks for software updates is achieve faster compare to other techniques as installed package is saved in databased whereas, in other systems need to boot the VMI and shut it down after checking for software updates which is time consuming. On the other hand, online penetration suite is used to perform periodic or pre-rollout online scanning of virtual machine for software vulnerabilities. The periodic scan can be achieved in idle times

whereas the pre-rollout online scanning is accomplished before the machine goes live. The scans for software vulnerabilities is accomplished using well know security products. The drawback in this system is the update checker works with Linux only. This study could identify non-compliance as security threats [6].

An Offline Patching Scheme (OPS) could figure out a method to identify VMI with outdated software and patch VMI with latest software update efficiently therefore, it could solve the non-compliance issue. OPS based on two modules, the Collector and Patcher. Collector is used to find

out outdated software in the VMI. Patcher is used to patch the outdated software in the VMI with the latest updates and patches. However, the study has limitation to patch outdated VMI with Window OS. In addition, the system is unwilling to updates snapshots. OPS could identify data leakage and malware as security threats [7].

Another study by Jeswani et al. (2013) which could present ImageElves to detect out-dated software within VMI and patch, install software and check for compliance. This system works in two phases. The first phase is to investigate the target VMI and creates manifest and signature updates. In the second phase, VMIs are taken offline and apply the manifest. This system has advances over other related work as reduce the downtimes due to simultaneously apply the updates to all dormant images. The drawback in this system there might be failed for the higher level applications to function correctly after applying the updates. Furthermore, applying upgrade to VMI files work properly for binary files except there are possibilities to create more equivalent classes than it is necessary. Finally, there is no failure recovery capabilities for the current implementation of Image Elves in case of the system running. This study could figure out non-compliance as security threat[8].

3. THREAT MODELLING

Threat modelling is a procedure used to identify and address security threats associated with different assets in the system. Threat modelling is used to locate security threats and identify mechanisms to protect the cloud services. Threat modelling is used to study the cloud service and classified the potential threats based on their effect on the cloud. To identify security requirements for the cloud services, threats need to be analysed based on criticality and likelihood. Decisions need to be taken regarding the potential threats related to the cloud services, specifically whether to mitigate the threats or accept the risk associated with the threats. Security of the cloud services was built based on threat modelling and security requirements. Identifying the threats associated with assets in the system helps to develop proper security requirements.

This is essential in case the security requirements are damaged; indeed, this could lead to faults in the security system related to the cloud service. Properly addressing the threats and suitable countermeasures to said threats reduces the ability of the attacker to misuse the cloud service. Threat modelling looks at the cloud services from the attacker

perspective to help the designers to predict the attacker goals or which assets are targeted [9] The threat modelling process consists of the following high-level steps, as shown in Figure 1.

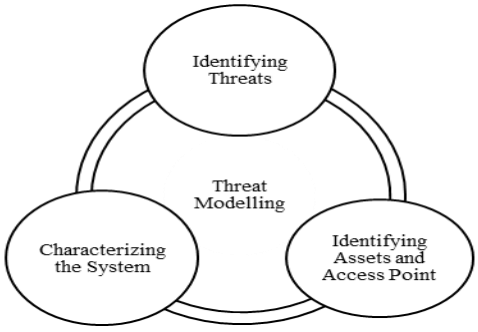


Figure 1 Threat Modelling

3.1 Characterizing the System

With regard to the scenario of OpenStack, which is one of the most popular open source cloud services, it includes the following components: Nova for computing, Glance for image services, Cinder for block storage, Neutron for networking, Keystone for identity services, Swift for object storage and Dashboard to access the cloud services. As shown in Figure 2, the physical network provides access to cloud administrators and cloud users. Firewalls are used to connect cloud administrators to the data centre, as shown in node 17 and node 19. In addition, the cloud administrators are connected to the data centre through an authentication server (host 18) and Nexus 7000 (node 20). The cloud users are connected to the data centre through the multi-layer concept used by Cisco. There are three layers where the cloud users are connected to the data centre. These layers are as follows [10]:

- In Layer 1, node 1 is used to establish connection between the cloud and the internet. Node 2 is used to link the user to the firewall. At the same time, the user, after being connected to the firewall, is connected to two different types of servers: the authentication server (host 3) as well as the DSN and Neutron server (node 4). These servers provide services to end-users and tenants. Following this, node 5, which is Cisco Nexen 7000, is used to route the request to the destination machines.

- In Layer 2, node 6 is a firewall which is used to connect the first layer to the second layer through Nexus 5000 node 7. Nexus 5000 is used to connect the rack server through Nexus 2000. Nexus 5000 is employed to connect servers inside the rack at compute level (hosts 8, 9, 10, 11 and 12).

- In Layer 3, another Nexen 7000 node 13 is used to connect layer 2 to the storage. Node 14 is a firewall which is used to connect Nexus 7000 and MDS 9000.

OpenStack components run on the authentication server in host 3 and host 18. Host 3 is designed for tenants and host 18 is designed for the administrators. In the first run the following components are working: Dashboard, Nova, Neutron, Keystone, Cinder, Swift, Glance and My SQL. In the second run, the same components along with additional components like billing system, which is known as Ceilometer. Node 4 represents the DNS server, which runs the Neutron components; this server provides the address for the machine running a requested service. The Nova is represented by nodes 8, 9, 10, 11 and 12. All physical components run four components: Hypervisor, Nova, Glance and Ceilometer. Finally, all physical machines run ssh for maintenance [11].

3.2 Identifying Threats

In the cloud data centre, as shown in Figure 2, attacks surface represent points when exploited by an attacker could leak information. Attacks surface can be classified into three types; the first attacks surface comes from physical network, which includes the hardware and software components such as servers or OS. The second type of attacks surface which are related to virtualization, such as an attack on hypervisor or virtual switches. The last type of attack surface is related to cloud computing, such as OpenStack components having security issues, e.g. Glance, Neutron, Nova, Ceilometer and keystone. It is obvious that the first attack surface is similar to

those related to the traditional network. On the other hand, attacks surface on the cloud OS and virtualization may also pose new security challenges, as they are unique to the cloud [12].

Attacks surface may come from two sides: attacks from the user side and attacks from the provider side. Let us consider an attack conducted by a user. There are two types of users: first is the normal user who is using the cloud service with the intention of attacking the service of the cloud tenant and its users or cloud providers. Second is a cloud tenant, who aims to attack another cloud tenant and his/her users or cloud provider.

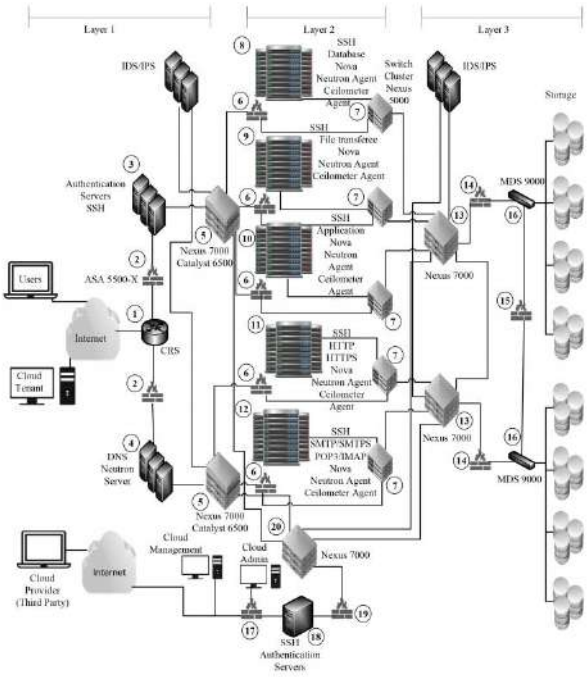


Figure 2 Cloud Data Center Infrastructure [11]

On the other hand, the Cloud provider could conduct another attack on the cloud. Cloud provider refers to the operator, who has privileged access to certain cloud components for maintenance or management, such as routers, switches or firewalls. The Cloud provider could exploit any of the aforementioned types of attacks to leak out information [11].

There are five threats related to the VMI which have been identified in the academic literature related to VMI: malware, data leakage, unauthorized access, compromised disk image and risk of non-compliance [7–11].

- Data leakage represents the intentional or unintentional leaking of sensitive information. This occurs when a user publishes his/her image without removing personal information. Sensitive information could include, for instance, cookies from the internet that can make it possible to extract sensitive information related to the image user.

- Malware are malicious software or virus that is situated inside the memory of VMI. Malware could affect the security of the VMI and might cause serious security issues for

the cloud. The malicious VMI, which includes malware, helps the attacker to bypass the security countermeasures, such as the firewall or the intrusion detection system.

- Unauthorized access is an illegal access to a service without permission. These users could bypass the security mechanisms or use illegitimate accounts to access the VMI and threaten the confidentiality, availability and integrity of the VMI.

- Compromised disk image could be disclosed during the storage stage due to someone installing malicious software on the VMI or someone gaining unauthorized access to the VMI. The disk image is vulnerable to outside attackers, and could also be susceptible to inside attacks such as malicious users or administrators.

- Non-compliance represents storing in a repository, retrieving from a repository or running VMI with expired software or unlicensed Software. This could happen when a dormant image is not patched with the latest software updates or is not scanned for worms or malicious software. Expired software represents software with an expired license and will be detected when the image is active.

3.3 Identifying Assets and Access Point

The identified asset for this research is the VMI. As this research is accomplished on OpenStack, the Glance project is used to save and maintain the VMI in the cloud service. In addition, access points in the scenario of the VMI are achieved through the Glance project, the Nova project and Cinder in OpenStack. The VMI is copied from the Glance project to the local disk inside the compute/Nova project for the purpose of lunching an instance from the VMI. In addition, a flavour needs to be selected as well as additional attributes for the launching of the VM. Flavour represents a set of virtual resources. Flavour identifies the CPU number, RAM amount available and disk size. There are predefined flavours, thus allowing the user to choose the suitable option for their requested instance. The selected flavour provides root volume, which is labelled vda in Figure 3, as well as an additional storage, labelled vdb. Vdb will be deleted once the instance is deleted, as it is an ephemeral disk. Vdc is the virtual disk, which is connected to cinder volume.

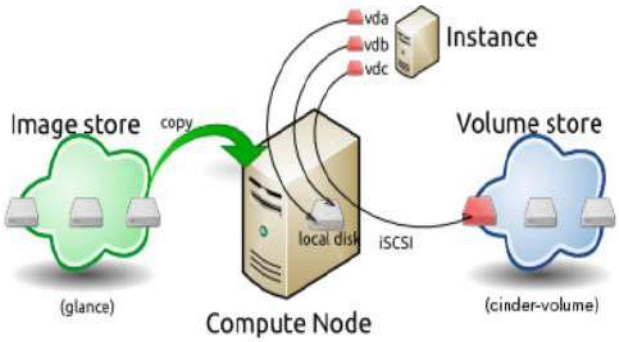


Figure 3 Instance Creation from an Image [13]

Cinder volume is a persistent block storage service provided by OpenStack and can replace the ephemeral storage provided by the instance flavour vdb. The compute project is connected to the

cinder volume through iSCSI. Once the compute node starts to provision the vCPU and memory resources, the instance boots up from the vda (OpenStack, 2018; CVE Details, 2016).

4. THREATS CLASSIFICATION

The identified threats are classified into six types based on their effects. This is achieved using the STRIDE classification model as shown in Figure 4. STRIDE classification can be broken down as follows [18]:

- Spoofing: happens when unauthorised users use the credentials of an authorised user or legitimate user with malicious behaviour trying to gain access to inaccessible assets.

- Tampering: refers to changing the data or operation to perform an attack. Users can change the data or operation which is delivered to them and return said data, therefore manipulating client-side validation.

- Repudiation: pertains to a situation whereby the user could deny his/her activity when there is no sufficient monitoring or recording of his/her activity while he/she is working on the system.

- Information disclosure: occurs when information is exposed to unauthorised users who do not have right to access it.

- Denial of service: a legitimate user is not willing to access a certain service because of malicious software, a lack of internet, or power failure.

- Elevation of privilege: unauthorized users or attacker can elevate their role to a higher privileged role in the information system.

Based on the definition of the identified threats in previous section and the above threats classification, threats are mapped to its equivalent in STRIDE classification model. Data leakage, data breaches or data lost is mapped to information disclosure and tampering as it affects data integrity and confidentiality[19].

Malware is one of security threat that is used by an adversary to attack the VMI through spoofing as the adversary can hide his identity and send malware to victim therefore, malware is linked to spoofing category in STRIDE classification model [20]. In addition, tampering threatens the data integrity or operation flow. The adversary exploits being an authorized user to attachment malware in the system therefore, malware is classified as tampering in STRIDE classification model [21]. Furthermore, Malware might cause denial of service as the service is flooded by requests to initialize instances [22]. Information disclosure is another cause of malware as it is an effect of illegitimate user who exposes data [23].

Unauthorized access is another security threats to the VMI. Spoofing is a method which can be exploited by attacker to perform unauthorized access to the VMI as spoofing permits attackers to hide their identity from the security mechanism and gain unlawful access to the VMI [24]. In addition, information disclosure might be caused by unauthorized access to the VMI from an adversary which exposes data to unauthorized access and affects data confidentiality [25].

Moreover, unauthorized access is mapped to elevation of privilege as an attacker changes the users membership or their privileges [26].

Compromised disk image is a security problem that affects the VMI which is caused by tampering with data [27] or information disclosure[28].

Non-compliance is a security issue for the VMI and needs to be considered. Non-compliance is mapped to Elevation of privilege in the STRIDE threats classification as if the VMI is not updated with latest policies or software updates which might lead to bypass authorization of the system [26].

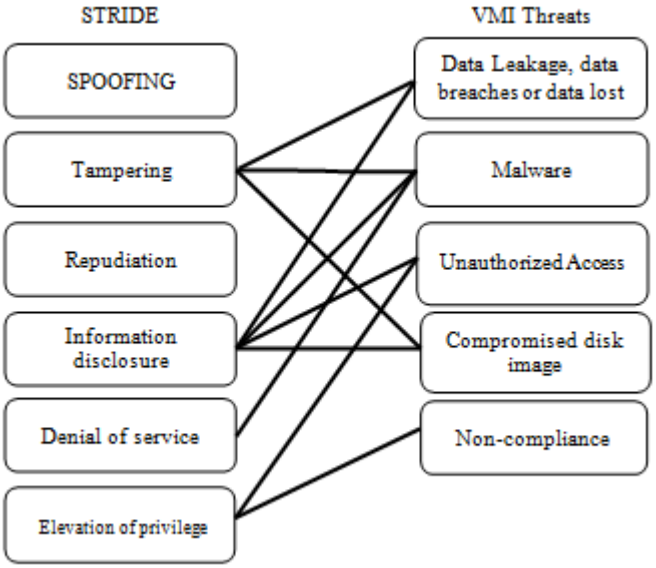


Figure 4 STRIDE Classification for the VMI threats

5. POTENTIAL ATTACK SCENARIOS FOR VMI

There are a number of vulnerabilities in the Glance project, Cinder project and Nova project in OpenStack which could be exploited by an adversary to attack VMIs. Attacks might come from:

- An adversary who has access to the Glance project, which is located in node 3 and node 18. The Glance project represents an entry point. Nova initializes an instance after copying a VMI to the Nova local disk. A malicious user can exploit one of the vulnerabilities, namely CVE-2016-7498 (OpenStack: List of all products and related security vulnerabilities) in Nova; these vulnerabilities are located in nodes 8, 9,10, 11 and 12 and perform an attack. Nova project represents here exit point to leak of information.
- An adversary could exploit one of vulnerabilities, namelyCVE-2015-5162, CVE-2014-7231, CVE-2014-7230, CVE-2014-3641 or CVE-2013-4183 (OpenStack : List of all products and related security vulnerabilities) in the Cinder project; these vulnerabilities are located in node 3 and 18. Exploiting said vulnerabilities would make it possible to perform an attack, as the Cinder volume is used by the Nova project to run an instance. In this case, the Nova or Cinder projects represent an exit point for information disclosure.

- Another possible attack could happen when the cloud tenant uploads the VMI, alongside malicious software, to the Glance project, which is located in node 3 or 18, in order to implement an attack. An infected VMI might have security implications for the security of the cloud and represents an entry point. The malicious cloud tenant could exploit one of the vulnerabilities, namely CVE-2017-7200, CVE-2015-8234, CVE-2015-5163, CVE-2015-3289 or CVE-2013-1840 (OpenStack : List of all products and related security vulnerabilities) in the Glance project to achieve an attack and threaten the security of the cloud; the Glance project therefore represents an exit point.
- The cloud provider can achieve all types of attacks on the VMI as he/she has privileged access to resources in the area between the Glance, Nova and Cinder projects, and can harm the cloud security.

TABLE 1 shows the severity of the vulnerabilities related to Nova, Cinder and Glance projects based on Common Vulnerability Scoring System (CVSS) [30]. In CVSS, the higher score shows the greater probability that the vulnerability could be exploited by an adversary. The 0 score represent the weak or no chance to conduct an attack whereas, 9.0 or 10.0 is very critical risk and can be exploited by an adversary to perform an attack.

Table 1 Nova, Cinder and Glance projects vulnerabilities with CVSS score

CVE number	**NONE**	**LOW**	**MEDIUM**	**HIGH**	**CRITICAL**
	0.0	0.1 - 3.9	4.0 - 6.9	7.0 - 8.9	9.0 - 10.0
Nova project vulnerability cvss score					
CVE-2016-7498	-	-	√	-	-
Cinder project vulnerability cvss score					
CVE-2015-5162	-	-	√	-	-
CVE-2014-7231	-	√	-	-	-
CVE-2014-7230	-	√	-	-	-
CVE-2014-3641	-	-	√	-	-
CVE-2013-4183	-	√	-	-	-
Glance project vulnerability cvss score					
CVE-2017-7200	-	-	√	-	-
CVE-2015-8234	-	-	√	-	-
CVE-2015-5163	-	√	-	-	-
CVE-2015-3289	-	-	√	-	-
CVE-2013-1840	-	√	-	-	-

6. THREAT AGENT

Threat agent is the player who force a threat on the system. It is trying to expose the integrity and confidentiality of the information saved in the system. Threat gent is an act that is made intentionally or unintentionally to destroy the system. Threats agents could be result of the following [31]:

- Natural disaster which comprises fire, flood, lighting or earthquake.
- Terrorists are kinds of threat agents which includes political terrorists, religious terrorists or anarchists.

- Competitors and organized crime that arise from commercial competitors who compete for resources such as a challenger trying to acquire a device firmware to harm its competitor's reputation.
- Thieves are threat agents who are associated with stealing mostly financial or personal data.
- Hackers cloud be group of malicious individual, employees of an organization who may be disgruntled or script kiddies. Hackers tend to use applications and tools that are developed by others such as viruses, worms or phishing.

There are two essential skills which help attackers to achieve an attack: reconnaissance skills and arsenal size. The reconnaissance skills represents the ability of an attacker to synthase accurate information regarding the target system. High reconnaissance skills expend the likelihood that will acquire enough information regards the target system while low reconnaissance skills illustrate that the attacker has no sufficient information to perform successful attack. Arsenal size represents the number of usable exploits at attacker's disposal. The strength of an attacker is evaluated by their ability to acquire or develop a large arsenal of obtainable exploits and reconnaissance skills which help to make a successful attack [32].

In the scenario of VMI, the attacker has sufficient information about OpenStack system. The attacker has a clear idea about where VMI is saved, where an instance is initialized which represent reconnaissance skills. Whereas, vulnerabilities that could be exploited to perform an attack in the projects of Cinder, Nova and Glance projects represents arsenal size. An attacker needs to have certain skills to exploit one of the vulnerabilities in Cinder, Nova or Glance project to perform the attack on the VMI.

To exploit the vulnerability in Nova project:

- The vulnerability namely CVE-2016-7498 (OpenStack: List of all products and related security vulnerabilities) required from the attacker to be logging on the OpenStack project as a legitimate user through command line or via desktop session or web interface. This vulnerability has very low access complexity to be exploited. In this vulnerability, the attacker exploit it to delete the instance while it is in resize state and cause denial of service.

To exploit the vulnerabilities in Cinder project:

- The vulnerability namely CVE-2015-5162, it is required from the attacker to create and upload a crafted disk image with malicious software to cause denial of service. This vulnerability occurs because image parser does not limit the qemu image calls.
- Another vulnerability in Cinder CVE-2014-7231 causes information disclosure when exploited. It is important that the attacker needs to be local user in order to read the log file to obtain the password related to in strutils.mask_password function and can leak information.
- For vulnerability CVE-2014-7230 required the same skills needed in the vulnerability CVE-2014-7231 but, to obtain the password to read the log is acquired from processutils.execute function. This vulnerability causes information disclosure.
- The vulnerability CVE-2014-3641 required form the attacker to be logged to the system through desktop session, command line or web interface. This vulnerability does not require sophisticated knowledge to be exploited. The attacker needs to be remotely

authenticated to obtain data from cinder volume by cloning and attaching the volume to the header of crafted qcow2 header.

- In CVE-2013-4183, the attacker requires to be a local user to obtain sensitive information from snapshot of the VMI. This vulnerability leaks information from clear_volume function in LVM Volume Driver in OpenStack Cinder as it does not clear data properly when deleting the snapshots.

To exploit the vulnerabilities in Glance project:

- The vulnerability CVE-2017-7200, masked network port scan is performed by an attacker using the image Service API v1. It is possible for an attacker to create an image with URL using the v1. The internal network could be monitored by an attacker while appearing masked.
- The vulnerability CVE-2015-8234, it is required from remote authenticated attacker to create a crafted image to bypass the signature verification process in order to attack MD5.
- To exploit the vulnerability CVE-2015-5163, it is required from an attacker to be authenticated as local user to read an arbitrary files through crafted backing file for the qcow2 image to leak information.
- Another vulnerability in Glance project CVE-2015-3289 permits an adversary to cause denial of service through continuously using import task flow API to create images and delete them.
- The vulnerability CVE-2013-1840 in Glance project allows a remote authentication attacker to obtain the operator's backend credentials via request for a cache image.

Table 2 shows the required skills to exploit a certain vulnerability.

Table 2 Skills required by an attacker to exploit a vulnerability and Vulnerability Type

CVE number	**OpenStack Project**	**Skills to attack the vulnerability**	**Vulnerability Type**
CVE-2016-7498	Nova	login as authenticated user	denial of service
CVE-2015-5162	Cinder	create and upload crafted disk image	denial of service
CVE-2014-7231	Cinder	login as authenticated user to read log files	information disclosure
CVE-2014-7230	Cinder	login as authenticated user to obtain password	information disclosure
CVE-2014-3641	Cinder	access through desktop session, command line and web interface	information disclosure
CVE-2013-4183	Cinder	remotely authenticated	information disclosure
CVE-2017-7200	Glance	perfume mask network scan	information disclosure
CVE-2015-8234	Glance	created crafted image	bypass restriction
CVE-2015-5163	Glance	login as authenticated user	information disclosure
CVE-2015-3289	Glance	login as authenticated user	denial of service
CVE-2013-1840	Glance	remotely authenticated	information disclosure

7. DISCUSSION

In the literature review, five security threats have been identified and they are: malware, data leakage, unauthorized access, compromised disk image and risk of non-compliance that threatens the security of VMI. The identified threats was classified using STRIDE classification model as shown in Figure 4. The results of threats classification show that information disclosure is the most possible type that might occur as many security threats related to VMI lead to it. In addition, the identified vulnerabilities related to Nova, Glance and Cinder projects in OpenStack as shown in TABLE 2, it is obvious most of vulnerabilities when exploited by an adversary lead to information disclosure therefore, the threats that lead to information disclosure and the corresponding vulnerabilities need special attention to provide security for the VMI.

8. CONCLUSION

Threats modelling is the key element to identify security threats related to assets in the system. Threat modelling is used to identify security threats related to the VMI in cloud computing. The identified threats was classified to its threat type to study the effect of each individual threat that might cause when an attack happen on the VMI. Potential attack scenarios were drawn based on the vulnerabilities found in projects where the VMI store and launch with the skills required from the attacker to perform an attack. In light of the threat classification, the attack scenario and the vulnerabilities related to Glance, Nova and Cinder, it can be seen that most of the vulnerabilities when exploited by an attacker cloud result in information disclosure which needs to be considered.

REFERENCES

[1] R. K. Hussein, A. Alenezi, H. F. Atlam, M. Q. Mohammed, R. J. Walters, and G. B. Wills, “Toward Confirming a Framework for Securing the Virtual Machine Image in Cloud Computing,” Adv. Sci. Technol. Eng. Syst. J., vol. 2, no. 4, pp. 44–50, 2017.

[2] R. K. Hussein, A. Alenezi, G. B. Wills, and R. J. Walters, “A Framework to Secure the Virtual Machine Image in Cloud Computing,” Proc. - 2016 IEEE Int. Conf. Smart Cloud, SmartCloud 2016, no. November, pp. 35–40, 2016.

[3] D. R. Thompson and C. W. Thompson, “Rfid security threat model,” no. May, 2014.

[4] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, “Managing security of virtual machine images in a cloud environment,” Proc. 2009 ACM Work. Cloud Comput. Secur. - CCSW ’09, no. Vm, p. 91, 2009.

[5] M. Kazim, R. Masood, and M. A. Shibli, “Securing the virtual machine images in Cloud computing,” SIN 2013 - Proc. 6th Int. Conf. Secur. Inf. Networks, pp. 425–428, 2013.

[6] R. Schwarzkopf, M. Schmidt, C. Strack, S. Martin, and B. Freisleben, “Increasing virtual machine security in cloud environments,” J. Cloud Comput. Adv. Syst. Appl., vol. 1, no. 1, p. 12, 2012.

[7] K. Fan, D. Mao, Z. Lu, and J. Wu, “OPS: Offline patching scheme for the images management in a secure cloud environment,” Proc. - IEEE 10th Int. Conf. Serv. Comput. SCC 2013, pp. 587–594, 2013.

[8] D. Jeswani, A. Verma, P. Jayachandran, and K. Bhattacharya, "ImageElves: Rapid and reliable system updates in the cloud," Proc. - Int. Conf. Distrib. Comput. Syst., no. i, pp. 390–399, 2013.

[9] M. Kazim and D. Evans, "Threat modeling for services in cloud," Proc. - 2016 IEEE Symp. Serv. Syst. Eng. SOSE 2016, pp. 84–90, 2016.

[10] K. Bakshi, "Cisco Cloud Computing - Data Center Strategy , Architecture , and Solutions Point of View White Paper," Solutions, pp. 1–16, 2009.

[11] N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal, "Threat Modeling for Cloud Data Center Infrastructures," Springer, Cham, 2017, pp. 302–319.

[12] A. Alhebaishi, N., Wang, L., Jajodia, S. and Singhal, Threat Modeling for Cloud Data Center Infrastructures. 2017.

[13] R. Schwarzkopf, M. Schmidt, C. Strack, S. Martin, and B. Freisleben, "Increasing virtual machine security in cloud environments," pp. 1–12, 2012.

[14] K. Fan, D. Mao, Z. H. Lu, and J. Wu, "OPS: Offline patching scheme for the images management in a secure cloud environment," Proc. - IEEE 10th Int. Conf. Serv. Comput. SCC 2013, pp. 587–594, 2013.

[15] M. Kazim, R. Masood, and M. A. Shibli, "Securing the virtual machine images in cloud computing," Proc. 6th Int. Conf. Secur. Inf. Networks - SIN '13, no. April 2015, pp. 425–428, 2013.

[16] Openstack, "Images and instances," 2018. [Online]. Available: https://docs.openstack.org/glance/pike/admin/troubleshooting.html. [Accessed: 04-May-2018].

[17] CVE Details, "CVE-2016-7498," 2016. [Online]. Available: https://www.cvedetails.com/cve/CVE-2016-7498/. [Accessed: 18-Jun-2018].

[18] D. Thompson, "RFID security threat model," Conf. Appl. …, no. October, 2006.

[19] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013.

[20] A. Herzberg, "Protecting web users from phishing, spoofing and malware," 2006.

[21] A. Dehghantanha, A. Shaame, and K. Shanmugam, "An Educational Framework for Free and Open Source Software," Ijimt.Org, vol. 4, no. 1, 2013.

[22] F. C. Freiling, T. Holz, and G. Wicherski, "Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 3679 LNCS, pp. 319–335, 2005.

[23] M. Johnson and S. Dynes, "Inadvertent Disclosure-Information Leaks in the Extended Enterprise.," Weis, no. 2003, pp. 1–23, 2007.

[24] S. A. C. Schuckers and D. Ph, "Spoofing and Anti-Spoofing Measures," vol. 7, no. 4, pp. 56–62, 2002.

[25] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: A tutorial," IEEE Wirel. Commun., vol. 18, no. 2, pp. 66–74, 2011.

[26] G. Peterson, “From auditor-centric to architecture-centric: SDLC for PCI DSS,” Inf. Secur. Tech. Rep., vol. 15, no. 4, pp. 150–153, 2010.

[27] S. M. Specht and R. B. Lee, “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures,” Proc. 17th Int. Conf. Parallel Distrib. Comput. Syst. 2004 Int. Work. Secur. Parallel Distrib. Syst., no. September, pp. 543–550, 2004.

[28] K. Woods, C. A. Lee, and S. Garfinkel, “Extending digital repository architectures to support disk image preservation and access,” Proceeding 11th Annu. Int. ACM/IEEE Jt. Conf. Digit. Libr. - JCDL ’11, p. 57, 2011.

[29] Virginia Braun & Victoria Clarke, “Openstack : List of all products and related security vulnerabilities.” [Online]. Available: https://www.cvedetails.com/product-list/vendor_id-11727/Openstack.html. [Accessed: 21-Jun-2018].

[30] First improving security together, “Common Vulnerability Scoring System v3 . 0 Examples,” no. July, pp. 1–38, 2016.

[31] S. Vidalis and A. Jones, “Analyzing Threat Agents and Their Attributes.,” Eciw, no. June 2014, pp. 1–15, 2005.

[32] N. Ben-Asher, J. Morris-King, B. Thompson, and W. J. Glodek, “Attacker skill defender strategies and the effectiveness of migration-based moving target defense in cyber systems,” 11th Int. Conf. Cyber Warf. Secur. ICCWS2016, no. March, p. 21, 2016.

AUTHORS

Raid Khalid Hussein, PhD candidate University of Southampton His research interest cyber security, cloud computing, Cloud forensic, access control and internet of things.

Prof Vladimiro Sassone, Cyber Security, Head of group, Professorial Strategy Committee and Strategy Committee. University of Southampton. His research interest are in cyber security spanning over trust, anonymity, cyber control, privacy and security of Cloud industrial control systems and internet of things.

QOS-DRIVEN JOB SCHEDULING: MULTI-TIER DEPENDENCY CONSIDERATIONS

Husam Suleiman and Otman Basir
Department of Electrical and Computer Engineering, University of Waterloo

ABSTRACT

For a cloud service provider, delivering optimal system performance while fulfilling Quality of Service (QoS) obligations is critical for maintaining a viably profitable business. This goal is often hard to attain given the irregular nature of cloud computing jobs. These jobs expect high QoS on an on-demand fashion, that is on random arrival. To optimize the response to such client demands, cloud service providers organize the cloud computing environment as a multi-tier architecture. Each tier executes its designated tasks and passes the job to the next tier; in a fashion similar, but not identical, to the traditional job-shop environments. An optimization process must take place to schedule the appropriate tasks of the job on the resources of the tier, so as to meet the QoS expectations of the job. Existing approaches employ scheduling strategies that consider the performance optimization at the individual resource level and produce optimal single-tier driven schedules. Due to the sequential nature of the multi-tier environment, the impact of such schedules on the performance of other resources and tiers tend to be ignored, resulting in a less than optimal performance when measured at the multi-tier level.

In this paper, we propose a multi-tier-oriented job scheduling and allocation technique. The scheduling and allocation process is formulated as a problem of assigning jobs to the resource queues of the cloud computing environment, where each resource of the environment employs a queue to hold the jobs assigned to it. The scheduling problem is NP-hard, as such a biologically inspired genetic algorithm is proposed. The computing resources across all tiers of the environment are virtualized in one resource by means of a single queue virtualization. A chromosome that mimics the sequencing and allocation of the tasks in the proposed virtual queue is proposed. System performance is optimized at this chromosome level. Chromosome manipulation rules are enforced to ensure task dependencies are met. The paper reports experimental results to demonstrate the performance of the proposed technique under various conditions and in comparison with other commonly used techniques.

KEYWORDS

Cloud Computing, Task Scheduling and Allocation, QoS Optimization, Load Balancing, Genetic Algorithms

1. INTRODUCTION

The advent of cloud computing has emerged as one of the latest revolutions of computing paradigms [1–4]. It leverages a set of existing technologies and computing resources pooled in a cloud data center. Clients utilize cloud resources to perform complex tasks that are not easily achievable by their own infrastructure. Such resources are broadly accessed and provided as a service to clients on-demand, thus mitigate the complexity and time associated with the purchase and deployment of a traditional physical infrastructure at the client's side.

Typically, cloud computing environments experience variant workloads that entail client jobs of different QoS expectations, tardiness allowances, and computational demands. Jobs can be delay-sensitive and tightly coupled with client satisfactions, and thus cannot afford SLA violation costs. Such workload variations often occur within a short period of time and are not easily predictable,

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 133-155, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90912

causing system bottlenecks and thus execution difficulties on cloud resources to fulfill such expectations [5]. It is imperative that a cloud service provider efficiently accommodates and responds to such demands in a timely manner, so that client experience and system performance are optimized.

Thus, the scheduling in cloud computing has become a driving theme to support a scalable infrastructure that formulates optimal workload schedules on cloud resources and mitigates potential SLA violation penalties [6, 7]. The conundrum of a cloud service provider resolves around conciliating these conflicting objectives. A service provider may adopt admission control mechanisms to drop extra incoming jobs, however the likelihood of SLA violations and thus dissatisfied clients increase, which thus incurs SLA penalties on the client and service provider. In contrast, a service provider may often over-allocate resources to distinctly meet the incremental client demands and thus alleviate SLA violations, however it runs the risk of increasing the operational cost and leaving resources under-utilized.

A major limitation in schedulers of existing approaches is that they often optimize the performance of schedules at the individual resource level of a single-tier environment. However, it is typical that formulating schedules in a complex multi-tier cloud environment is harder than a traditional single-tier environment because of dependencies between the tiers. A performance degradation in a tier would propagate to negatively affect the performance of schedules in subsequent (dependent) tiers, thus causing the SLA violation penalties and likelihood of dissatisfied clients to increase.

Overall, such schedulers in their optimization strategies fail to capture QoS expectations and their associated penalties in a multi-tier environment. This paper presents a penalty-based multi-tier-driven load management approach that contemplates the impact of schedules in a tier on the performance of schedules constructed in subsequent tiers, thus optimizes the performance globally at the multi-tier level of the environment. The proposed approach accounts for tier dependencies to mitigate the potential of shifting and escalation of SLA violation penalties when jobs progress through subsequent tiers. Because the scheduling problem is NP-hard, a biologically inspired genetic algorithm supported with virtualized and segmented queue abstractions are proposed to efficiently seek (near-)optimal schedules at the multi-tier level, in a reasonable time.

2. BACKGROUND AND RELATED WORK

Scheduling and allocation of jobs have been presented in the literature among the challenging problems in cloud computing for the past few years [8–11]. Jobs are to be effectively scheduled and consolidated on fewer resources to deliver better system performance. Existing approaches investigate the problem from various perspectives, mostly tackled in a single-tier environment subject to common conflicting optimization objectives. The makespan and response time of jobs, as well as the resource utilization are typically the performance optimization metrics used to assess the efficacy of service delivery in achieving better user experience/satisfaction and SLA guarantees. Because the scheduling problem is NP-hard, the efficacy of scheduling approaches depends not only on fulfilling client demands and QoS obligations, but also on optimizing system performance.

Existing approaches employ different tardiness cost functions to quantify SLA violation penalties, so as to optimize the performance of schedules and mitigate their associated penalties. Chi *et al*. [12] and Moon *et al*. [13] adopt a stepwise function to represent different levels of SLA penalties. However, the stepwise function does not exactly reflect QoS penalty models required to tackle SLA violations of real systems. This function would typically incur a sudden change in the SLA penalty (increment/decrement from a level to another) when a slight variation in the job's completion time occurs at the transient-edge of two consecutive steps of the function, which is inaccurate. In addition, a fixed penalty level would be constantly held for each period of SLA

violations, which thus inaccurately incurs equal SLA penalties for different service violation times in the same step-period. Also, formulating the cost value of each penalty level with respect to SLA violation times is still to be precisely tackled.

In addition, Stavrinides *et al*. [14] use a linear monetary cost function to quantify multiple penalty layers (categories) of SLA violations. The tardiness metric, represented by the completion time of client jobs, is employed to calculate the cost incurred from the different layers of SLA violations. They investigate the effect of workloads of different computational demands on the performance of schedules in a single-tier environment, focusing on fair billing and meeting QoS expectations of clients. However, the linear function would not reflect the monetary cost of SLA violations in real systems, thus the performance and optimality of schedules formulated based on such cost calculations would be affected.

Furthermore, improved Min-Min and Max-Min scheduling are widely employed to tackle the problem by producing schedules at the individual resource level of the tier. Rajput *et al*. [15] and Chen *et al*. [16] present Min-Min based scheduling algorithms to minimize the makespan of jobs and increase the resource utilization in a single-tier environment. Generally, a Min-Min approach schedules the job with the minimum completion time on the resource that executes the job at the earliest opportunity, yet negatively affects the execution of jobs with larger completion times [17]. In contrast, a Max-Min based approach typically utilizes powerful resources to speedup the execution of jobs with the maximum completion times, however produces poor average makespan [18].

In their optimization strategies, the Min-Min and Max-Min based approaches rely primarily on the computational demands of jobs to produce optimal schedules at the resource level. They fail to produce minimum penalty schedules that accurately account for QoS obligations of jobs at the multi-tier level, which would negatively impact provider's SLA commitments. In addition, such approaches do not consider tier dependencies of a multi-tier cloud environment, thus SLA violation penalties of schedules at the resource level would propagate to escalate in subsequent tiers, which would negatively impact system performance.

Some approaches focus on balancing the workloads among resources, as well as employing different strategies to speedup job executions [19, 20]. Maguluri *et al*. [21] present a throughput-optimal algorithm that tackles the execution of jobs with unknown sizes. However, a throughput-based scheduling generally disregards the actual job running times in resources, and instead, focuses on queue lengths measured by the number of jobs, which is not necessarily accurate.

Redundancy-based strategies are also adopted and proven to speedup the execution of jobs [22, 23]. For instance, Nahir *et al*. [24] present a replication-based balancing algorithm that aims at minimizing the queueing overhead and the job's response time. Multiple copies (replicas) of each client's job are created and distributed on resource queues of a tier. Once a copy of the job completes the execution from a resource, other copies are deleted from the other resource queues. In addition, Kristenet *et al.* [25, 26] present the power of d choices for redundancy to send copies of a job to only d resources selected at random, so as to reduce the number of duplicated jobs in resource queues of the tier.

However, the optimization strategy of replication-based approaches does not employ the different QoS obligations and demands of jobs, thus, would not mitigate SLA violation penalties. If the mechanisms of admission control and resource over-allocation are not adopted, a replication-based approach might overload resource queues of tiers with a significant amount of jobs. Thus, the scheduler would potentially experience difficulties in managing the execution of such workloads to meet such QoS obligations at the multi-tier level.

Similar balancing approaches are widely adopted such as Least Connection (LC) weighted algorithms, Round Robin (RR) weighted algorithms [27], Random selection, and Shortest-Queue [28, 29]. These balancing approaches are provided as a service by popular cloud providers such as

Windows Azure, Amazon ELB, and HP-CLB [30]. Also, Wang *et al*. [31] and Lu *et al*. [32] present the Join-Idle-Queue (JIQ) balancing algorithm that assigns incoming jobs to only idle resource queues in a single-tier environment. Multiple dispatchers are employed to hold incoming jobs; each dispatcher keeps IDs of idle resources in the tier.

However, the JIQ-based balancing algorithm does not account for QoS expectations of jobs when a scheduling decision is made. Thus, high priority and delay-intolerant jobs might have to wait in a dispatcher to get an idle resource, while simultaneously some other delay-tolerant jobs in another dispatcher have already got idle resources for execution. In a complex multi-tier environment, the former balancing approaches would produce schedules that are poor in performance because they neither effectively reflect the system state nor account for dependencies between the tiers, and thus would not accurately meet the different QoS obligations of clients.

Furthermore, resource over-allocation is a viable option proven to provide high system performance, meet client demands, and mitigate SLA violations. Typically, clients negotiate with the service provider to submit estimates on the execution/completion times of their jobs. However, such estimates often tend to be either underestimated or inaccurate. For this purpose, Reig *et al*. [33] present an analytical predictor to infer job information and accordingly decide on the minimum allocation of resources required to execute client jobs before their deadlines; that is, to avoid inaccurate run-time estimates of clients and thus mitigate SLA violations. The scheduler policy adopts a job rejection strategy in two different scenarios. A job is rejected when its QoS obligations cannot be met, or when another higher priority job arrives to the system that negatively impacts SLA obligations of both jobs. However, such rejection policies would incur harsh SLA violation penalties on the client and service provider.

In addition, Hoang *et al*. [34] present a Soft Advance Reservation (SAR) method to meet SLA requirements and tackle error-prone estimates on job executions provided by the clients. Generally speaking, an over-sourced environment would reduce the likelihood of SLA violations and thus dissatisfied clients, however it would be significantly costly to acquire and operate. In contrast, the cloud service provider may allocate a small number of resources to reduce the operational cost, but with the expense of rejecting or discarding jobs that the provider would not meet their QoS expectations.

The meta-heuristic approaches are also presented to tackle scheduling problems in cloud computing environments [35–37]. Such approaches are adopted to efficiently solve NP-hard computational-expensive problems, however the approaches deliver a near-optimal performance in a timely manner and potentially reduce the running time of the scheduling algorithms. Goudarzi *et al*. [38] present a heuristic-based allocation method to meet client SLAs and maximize the profit of the service provider in a data center of multiple clusters. However, each cluster adopts a centralized dispatcher associated with multiple resources comprising together a single-tier environment.

Zhang *et al*. [39] propose a meta-heuristic scheduling algorithm that provides near-optimal resource configurations so as to maximize the profit and minimize the response time of jobs, in a centralized single-tier environment. Also, Zuo *et al*. [40] present an Ant Colony Optimization based scheduling method that finds a balance between the system performance represented by the makespan of jobs and the budget cost on the client. The former meta-heuristic approaches also tackle the problem in a single-tier environment and typically aim at optimizing the performance of schedules *locally* at the individual resource level of the tier, similar to Min-Min and Max-Min based approaches. However, they do not support the complexity and obligations of the multi-tier environment, therefore do not produce job schedules that are optimized at the multi-tier level and thus would not accurately mitigate SLA penalties.

As a general observation, current scheduling approaches in cloud computing fail to contemplate the impact of schedules optimized in a given tier on the performance of schedules on the subse-

quent tiers. Such approaches do not effectively tackle dependencies between tiers of the multi-tier cloud environment. Instead, the approaches evaluate the optimality of schedules at the individual resource level of the single-tier environment, therefore SLA violation penalties in a tier would typically shift to and escalate in subsequent tiers leading to a potential increase in the likelihood of dissatisfied clients.

Furthermore, the reality is that clients of cloud computing have different computational demands and strict QoS expectations. Client jobs demand for services from multiple cloud resources characterized by multiple tiers of execution. Such jobs sometimes are delay-intolerant and tightly coupled with client satisfactions, and thus cannot afford SLA violation penalties. Workload variations occur within a short period of time and are not easily predictable, thus causing execution difficulties on the cloud service provider to fulfill such expectations and deliver optimal performance. Due to resource limitations and the complexity incurred from the multi-tier dependencies, formulating optimal schedules to satisfy various QoS obligations of client demands at the multi-tier level while maintaining high system performance is not a trivial task.

In this paper, a penalty-oriented approach is proposed to influence scheduling in the multi-tier cloud environment. The proposed approach contemplates tier dependencies to produce minimum-penalty schedules at the multi-tier level. The SLA violation penalties of job schedules in a tier are to be alleviated when jobs progress through subsequent tiers, and accordingly the performance of such schedules is optimized *globally* at the multi-tier level. Since the problem is NP-hard, a biologically inspired meta-heuristic approach along with system virtualized and segmented queue abstractions are proposed to efficiently seek (near-)optimal schedules in a reasonable time.

3. PENALTY-ORIENTED MULTI-TIER SLA CENTRIC SCHEDULING OF CLOUD JOBS

A multi-tier cloud computing environment consisting of N sequential tiers is considered:

$$T = \{T_1, T_2, T_3, ..., T_N\} \tag{1}$$

Each tier T_j employs a set of identical computing resources R_j:

$$R_j = \{R_{j,1}, R_{j,2}, R_{j,3}, ..., R_{j,M}\} \tag{2}$$

Each resource $R_{j,k}$ employs a queue $Q_{j,k}$ that holds jobs waiting for execution by the resource. Jobs with different resource computational requirements and QoS obligations are submitted to the environment. It is assumed that these jobs are submitted by different clients and hence are governed by various SLA's. Jobs arrive at the environment in streams. A stream S is a set of jobs:

$$S = \{J_1, J_2, J_3, ..., J_l\} \tag{3}$$

The index of each job J_i signifies its arrival ordering at the environment. For example, job J_1 arrives at the environment before job J_2. Jobs arrive in random manner. Job J_i arrives at tier T_j at time $A_{i,j}$ via the queue of the job dispatcher JD_j of the tier. It has a prescribed execution time $\mathcal{E}_{i,j}$ at each tier. Each job has a service deadline which in turn stipulates a target completion time $\mathcal{C}_i^{(t)}$ for the job J_i in the multi-tier environment.

$$J_i = \left\{ A_{i,j}, \mathcal{E}_{i,j}, \mathcal{C}_i^{(t)} \right\}, \quad \forall\, T_j \in T \tag{4}$$

Jobs submitted to tier T_j are queued for execution based on an ordering β_j. As shown in Figure 1, each tier T_j of the environment consists of a set of resources R_j. Each resource $R_{j,k}$ has a queue

$Q_{j,k}$ to hold jobs assigned to it. For instance, resource $R_{j,1}$ of tier T_j is associated with queue $Q_{j,1}$, which consists of 4 jobs (J_6, J_7, J_8, and J_{10}) waiting for execution. A virtual-queue is a cascade of all queues of the tier as shown in Figure 2. The total execution time $\mathcal{ET}_i$ of each job J_i is as follows:

$$\mathcal{ET}_i = \sum_{j=1}^{N} \mathcal{E}_{i,j} \tag{5}$$

The target completion time $\mathcal{C}_i^{(t)}$ of job J_i represents an explicit QoS obligation on the service provider to complete the execution of the job. Thus, the $\mathcal{C}_i^{(t)}$ incurs a service deadline $\mathcal{DL}_i$ for the job in the environment. The service deadline $\mathcal{DL}_i$ is higher than the total prescribed execution time $\mathcal{ET}_i$ and incurs a total waiting time allowance $\omega\mathcal{AL}_i$ for job J_i in the environment.

$$\begin{aligned} \mathcal{DL}_i &= \mathcal{C}_i^{(t)} - A_{i,j} \\ &= \mathcal{ET}_i + \omega\mathcal{AL}_i \end{aligned} \tag{6}$$

Each job J_i has a response time $\mathcal{RT}_i^{\beta}$ that is a function of the total execution time $\mathcal{ET}_i$ and the total waiting time $\omega\mathcal{T}_i^{\beta}$.

$$\mathcal{RT}_i^{\beta} = \sum_{j=1}^{N} (\mathcal{E}_{i,j} + \omega_{i,j}^{\beta_j}) = \mathcal{ET}_i + \omega\mathcal{T}_i^{\beta} \tag{7}$$

where $\omega_{i,j}^{\beta_j}$ represents the waiting time of job J_i at tier T_j; β_j is the ordering that governs the order of execution of jobs at tier T_j. The $\omega\mathcal{T}_i^{\beta}$ represents the total waiting time of job J_i spends waiting for its turn to be executed at all tiers T of the environment, according to the ordering β. Each job J_i has a departure time $D_{i,j}$ from tier T_j, which will be the arrival time $A_{i,j+1}$ of the job to the next tier T_{j+1}.

$$\beta = \bigcup_{j=1}^{N} \beta_j \tag{8}$$

As such, the time difference between the response time $\mathcal{RT}_i^{\beta}$ and the service deadline $\mathcal{DL}_i$ represents the service-level violation time α_i^{β} of job J_i, according to the ordering β of jobs in tiers T of the environment.

$$(\mathcal{RT}_i^{\beta} - \mathcal{DL}_i) = \begin{cases} \alpha_i^{\beta} > 0, & \text{The client is not satisfied} \\ \alpha_i^{\beta} \leq 0, & \text{The client is satisfied} \end{cases} \tag{9}$$

However, the execution time $\mathcal{E}_{i,j}$ of job J_i at tier T_j is pre-defined in advance. Therefore, the resource capabilities of each tier T_j are not considered and, thus, the total execution time $\mathcal{ET}_i$ of job J_i is constant. Instead, the primary concern is on the queueing-level of the environment represented by the total waiting time $\omega\mathcal{T}_i^{\beta}$ of job J_i at all tiers T according to the ordering β.

Accordingly, the service-level violation time α_i^{β} of job J_i in the environment is subject to an SLA that stipulates an exponential penalty curve ϱ_i:

$$\begin{aligned} \varrho_i &= \chi * (1 - \mathrm{e}^{-\nu(\mathcal{RT}_i^{\beta} - \mathcal{DL}_i)}) \\ &= \chi * (1 - \mathrm{e}^{-\nu(\omega\mathcal{T}_i^{\beta} - \omega\mathcal{AL}_i)}) \\ &= \chi * (1 - \mathrm{e}^{-\nu(\alpha_i^{\beta})}) \end{aligned} \tag{10}$$

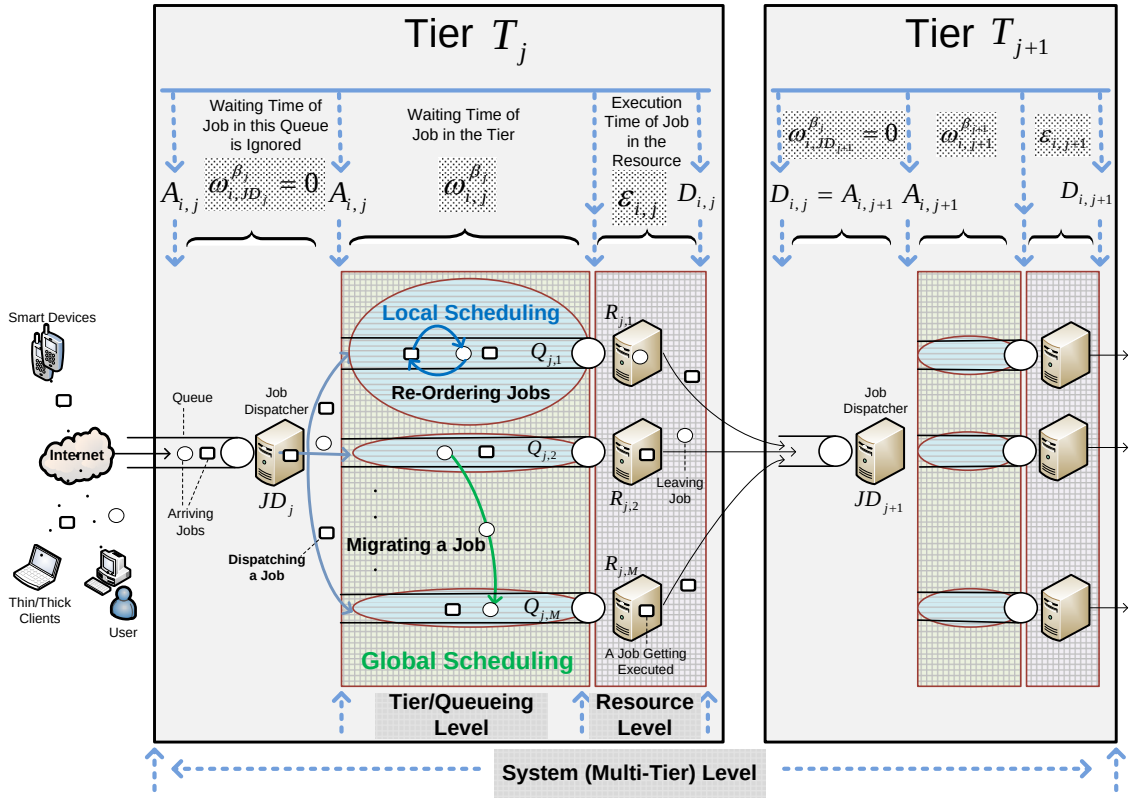


Figure 1. System Model of the Multi-Tier Environment

where χ is a monitory cost factor and ν is an arbitrary scaling factor. As such, the total penalty cost of stream l across all tiers is given by φ:

$$\varphi = \sum_{i=1}^{l} \varrho_i \tag{11}$$

3.1. Multi-Tier Waiting Time Allowance $\omega\mathcal{AL}_i$ Formulation

The performance of job schedules is formulated with respect to the multi-tier waiting time allowance $\omega\mathcal{AL}_i$ of each job J_i. Accordingly, the SLA violation penalty is evaluated at the multi-tier level of the environment. The objective is to seek job schedules in tiers of the environment such that the total SLA violation penalty of jobs would be minimized *globally* at the multi-tier level of the environment.

The total waiting time $\omega\mathcal{T}_i^{\beta}$ of job J_i currently waiting in tier T_p, where $p<N$, is not totally known because the job has not yet completely finished execution from the multi-tier environment. Therefore, the job's $\omega\mathcal{T}_i^{\beta}$ at tier T_p is estimated and, thus, represented by $\omega\mathcal{CX}_{i,p}^{\beta}$ according to the scheduling order β of jobs. As such, the job's service-level violation time α_i^{β} at tier T_p would be represented by the expected waiting time $\omega\mathcal{CX}_{i,p}^{\beta}$ of job J_i in the current tier T_p and the waiting time allowance $\omega\mathcal{AL}_i$ incurred from the job's service deadline $\mathcal{DL}_i$ at the multi-tier level of the environment.

$$\alpha_i^{\beta} = \omega\mathcal{CX}_{i,p}^{\beta} - \omega\mathcal{AL}_i \tag{12}$$

where the expected waiting time $\omega\mathcal{CX}_{i,p}^{\beta}$ of job J_i at tier T_p incurs the total waiting time $\omega\mathcal{T}_i^{\beta}$ of

job J_i at the multi-tier level.

$$\omega\mathcal{CX}_{i,p}^{\beta} = \sum_{j=1}^{(p-1)} (\omega_{i,j}^{\beta_j}) + \omega\mathcal{EL}_{i,p} + \omega\mathcal{RM}_{i,p}^{\beta_p} \tag{13}$$

where $\omega_{i,j}^{\beta_j}(\forall j \leq (p-1))$ represents the waiting time of job J_i in each tier T_j in which the job has completed the execution in, $\omega\mathcal{EL}_{i,p}$ represents the elapsed waiting time of job J_i in the tier T_p where the job currently resides, and $\omega\mathcal{RM}_{i,p}^{\beta_p}$ represents the remaining waiting time of job J_i according to the scheduling order β_p of jobs in the current holding tier T_p.

$$\beta_j = \bigcup_{k=1}^{M_k} \mathrm{I}(Q_{j,k}), \quad \forall j \in [1, N] \tag{14}$$

$$\omega\mathcal{RM}_{i,j}^{\beta_j} = \sum_{h \in \mathrm{I}(Q_{j,k}),\ h \text{ precedes job } J_i}^{\forall} \mathcal{E}_{h,j}, \quad \forall j \in [1, N] \tag{15}$$

where $\mathrm{I}(Q_{j,k})$ represents indices of jobs in $Q_{j,k}$. For instance, $\mathrm{I}(Q_{1,2}) = \{3, 5, 2, 7\}$ signifies that jobs J_3, J_5, J_2, and J_7 are queued in $Q_{1,2}$ such that job J_3 precedes job J_5, which in turn precedes job J_2, and so on. However, the elapsed waiting time $\omega\mathcal{EL}_{i,j}$ affects the execution priority of the job. The higher the time of $\omega\mathcal{EL}_{i,j}$ of job J_i in the tier T_j the lower the remained allowed time of $\omega\mathcal{AL}_i$ of job J_i at the multi-tier level, thus, the higher the execution priority of job J_i in the resource.

The objective is to find scheduling orders $\beta = (\beta_1, \beta_2, \beta_3, \ldots, \beta_N)$ for jobs of each tier T_j such that the stream's total penalty cost φ is minimal:

$$\underset{\beta}{\text{minimize}}\ (\varphi) \equiv \underset{\beta}{\text{minimize}}\ \Big(\sum_{i=1}^{l}\sum_{p=1}^{N}(\omega\mathcal{CX}_{i,p}^{\beta} - \omega\mathcal{AL}_i)\Big) \tag{16}$$

3.2. Differentiated Waiting Time Allowance $\omega\mathcal{PT}_{i,j}$ Formulation

The performance of job schedules is formulated with respect to a differentiated waiting time $\omega\mathcal{PT}_{i,j}$ of the job J_i at each tier T_j. The $\omega\mathcal{PT}_{i,j}$ is derived from the multi-tier waiting time allowance $\omega\mathcal{AL}_i$ of job J_i, with respect to the execution time $\mathcal{E}_{i,j}$ of the job J_i at the tier level relative to the job's total execution time $\mathcal{ET}_i$ at the multi-tier level of the environment.

$$\omega\mathcal{PT}_{i,j} = \omega\mathcal{AL}_i * \frac{\mathcal{E}_{i,j}}{\mathcal{ET}_i} \tag{17}$$

In this case, the higher the execution time $\mathcal{E}_{i,j}$ of job J_i in tier T_j, the higher the job's differentiated waiting time allowance $\omega\mathcal{PT}_{i,j}$ in the tier T_j. Accordingly, the SLA violation penalty is evaluated at the multi-tier level with respect to the $\omega\mathcal{PT}_{i,j}$ of each job J_i.

The waiting time $\omega_{i,j}^{\beta_j}$ of job J_i at tier T_j would not be totally known until the job completely finishes the execution from the tier, however, it can be estimated by $\omega\mathcal{PX}_{i,j}^{\beta_j}$ according to the current scheduling order β_j of jobs in the tier T_j. As such, the service-level violation time $\alpha\mathcal{T}_{i,j}^{\beta_j}$ of job J_i in the tier T_j according to the scheduling order β_j of jobs would be represented by the expected waiting time $\omega\mathcal{PX}_{i,j}^{\beta_j}$ and the differentiated waiting time allowance $\omega\mathcal{PT}_{i,j}$, of the job in the tier T_j.

$$\alpha\mathcal{T}_{i,j}^{\beta_j} = \omega\mathcal{PX}_{i,j}^{\beta_j} - \omega\mathcal{PT}_{i,j} \tag{18}$$

$$\alpha_i^{\beta} = \sum_{j=1}^{N} \alpha\mathcal{T}_{i,j}^{\beta_j} \tag{19}$$

where α_i^{β} is the total service-level violation time of the job J_i at all tiers of the environment according to the scheduling order β. The expected waiting time $\omega\mathcal{PX}_{i,j}^{\beta_j}$ incurs the actual waiting time $\omega_{i,j}^{\beta_j}$ of job J_i in tier T_j, and thus depends on the elapsed waiting time $\omega E\mathcal{L}_{i,j}$ and the remaining waiting time $\omega\mathcal{RM}_{i,j}^{\beta_j}$ of the job J_i according to the scheduling order β_j of jobs in the current holding tier T_j.

$$\omega\mathcal{PX}_{i,j}^{\beta_j} = \omega E\mathcal{L}_{i,j} + \omega\mathcal{RM}_{i,j}^{\beta_j} \tag{20}$$

The elapsed waiting time parameter $\omega E\mathcal{L}_{i,j}$ of job J_i in tier T_j affects the job's execution priority in the resource. The higher the time of $\omega E\mathcal{L}_{i,j}$, the lower the remained time of the differentiated waiting allowance $\omega\mathcal{PT}_{i,j}$ of job J_i in the tier T_j, therefore the higher the execution priority of the job J_i in the resource, so as to reduce the service-level violation time $\alpha\mathcal{T}_{i,j}^{\beta_j}$ of the job in the tier T_j of the environment.

As such, the objective is to find scheduling orders $\beta = (\beta_1, \beta_2, \beta_3, \ldots, \beta_N)$ for jobs of each tier T_j such that the stream's total penalty cost φ is minimal:

$$\underset{\beta}{\text{minimize}}\ (\varphi) \equiv \underset{\beta}{\text{minimize}}\ \Big(\sum_{i=1}^{l}\sum_{j=1}^{N}(\omega\mathcal{PX}_{i,j}^{\beta_j} - \omega\mathcal{PT}_{i,j})\Big) \tag{21}$$

4. MULTI-TIER-BASED MINIMUM PENALTY SCHEDULING: A GENETIC ALGORITHM FORMULATION

This paper is concerned with the SLA-driven, penalty-based scheduling of jobs in a multi-tier cloud environment. The scheduling tackles tier dependencies by contemplating the impact of schedules optimized in a given tier on the performance of schedules in subsequent tiers. Thus, the potential of shifting and escalation of SLA violation penalties of schedules in a tier are mitigated when jobs progress through tiers of the environment. It is desired to produce job schedules that are penalty-minimum at the multi-tier level.

However, finding job schedules at the multi-tier level to minimize the SLA violation penalties is an NP problem. Jobs can be tightly coupled with the client experience and QoS obligations. Given the prohibitively large number of candidate schedules (permutations) of an excessive volume of critical jobs with their computational complexity in a multi-tier environment, it is never desirable to adopt the brute-force search strategy to seek minimum penalty schedules at the multi-tier level. The dimensionality of the search space of the multi-tier environment demands for an effective strategy that finds acceptable solutions. Thus, a meta-heuristic search strategy, such as Permutation Genetic Algorithms (PGA), is a viable option for efficiently exploring and exploiting the large space of scheduling permutations [41]. Genetic algorithms have been successfully adopted in various problem domains and shown less computational effort [42]. They have undisputed success in yielding near optimal solutions for large scale problems, in reasonable time [43].

Scheduling the client jobs entails two steps: (1) allocating/distributing the jobs among the different tier resources. Jobs that are allocated to a given resource are queued in the queue of that resource; (2) ordering the jobs in the queue of the resource such that their total SLA violation time is minimal. What makes the problem increasingly hard is the fact that jobs continue to arrive, while the prior jobs are waiting in their respective queues for execution. Thus, the scheduling process needs

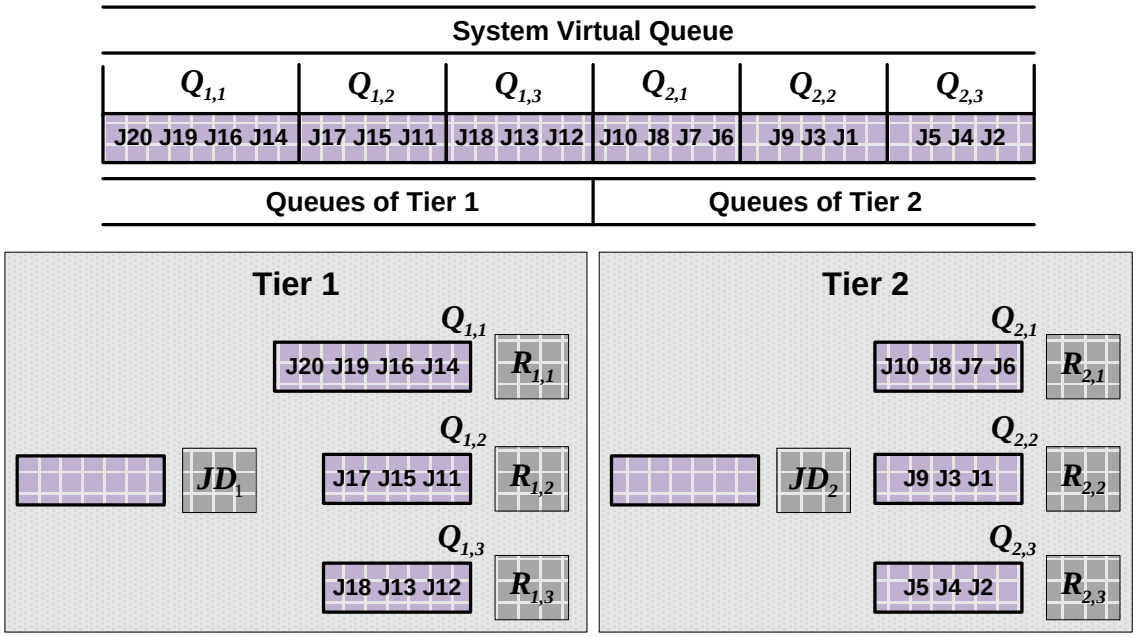


Figure 2. The System Virtual Queue

to respond to the job arrival dynamics to ensure that job execution at all tiers remains waiting-time optimal. To achieve this, job ordering in each queue should be treated as a continuous process. Furthermore, jobs should be migrated from one queue to another so as to ensure balanced job allocation and maximum resource utilization. Thus, the two operators are employed to construct optimal job schedules:

- The *reorder* operator is used to change the ordering of jobs in a given queue so as to find an ordering that minimizes the total SLA violation time of all jobs in the queue.
- The *migrate* operator, in contrast, is used to exploit the benefits of moving jobs between the different resources of the tier so as to reduce the total SLA violation time at the multi-tier level. This process is adopted at each tier of the environment.

However, implementing the *reorder/migrate* operators in a PGA search strategy to create job schedules at the multi-tier level of the environment is not a trivial task. This implementation complexity can be relaxed by virtualizing queues of the tiers into one *system virtual queue*. As shown in Figure 2, the system virtual queue is simply a cascade of the resource queues of the multi-tier environment.

In this way, the reorder/migrate operators running at the queue/tier level are converged into simply a reorder operator running at the multi-tier level. This system virtualization simplifies the PGA solution formulation toward finding schedules that are penalty-minimum at the multi-tier level. A consequence of this abstraction is the length of the permutation chromosome and the associated computational cost. This system virtual queue will serve as the chromosome of the solution that represents the scheduling of jobs on resource queues of tiers. An index of a job in this queue represents a gene. The ordering of jobs in a system virtual queue signifies the order at which the jobs in this queue are to be executed by the resource associated with that queue. Solution populations are created by permuting the entries of the system virtual queue, using the *order* and *migrate* operators. The system virtual queue in Figures 2 and 3 has six queues ($Q_{1,1}$, $Q_{1,2}$, $Q_{1,3}$, $Q_{2,1}$, $Q_{2,2}$, and $Q_{2,3}$) cascaded to construct one system virtual queue.

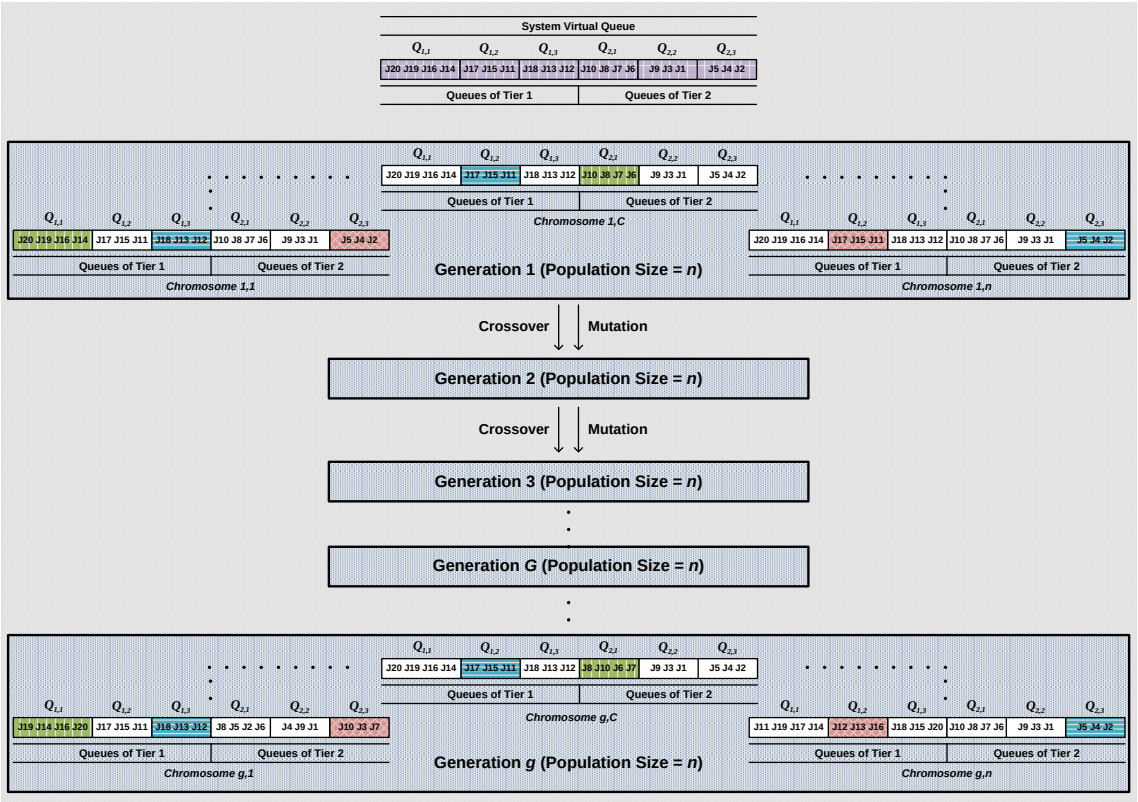


Figure 3. A System Virtualized Queue Genetic Approach

4.1. Evaluation of Schedules

The quality of a job schedule in a system virtual queue realization (chromosome) is assessed by a fitness evaluation function. For a chromosome r in generation G, the fitness value $f_{r,G}$ is represented by the SLA violation cost of the schedule in the system virtual queue computed at the multi-tier level. Two different fitness evaluation functions are adopted in two different solutions:

$$f_{r,G} = \begin{cases} \sum_{i=1}^{l} (\omega \mathcal{CX}_{i,p}^{\beta} - \omega \mathcal{AL}_i), \ \omega \mathcal{AL}_i \text{ based Scheduling} \\ \sum_{i=1}^{l} (\omega \mathcal{PX}_{i,j}^{\beta_j} - \omega \mathcal{PT}_{i,j}), \ \omega \mathcal{PT}_{i,j} \text{ based Scheduling} \end{cases} \tag{22}$$

In both scenarios, the SLA violation cost of job J_i is represented by the job's waiting time (either $\omega \mathcal{CX}_{i,p}^{\beta}$ or $\omega \mathcal{PX}_{i,j}^{\beta_j}$) according to its scheduling order β in the system virtual queue and the job's waiting allowance (either $\omega \mathcal{AL}_i$ or $\omega \mathcal{PT}_{i,j}$) incurred from the job's deadline $\mathcal{DL}_i$ at the multi-tier level.

The normalized fitness value F_r of each schedule candidate is computed as follows:

$$F_r = \frac{f_{r,G}}{\sum_{C=1}^{n} (f_{C,G})}, \quad r \in C \tag{23}$$

Based on the normalized fitness values of the candidates, the Russian Roulette is used to select a set of schedule candidates to produce the next generation population, using the combination and mutation operators.

4.2. Evolving the Scheduling Process

The job schedule of the system virtual queue is evolved to produce a population of multiple system virtual queues, each of which represents a chromosome that holds a new scheduling order of jobs in resource queues of the multi-tier environment. The crossover and mutation genetic operators are applied on randomly selected system virtual queues from the current population to produce the new population. Such operators explore and exploit the search space of possible scheduling options without getting stuck in locally optimum solutions. The *Single-Point* crossover and *Insert* mutation operators are used; rates of these operators in each generation are set to be 0.1 of the population size.

The evolution process of schedules of the system virtual queues along with the genetic operators are explained in Figure 3. Each segment in the system virtual queue corresponds to an actual queue associated with a resource in the tier. In each generation, each segment is subject to one of the following states:

- Maintain the same scheduling set and order of jobs held in the previous generation;
- Get a new scheduling order for the same set of jobs held in the previous generation;
- Get a different scheduling set and order of jobs.

For instance, queue $Q_{2,3}$ of *Chromosome* $(1,n)$ in the first generation maintains exactly the same scheduling set and order of jobs in the final generation shown in queue $Q_{2,3}$ of *Chromosome* (g,n). In contrast, queue $Q_{1,1}$ of *Chromosome* $(1,1)$ in the first generation maintains the same scheduling set of jobs in the final generation, yet has got a new scheduling order of jobs as shown in queue $Q_{1,1}$ of *Chromosome* $(g,1)$. A similar observation is shown in queue $Q_{2,1}$ of *Chromosomes* $(1,C)$ and (g,C) that has only got the scheduling order changed, however $Q_{2,2}$ and $Q_{2,3}$ of the same tier have got the same scheduling set and order of jobs held in the first generation. On the other side, some other queues would neither maintain the same scheduling set nor the same scheduling order of jobs in the last generation, such as queue $Q_{1,2}$ of *Chromosomes* $(1,n)$ and (g,n). Thus, if *Chromosome* $(g,1)$ is later selected as the best chromosome of the genetic solution, the state of the multi-tier environment is represented as follows:

- Queues of resources $R_{1,2}$ and $R_{1,3}$ of the first tier T_1 would maintain the same schedules of jobs of the first generation.
- The queue of resource $R_{1,1}$ of the first tier T_1 would just get a new scheduling order of the same set of jobs held in the first generation.
- Queues of resources $R_{2,1}$, $R_{2,2}$, and $R_{2,3}$ of the second tier T_2 would hold totally new schedules of jobs.

5. EXPERIMENTAL WORK AND DISCUSSIONS ON RESULTS

The adopted cloud environment in this paper consists of two tiers, each of which has 3 computing resources. The jobs generated into the cloud environment are atomic and independent of each other. A job is first executed on one of the computing resources of the first tier and then moves for execution on one of the resources of the second tier. Each job is served by only one resource at a time, as the scheduling strategy is non-preemptive.

Jobs arrive at the first tier and are queued in the arrival queue (tier's dispatcher) of the environment. The arrival behaviour is modeled on a Poisson process. The running time of each job in

a computing resource is assumed to be known in advance, generated with a rate $\mu = 1$ from the exponential distribution function $\exp(\mu = 1)$ [44]. In each tier T_j, job migrations from a queue to another queue are permitted. The waiting time allowance $\omega\mathcal{AL}_i$ of each job J_i is generated with respect to the job's total execution time $\mathcal{ET}_i$ at the multi-tier level of the environment as follows:

$$\omega\mathcal{AL}_i = \mathcal{ET}_i * 20\% \tag{24}$$

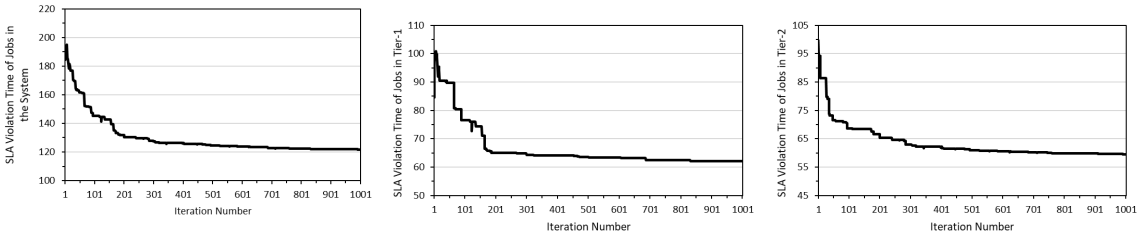
Accordingly, the differentiated waiting time allowance $\omega\mathcal{PT}_{i,j}$ of each job J_i is generated using Equation 17.

5.1. The Experimental Approach

Two experiments are conducted, the system virtualized queue and segmented queue. To seek optimal schedules that produce minimum SLA penalty among all jobs at the multi tier level, the system virtual queue is employed and the multi-tier-driven genetic algorithm operates on all queues of the multi-tier environment simultaneously. The system virtual queue starts with an initial system-state and a QoS penalty that represent a schedule β of jobs. The genetic solution finds an enhanced schedule that reduces the SLA penalty of the system-state at the multi-tier level, which in turn is translated into an enhanced schedule of jobs in the resource queues of tiers. In contrast, the segmented queue scheduling employs the genetic solution to seek an optimal schedule at the individual queue level of the tiers, in a reduced search space, such that the QoS penalty is reduced at the queue level of the tier and consequently at the multi-tier level. However, the penalty exponential scaling parameter ν is set to be $\nu = 0.01$. In both experiments, each population employs 10 chromosomes.

5.2. QoS Penalty Scheduling Evaluation of the Waiting Time Allowance $\omega\mathcal{AL}_i$

The job schedules have been conducted according to the multi-tier waiting time allowance $\omega\mathcal{AL}_i$ of each job J_i. The service-level violation time of each job J_i is measured at the multi-tier level with respect to the $\omega\mathcal{AL}_i$ of the job; accordingly, the SLA violation penalty payable by the service provider is quantified. The system virtualized queue and segmented queue genetic solutions are used to efficiently seek optimal job schedules. Overall, the scheduling approach has been proven to enhance the performance by producing optimal job schedules that reduce the total service-level violation time of jobs and their associated SLA penalty *globally* at the multi-tier level of the environment (as shown in Figures 4 and 5, as well as Tables 1 and 2).



(a) System-Level (Total of 46 Jobs)

(b) Tier-1 (21 Jobs)

(c) Tier-2 (25 Jobs)

Figure 4. System Virtualized Queue Scheduling with Respect to Multi-Tier $\omega\mathcal{AL}_i$

The scheduling approach along with the system virtualized queue genetic solution has been applied to seek an optimal scheduling of jobs. Figure 4 and Table 1 represent a state of a multi-tier environment that contains 46 jobs; 21 jobs are allocated to tier T_1 and 25 jobs are allocated to tier

T_2. At the start, the total service-level violation time of the initial scheduling order of the 46 jobs on both tiers initiates with 184 units of violation time (as shown in Figure 4a). Then, the scheduling approach along with the system virtualized queue genetic setup has formed an enhanced schedule for the 46 jobs on resource queues of both tiers, that optimizes the performance at the multi-tier level by 34% to reach 121 units of violation time. As a results, the SLA penalty payable by the service provider is also optimized by 24%, a reduction from 1.2 for the initial schedule to 0.91 for the enhanced schedule of the 46 jobs (as shown in Table 1).

Table 1. System Virtualized Queue Scheduling with Respect to Multi-Tier $\omega\mathcal{AL}_i$

	Number[1] of Jobs	Initial[2]		Enhanced[3]		Improvement	
		Violation	Penalty	Violation	Penalty	Violation %	Penalty %
System-Level, Figure 4a	46	184.39	1.2	121.69	0.91	34.01%	24.17%
Tier-1, Figure 4b	21	84.60	0.57	62.16	0.46	26.53%	18.91%
Tier-2, Figure 4c	25	99.80	0.63	59.53	0.45	40.35%	28.95%

[1] **Number of Jobs** represents the total number of jobs in queues of the tier/environment. For instance, the first entry (46 jobs) shows that the multi-tier environment contains 46 jobs in total. The second (21 jobs) and third (25 jobs) entries of the table mean that the 3 queues of tier-1 and tier-2 are allocated 21 and 25 jobs, respectively.
[2] **Initial Violation** represents the total SLA violation time of jobs according to their initial scheduling before using the system virtualized queue genetic solution.
[3] **Enhanced Violation** represents the total SLA violation time of jobs according to their final/enhanced scheduling found after using the system virtualized queue genetic solution.

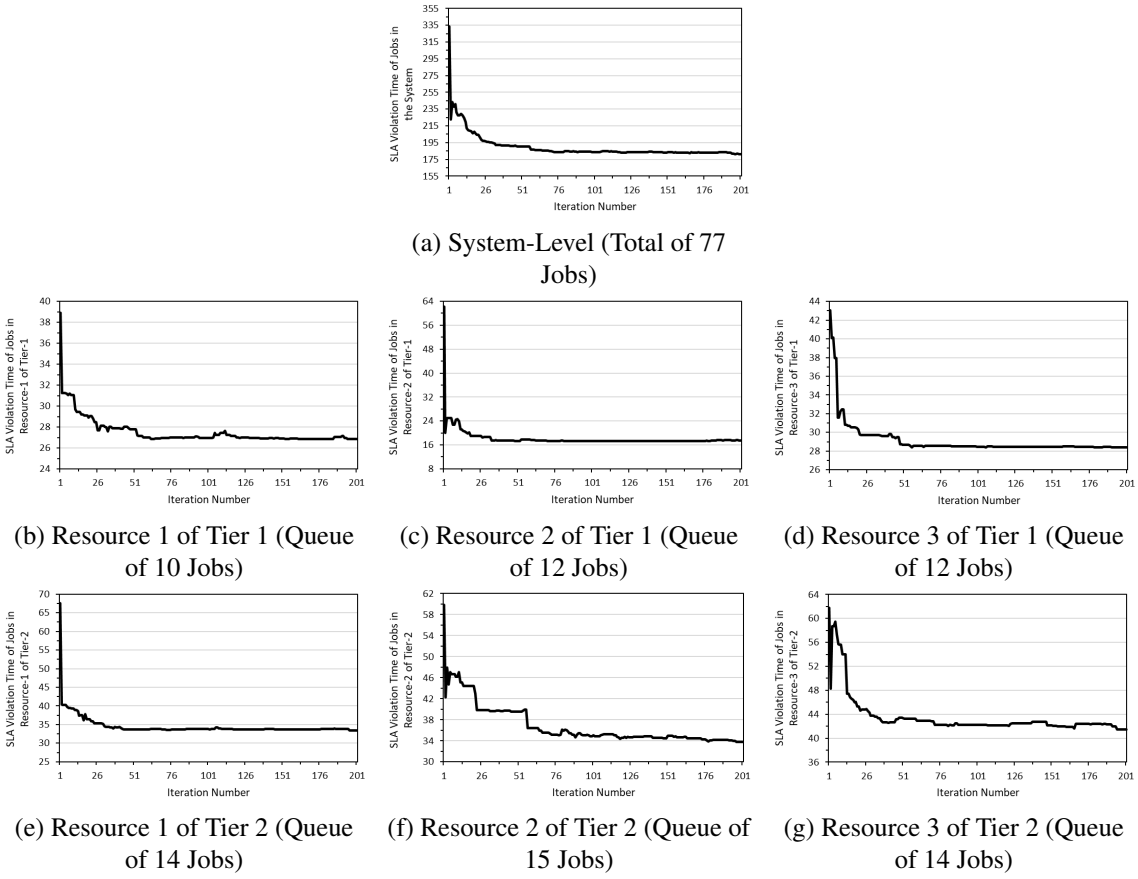
The former enhancements achieved *globally* at the multi-tier level of the environment would consequently optimize the performance of job schedules in each individual tier, thus, reduce the total service-level violation time and SLA penalty of the virtual-queue of each tier. For instance, the initial schedule of the virtual-queue (25 jobs) of tier T_2 shown in Figure 4c began with 99.8 units of violation time. Then, the performance has been optimized by 40% to reach 59.5 units of violation time for the enhanced schedule of jobs as a consequence of applying the scheduling approach along with the system virtualized queue genetic setup. As such, the total SLA penalty of jobs at tier T_2 has been reduced by 28.95% (as shown in Table 1). Similarly, the results reported in Figure 4b and Table 1 demonstrate the effectiveness of the system virtualized queue scheduling approach in reducing the total service-level violation time and penalty of the virtual-queue (21 jobs) of tier T_1 by 26.5% and 18.9%, respectively.

Table 2. Segmented Queue Scheduling with Respect to Multi-Tier $\omega\mathcal{AL}_i$

	Number of Jobs	Initial[4]		Enhanced[5]		Improvement	
		Violation	Penalty	Violation	Penalty	Violation %	Penalty %
System-Level, Figure 5a	77	333.37	2.537	181.26	1.56	45.63%	38.51%
Resource-1 Tier-1, Figure 5b	10	62.13	0.463	17.34	0.16	72.09%	65.59%
Resource-2 Tier-1, Figure 5c	12	38.93	0.322	26.84	0.24	31.05%	27.00%
Resource-3 Tier-1, Figure 5d	12	43.08	0.350	28.41	0.25	34.06%	29.35%
Resource-1 Tier-2, Figure 5e	14	67.57	0.491	33.43	0.28	50.52%	42.15%
Resource-2 Tier-2, Figure 5f	15	59.86	0.450	33.77	0.29	43.58%	36.37%
Resource-3 Tier-2, Figure 5g	14	61.80	0.461	41.46	0.34	32.91%	26.37%

[4] **Initial Violation** represents the total SLA violation time of jobs according to their initial scheduling before using the segmented queue genetic solution.
[5] **Enhanced Violation** represents the total SLA violation time of jobs according to their final/enhanced scheduling found after using the segmented queue genetic solution.

In contrast, the scheduling approach with the segmented queue genetic solution has been applied on each individual queue of the tier to seek an optimal scheduling of jobs in that queue. The results (reported in Figure 5 and Table 2) demonstrate the effectiveness of this scheduling approach in optimizing the performance of the job schedule of 77 jobs in the environment so as to reduce the service-level violation time and SLA penalty. Tier T_1 is allocated 34 jobs distributed into 12, 10,



(a) System-Level (Total of 77 Jobs)

(b) Resource 1 of Tier 1 (Queue of 10 Jobs)

(c) Resource 2 of Tier 1 (Queue of 12 Jobs)

(d) Resource 3 of Tier 1 (Queue of 12 Jobs)

(e) Resource 1 of Tier 2 (Queue of 14 Jobs)

(f) Resource 2 of Tier 2 (Queue of 15 Jobs)

(g) Resource 3 of Tier 2 (Queue of 14 Jobs)

Figure 5. Segmented Queue Scheduling with Respect to Multi-Tier $\omega\mathcal{AL}_i$

and 12 jobs in the resource queues $Q_{1,1}$, $Q_{1,2}$, and $Q_{1,3}$, respectively. On the other side, tier T_2 contains 43 jobs whereby $Q_{2,1}$ is allocated 12 jobs, $Q_{2,2}$ 10 jobs, and $Q_{2,3}$ 12 jobs.

The initial schedule of the 77 jobs in resource queues of both tiers has at the beginning started with 333 units of violation time at the multi-tier level of the environment, as shown in Figure 5a. Then, the scheduling approach with the segmented queue genetic setup has been applied on each individual queue of each tier. This scheduling approach has formed an enhanced scheduling of jobs in each queue that has reduced, at the multi-tier level, the total service-level violation time of jobs by 45% to reach 181 units of violation time. As a result, the total SLA violation penalty payable by the service provider has been optimized by 38.5%, a reduction from 2.537 for the initial scheduling to 1.56 for the enhanced scheduling of jobs.

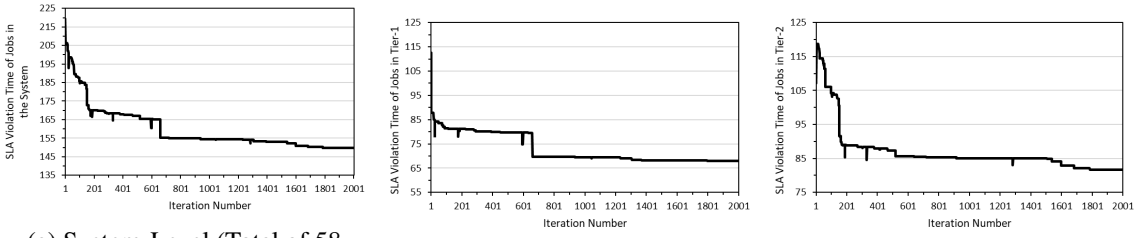
Similar observations are in order with respect to improving the total service-level violation time and SLA penalty of each individual resource-queue in each tier as a result of employing the segmented queue genetic solution. For instance, the resource-queue $Q_{1,1}$ of tier T_1 shown in Figure 5b contains 10 jobs, but its total service-level violation time and penalty is reduced by 72% and 65.6%, respectively.

Thus, the system virtualized queue and segmented queue genetic solutions have efficiently explored a big solution search space using a small number of genetic iterations to achieve such enhancements. Figure 4b shows that the system virtualized queue required a total of only $1{,}000$ genetic iterations to efficiently seek an optimal schedule of jobs in tier T_1, each iteration employs 10 chromosomes to evolve the optimal schedule. As such, 10×10^3 scheduling orders are constructed and genetically manipulated throughout the search space, as opposed to 21! (approxi-

mately 5×10^{19}) scheduling orders if a brute-force search strategy is employed to seek the optimal scheduling of jobs. Similar observations are in order with respect to the results reported on the segmented queue genetic solution.

5.3. QoS Penalty Scheduling Evaluation of the Differentiated Waiting Time $\omega\mathcal{PT}_{i,j}$

The job schedules have been conducted according to the differentiated waiting time allowance $\omega\mathcal{PT}_{i,j}$ of each job J_i at the tier level, which is derived from the waiting time allowance $\omega\mathcal{AL}_i$ of the job at the multi-tier level of the environment. Thus, the service-level violation time of each job J_i is measured with respect to the $\omega\mathcal{PT}_{i,j}$ of the job in the tier, and accordingly the SLA violation penalty payable by the service provider is quantified. The system virtualized queue and segmented queue genetic solutions are used to efficiently seek optimal scheduling orders of jobs. Overall, the efficacy of the scheduling approach has been proven to produce optimal schedules that reduce the total service-level violation time of jobs and their associated SLA penalty at the multi-tier level of the environment (as shown in Figures 6 and 7, as well as Tables 3 and 4).



(a) System-Level (Total of 58 Jobs)

(b) Tier-1 (26 Jobs)

(c) Tier-2 (32 Jobs)

Figure 6. System Virtualized Queue Scheduling with Respect to Differentiated $\omega\mathcal{PT}_{i,j}$

Figure 6a and Table 3 represent a multi-tier environment that comprises 58 jobs; 26 jobs are allocated in tier T_1 and 32 jobs are allocated in tier T_2. At the start, the schedule of the 58 jobs in both tiers produced 219.5 units of violation time. After the scheduling approach along with the system virtualized queue genetic solution is applied on the tiers, an enhanced schedule for the 58 jobs in both tiers has been formed. Consequently, the service-level violation time of the enhanced scheduling of jobs is optimized at the multi-tier level by 31.85% to reach 149.6 units of violation time. As a result, the associated SLA violation penalty presented in Table 3 is optimized by 21.64%, a reduction from 1.34 for the initial schedule to 1.05 for the enhanced schedule of jobs. Similarly, such enhancements reduce the total violation time and SLA penalty of the virtual queue of each individual tier (as shown in Figures 6b and 6c, as well as Table 3). For instance,

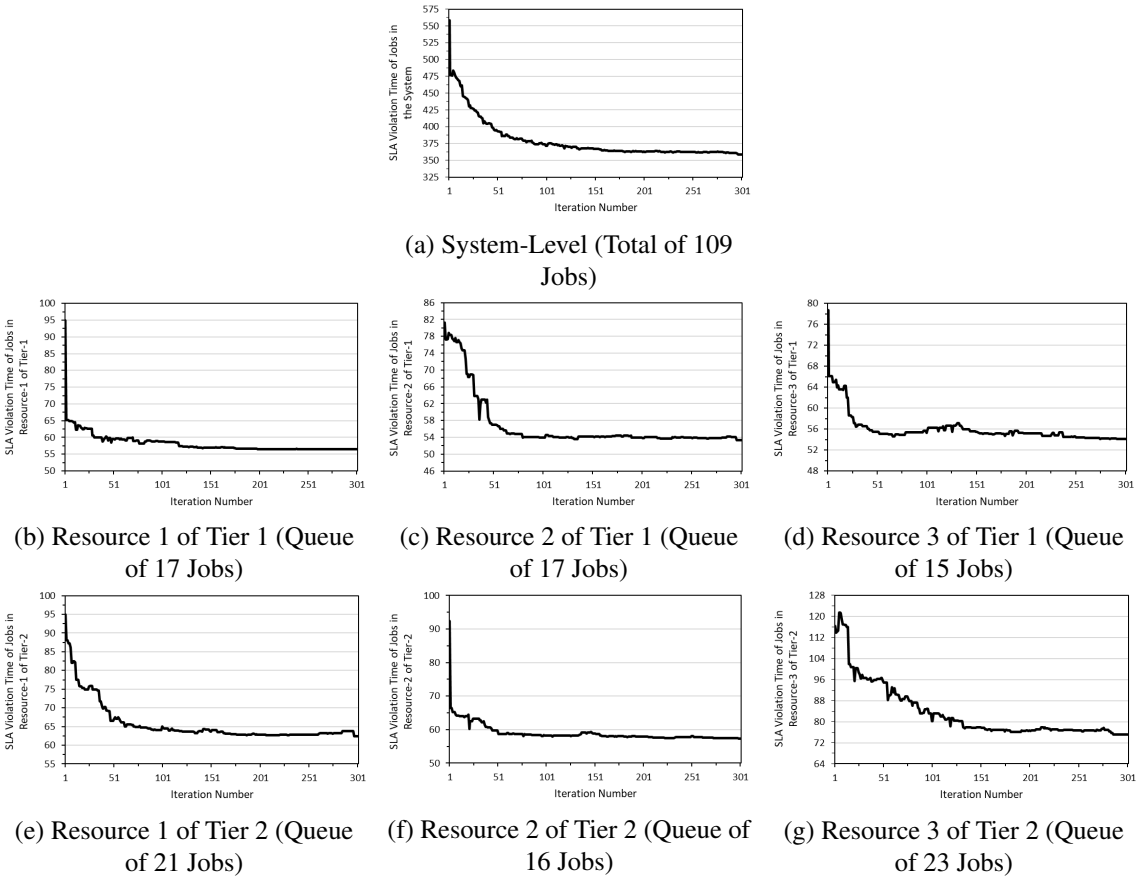
Table 3. System Virtualized Queue Scheduling with Respect to Differentiated $\omega\mathcal{PT}_{i,j}$

	Number[1]	**Initial**[2]		**Enhanced**[3]		**Improvement**	
	of Jobs	**Violation**	**Penalty**	**Violation**	**Penalty**	**Violation %**	**Penalty %**
System-Level, Figure 6a	58	219.53	1.34	149.62	1.05	31.85%	21.64%
Tier-1, Figure 6b	26	112.47	0.68	68.03	0.49	39.51%	26.91%
Tier-2, Figure 6c	32	107.07	0.66	81.58	0.56	23.80%	15.14%

[1] **Number of Jobs** represents the total number of jobs in queues of the tier/environment. For instance, the first entry (58 jobs) shows that the multi-tier environment contains 58 jobs in total. The second (21 jobs) and third (25 jobs) entries of the table mean that the 3 queues of tier-1 and tier-2 are allocated 26 and 32 jobs, respectively.

[2] **Initial Violation** represents the total SLA violation time of jobs according to their initial scheduling before using the system virtualized queue genetic solution.

[3] **Enhanced Violation** represents the total SLA violation time of jobs according to their final/enhanced scheduling found after using the system virtualized queue genetic solution.



(a) System-Level (Total of 109 Jobs)

(b) Resource 1 of Tier 1 (Queue of 17 Jobs)

(c) Resource 2 of Tier 1 (Queue of 17 Jobs)

(d) Resource 3 of Tier 1 (Queue of 15 Jobs)

(e) Resource 1 of Tier 2 (Queue of 21 Jobs)

(f) Resource 2 of Tier 2 (Queue of 16 Jobs)

(g) Resource 3 of Tier 2 (Queue of 23 Jobs)

Figure 7. Segmented Queue Scheduling with Respect to Differentiated $\omega\mathcal{PT}_{i,j}$

the violation time and SLA penalty of the virtual-queue (26 jobs) of tier T_1 have respectively been reduced by 39.5% and 26.9%, as shown in Figure 6b.

Furthermore, similar observations are in order with respect to the segmented queue genetic solution shown in Figure 7 and Table 4, where the total service-level violation time and penalty of the 109 jobs in the resource queues of both tiers are reduced at the multi-tier level by 35.7% and 11%, respectively. Also, these enhancements affect the total violation time and penalty of the job schedules in each individual queue of each tier. For instance, the total violation time of $Q_{1,1}$ (17 jobs) shown in Figure 7b is reduced by 40.5%, which accordingly reduced the SLA violation penalty of jobs in the queue by 29.5%.

Table 4. Segmented Queue Scheduling with Respect to Differentiated $\omega\mathcal{PT}_{i,j}$

	Number of Jobs	**Initial**[4]		**Enhanced**[5]		**Improvement**	
		Violation	**Penalty**	**Violation**	**Penalty**	**Violation %**	**Penalty %**
System-Level, Figure 7a	109	558.33	3.61	358.73	2.69	35.75%	25.49%
Resource-1 Tier-1, Figure 7b	17	94.88	0.61	56.49	0.43	40.46%	29.57%
Resource-2 Tier-1, Figure 7c	17	81.28	0.56	53.34	0.41	34.37%	25.70%
Resource-3 Tier-1, Figure 7d	15	78.71	0.54	54.11	0.42	31.26%	23.30%
Resource-1 Tier-2, Figure 7e	21	94.92	0.61	62.42	0.46	34.25%	24.25%
Resource-2 Tier-2, Figure 7f	16	92.29	0.60	57.35	0.44	37.86%	27.58%
Resource-3 Tier-2, Figure 7g	23	116.25	0.69	75.03	0.53	35.46%	23.21%

[4] **Initial Violation** represents the total SLA violation time of jobs according to their initial scheduling before using the segmented queue genetic solution.
[5] **Enhanced Violation** represents the total SLA violation time of jobs according to their final/enhanced scheduling found after using the segmented queue genetic solution.

5.4. Comparison of the Approaches

Figure 8 and Table 5 contrast the performance of the scheduling approaches with respect to the total service-level violation time of jobs. The initial job schedules in the resource queues, and by implication, that of the system virtualized and segmented queues are the same. The WRR-based scheduling of jobs entails 3,812 units of violation time, whilst the WLC-based scheduling entails 3,563 units of violation time (as shown in Table 5). The scheduling approach along with the system virtualized queue and segmented queue genetic solutions has been applied to efficiently find optimized schedules that reduce the service-level violation time of jobs at the multi-tier level.

Table 5. Total SLA Violation Time

Multi-Tier $\omega\mathcal{PT}_{i,j}$ Based Scheduling		**Multi-Tier $\omega\mathcal{AL}_i$ Based Scheduling**		**WLC**	**WRR**
System Virtualized Queue	**Segmented Queue**	**System Virtualized Queue**	**Segmented Queue**		
1,859	2,495	2,363	2,700	3,563	3,812

The multi-tier based scheduling with respect to the total waiting allowance $\omega\mathcal{AL}_i$ along with the segmented queue genetic solution entails 2,700 units of violation time, a 29% reduction compared with the WRR strategy and 24% reduction compared with the WLC strategy. For the system virtualized queue genetic setup, the multi-tier $\omega\mathcal{AL}_i$ based scheduling produces job schedules that entail 2,363 units of violation time, which is a reduction of 38% compared with the WRR strategy and 34% compared with the WLC strategy.

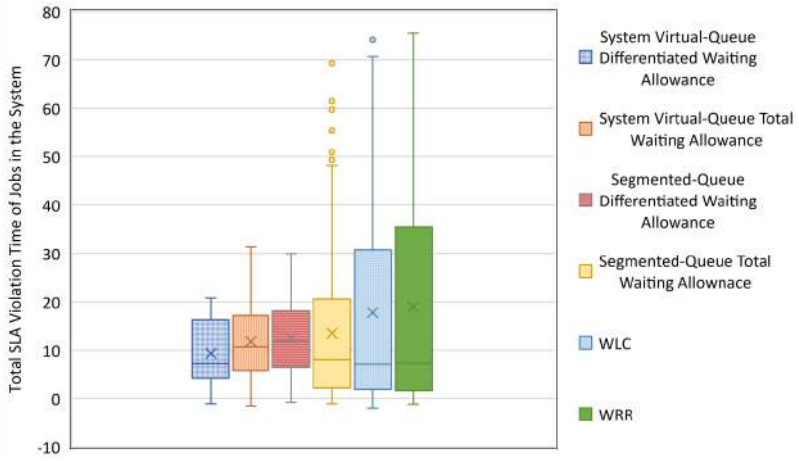


Figure 8. Comparison of the Approaches

In contrast, the multi-tier based scheduling with respect to the differentiated waiting time allowance $\omega\mathcal{PT}_{i,j}$ generally produces better performance than the multi-tier $\omega\mathcal{AL}_i$ based scheduling. The $\omega\mathcal{PT}_{i,j}$ based scheduling along with the system virtualized queue genetic solution has produced job schedules that entail 1,859 units of violation time, a reduction of 51% compared with the WRR strategy and 48% compared with the WLC strategy. On the other side of using the segmented queue genetic solution, the $\omega\mathcal{PT}_{i,j}$ based scheduling entails 2,495 units of violation time, which gets 35% and 30% reductions compared with the WRR and WLC strategies, respectively.

Figure 8 depicts the average and maximum waiting performance of the scheduling strategies. Though, the $\omega\mathcal{PT}_{i,j}$ based scheduling along with the system virtualized queue genetic strategy shows the shortest average violation time and, therefore, the best performance among all the strategies; approximately an average of 9 units of service-level violation time. Using the segmented

queue genetic solution, the $\omega\mathcal{PT}_{i,j}$ based scheduling produces 13 units of average service violation time, which is close to the multi-tier $\omega\mathcal{AL}_i$ based scheduling along with the system virtualized queue genetic solution that shows approximately 14 units of average violation time. Nevertheless, the WRR and WLC job scheduling strategies delivered inferior performance.

Furthermore, similar observations are in order with respect to the maximum waiting performance. The WRR and WLC scheduling strategies produce the highest values of the maximum violation time of jobs, approximately 37 units of violation time for the WRR and 32 units of violation time for the WLC. The $\omega\mathcal{PT}_{i,j}$ based scheduling along with the system virtualized queue genetic strategy delivers the best performance in minimizing the total service-level violation time and thus the lowest SLA penalty; a maximum of 16 units of violation time.

6. CONCLUSION

This paper presents a penalty-driven approach that addresses the optimal scheduling and allocation of jobs of various QoS obligations and computational demands in a multi-tier cloud environment. The approach employs the job's waiting time and service-level violation time to measure the penalty payable due to SLA violations, thus establishes a multi-tier-driven framework for quantifying and facilitating the management of a penalty that a cloud service provider can utilize to formulate penalty-based schedules.

The scheduling approach contemplates the impact of schedules optimized in a given tier on the performance of schedules on subsequent tiers. The approach accounts for dependencies between tiers of the cloud environment to produce minimum penalty schedules at the multi-tier level. The performance of job schedules in a tier is optimized such that the potential of shifting and escalation of SLA violation penalties are mitigated when jobs progress through subsequent tiers.

The multi-tier-based biologically inspired genetic algorithm efficiently facilitates optimal scheduling of jobs, in a reasonable time. System virtualized and segmented queue abstractions mitigate the operator complexities of the scheduling process at the multi-tier level. Each queue abstraction represents a realization of an execution scheduling order of jobs. The virtualized abstraction collapses and reduces the solution search spaces of all queues of the multi-tier environment into a simple search space with one searching operator, that helps using the PGA efficiently seek optimal job schedules at the multi-tier level.

The scheduling approach employs the multi-tier waiting time allowance $\omega\mathcal{AL}_i$ and the differentiated waiting time allowance $\omega\mathcal{PT}_{i,j}$ of each job to make multi-tier-driven scheduling decisions. Both experiments demonstrate the efficacy of the scheduling approach in optimizing the performance of job schedules, thus minimizing the service-level violation time and penalty payable by the cloud service provider at the multi-tier level. This scheduling approach with respect to both types of waiting time allowances, along with the system virtualized queue genetic solution, produces superior performance compared with the WRR and WLC scheduling strategies.

7. FUTURE WORK

The penalty model presented in this paper treats the violation penalty of different job waiting times to be identical. In fact, jobs of equal waiting times might not necessarily be similar in QoS penalty as such jobs tend to have different sensitivities to waiting and SLA violation. Therefore, it is imperative to design a penalty model that accounts for various QoS penalty classes, so that the performance of schedules is optimized at the tier and multi-tier levels to reflect such sensitivities.

REFERENCES

[1] R. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, "NIST cloud computing reference architecture," in *Proceedings of the IEEE World Congress on Services*, July 2011, pp. 594–596.

[2] C. Thingom, G. Kumar, and G. Yeon, "An analysis of load balancing algorithms in the cloud environment," in *Proceedings of the International Conference on Communication and Electronics Systems*, October 2016, pp. 1–8.

[3] D. Puthal, B. Sahoo, S. Mishra, and S. Swain, "Cloud computing features, issues, and challenges: A big picture," in *Proceedings of the International Conference on Computational Intelligence and Networks*, January 2015, pp. 116–123.

[4] V. Chavan, K. Dhole, and P. Kaveri, "Dynamic selection of job scheduling policies for performance improvement in cloud computing," in *Proceedings of the International Conference on Computing for Sustainable Global Development*, March 2016, pp. 379–382.

[5] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," *Future Generation Computer Systems*, vol. 79, pp. 849–861, 2018.

[6] S. Mustafa, B. Nazir, A. Hayat, A. Khan, and S. Madani, "Resource management in cloud computing: Taxonomy, prospects, and challenges," *Computers & Electrical Engineering*, vol. 47, no. 10, pp. 186–203, 2015.

[7] A. Abdelmaboud, D. Jawawi, I. Ghani, A. Elsafi, and B. Kitchenham, "Quality of service approaches in cloud computing: A systematic mapping study," *Journal of Systems and Software*, vol. 101, no. 3, pp. 159–179, 2015.

[8] K. Nuaimi, N. Mohamed, M. Nuaimi, and J. Al-Jaroodi, "A survey of load balancing in cloud computing: Challenges and algorithms," in *Proceedings of the Symposium on Network Cloud Computing and Applications*, December 2012, pp. 137–142.

[9] A. Thakur and M. Goraya, "A taxonomic survey on load balancing in cloud," *Journal of Network and Computer Applications*, vol. 98, no. 11, pp. 43–57, 2017.

[10] S. Shaw and A. Singh, "A survey on scheduling and load balancing techniques in cloud computing environment," in *Proceedings of the International Conference on Computer and Communication Technology*, September 2014, pp. 87–95.

[11] K. Bey, F. Benhammadi, and R. Benaissa, "Balancing heuristic for independent task scheduling in cloud computing," in *Proceedings of the International Symposium on Programming and Systems*, April 2015, pp. 1–6.

[12] Y. Chi, H. J. Moon, H. Hacigumus, and J. Tatemura, "SLA-tree: A framework for efficiently supporting SLA-based decisions in cloud computing," in *Proceedings of the International Conference on Extending Database Technology*, November 2011, pp. 129–140.

[13] H. Moon, Y. Chi, and H. Hacigumus, "Performance evaluation of scheduling algorithms for database services with soft and hard SLAs," in *Proceedings of the Second International Workshop on Data Intensive Computing in the Clouds*, November 2011, pp. 81–90.

[14] G. Stavrinides and H. Karatza, "The effect of workload computational demand variability on the performance of a SaaS cloud with a multi-tier SLA," in *Proceedings of the IEEE International Conference on Future Internet of Things and Cloud*, August 2017, pp. 10–17.

[15] S. Rajput and V. Kushwah, "A genetic based improved load balanced Min-Min task scheduling algorithm for load balancing in cloud computing," in *Proceedings of the International Conference on Computational Intelligence and Communication Networks*, December 2016, pp. 677–681.

[16] H. Chen, F. Wang, N. Helian, and G. Akanmu, "User-priority guided Min-Min scheduling algorithm for load balancing in cloud computing," in *Proceedings of the National Conference on Parallel Computing Technologies*, February 2013, pp. 1–8.

[17] G. Patel, R. Mehta, and U. Bhoi, "Enhanced load balanced Min-Min algorithm for static meta task scheduling in cloud computing," *Procedia Computer Science*, vol. 57, no. 8, pp. 545–553, 2015.

[18] X. Li, Y. Mao, X. Xiao, and Y. Zhuang, "An improved Max-Min task-scheduling algorithm for elastic cloud," in *Proceedings of the International Symposium on Computer, Consumer and Control*, June 2014, pp. 340–343.

[19] B. Schroeder and M. Harchol-Balter, "Evaluation of task assignment policies for supercomputing servers: The case for load unbalancing and fairness," *Journal of Cluster Computing*, vol. 7, no. 2, pp. 151–161, 2004.

[20] M. Harchol-Balter, M. Crovella, and C. Murta, "On choosing a task assignment policy for a distributed server system," in *Proceedings of the International Conference on Computer Performance Evaluation: Modelling Techniques and Tools*, September 1998, pp. 231–242.

[21] S. Maguluri and R. Srikant, "Scheduling jobs with unknown duration in clouds," *IEEE/ACM Transaction on Networking*, vol. 22, no. 6, pp. 1938–1951, 2014.

[22] K. Gardner, M. Harchol-Balter, E. Hyytia, and R. Righter, "Scheduling for efficiency and fairness in systems with redundancy," *Performance Evaluation*, vol. 116, no. C, pp. 1–25, 2017.

[23] K. Gardner, S. Zbarsky, S. Doroudi, M. Harchol-Balter, E. Hyytia, and A. Scheller-Wolf, "Queueing with redundant requests: Exact analysis," *Queueing Systems: Theory and Applications*, vol. 83, no. 3-4, pp. 227–259, 2016.

[24] A. Nahir, A. Orda, and D. Raz, "Replication-based load balancing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 494–507, 2016.

[25] K. Gardner, S. Zbarsky, M. Harchol-Balter, and A. Scheller-Wolf, "The power of D choices for redundancy," *ACM Performance Evaluation Review*, vol. 44, no. 1, pp. 409–410, 2016.

[26] K. Gardner, S. Zbarsky, M. Velednitsky, M. Harchol-Balter, and A. Scheller-Wolf, "Understanding response time in the redundancy-d system," *ACM Performance Evaluation Review*, vol. 44, no. 2, pp. 33–35, 2016.

[27] W. Wang and G. Casale, "Evaluating weighted round robin load balancing for cloud web services," in *Proceedings of the International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, September 2014, pp. 393–400.

[28] S. Mehdian, Z. Zhou, and N. Bambos, "Join-the-shortest-queue scheduling with delay," in *Proceedings of the American Control Conference*, May 2017, pp. 1747–1752.

[29] A. Mukhopadhyay and R. Mazumdar, "Analysis of randomized join-the-shortest-queue (JSQ) schemes in large heterogeneous processor-sharing systems," *IEEE Transactions on Control of Network Systems*, vol. 3, no. 2, pp. 116–126, 2016.

[30] P.-H. Liang and J.-M. Yang, "Evaluation of two-level global load balancing framework in cloud environment," *International Journal of Computer Science & Information Technology*, vol. 7, no. 2, p. 1, 2015.

[31] C. Wang, C. Feng, and J. Cheng, "Distributed Join-the-Idle-Queue for low latency cloud services," *IEEE/ACM Transactions on Networking*, vol. 26, no. 5, pp. 2309–2319, 2018.

[32] M. Boor, S. Borst, and J. Leeuwaarden, "Load balancing in large-scale systems with multiple dispatchers," in *Proceedings of the IEEE Conference on Computer Communications*, May 2017, pp. 1–9.

[33] G. Reig, J. Alonso, and J. Guitart, "Prediction of job resource requirements for deadline schedulers to manage high-level SLAs on the cloud," in *Proceedings of the IEEE International Symposium on Network Computing and Applications*, July 2010, pp. 162–167.

[34] P. Hoang, S. Majumdar, M. Zaman, P. Srivastava, and N. Gael, "Resource management techniques for handling uncertainties in user estimated job execution times," in *Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, July 2014, pp. 626–633.

[35] Z. Liu, M. Squillante, and J. Wolf, "On maximizing service-level-agreement profits," in *Proceedings of the ACM Conference on Electronic Commerce*, October 2001, pp. 213–223.

[36] H. Goudarzi and M. Pedram, "Multi-dimensional SLA-based resource allocation for multi-tier cloud computing systems," in *Proceedings of the IEEE International Conference on Cloud Computing*, July 2011, pp. 324–331.

[37] H. Rahhali and M. Hanoune, "Hybrid heuristic algorithm for load balancing in the cloud," *International Jounral Computer Science and Network Security*, vol. 18, no. 4, pp. 109–115, 2018.

[38] H. Goudarzi and M. Pedram, "Maximizing profit in cloud computing system via resource allocation," in *Proceedings of the International Conference on Distributed Computing Systems Workshops*, June 2011, pp. 1–6.

[39] L. Zhang and D. Ardagna, "SLA based profit optimization in autonomic computing systems," in *Proceedings of the International Conference on Service Oriented Computing*, November 2004, pp. 173–182.

[40] L. Zuo, L. Shu, S. Dong, C. Zhu, and T. Hara, "A multi-objective optimization scheduling method based on the ant colony algorithm in cloud computing," *IEEE Access*, vol. 3, no. 12, pp. 2687–2699, 2015.

[41] Y. Xiaomei, Z. Jianchao, L. Jiye, and L. Jiahua, "A genetic algorithm for job shop scheduling problem using co-evolution and competition mechanism," in *Proceedings of the International Conference on Artificial Intelligence and Computational Intelligence*, October 2010, pp. 133–136.

[42] X. Li and L. Gao, "An effective hybrid genetic algorithm and tabu search for flexible job shop scheduling problem," *International Journal of Production Economics*, vol. 174, no. 4, pp. 93–110, 2016.

[43] M. Nouiri, A. Bekrar, A. Jemai, S. Niar, and A. Ammari, "An effective and distributed particle swarm optimization algorithm for flexible job-shop scheduling problem," *Journal of Intelligent Manufacturing*, vol. 29, no. 3, pp. 603–615, 2018.

[44] T. Atmaca, T. Begin, A. Brandwajn, and H. Castel-Taleb, "Performance evaluation of cloud computing centers with general arrivals and service," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 8, pp. 2341–2348, 2016.

INTENTIONAL BLANK

TRUST MODELLING FOR SECURITY OF IOT DEVICES

Naresh K. Sehgal[1], Shiv Shankar[2] and John M. Acken[3]

[1]Data Centre Group, Intel Corp, Santa Clara, CA
[2]Chief Data Scientist, Maphalli, Bangalore, India
[3]ECE Department, Portland State University, Portland, OR

ABSTRACT

IoT (Internet of Things), represents many kinds of devices in the field, connected to data-centers via various networks, submitting data, and allow themselves to be controlled. Connected cameras, TV, media players, access control systems, and wireless sensors are becoming pervasive. Their applications include Retail Solutions, Home, Transportation and Automotive, Industrial and Energy etc. This growth also represents security threat, as several hacker attacks been launched using these devices as agents. We explore the current environment and propose a quantitative and qualitative trust model, using a multi-dimensional exploration space, based on the hardware and software stack. This can be extended to any combination of IoT devices, and dynamically updated as the type of applications, deployment environment or any ingredients change.

KEYWORDS

Edge Computing, Security, Adaptive learning, Trust model, Threats, Cloud Computing, Information Security

1. INTRODUCTION

Security concerns [1] abound with the emergence of IoT devices in Cloud Computing. A recent DDOS (Distributed Denial of Service) attack was launched using hijacked home security cameras, while in another instance private video clips were stolen and posted on Internet. Vulnerabilities in other unprotected devices, such as home appliances (TV, Fridge) on a network can be used to launch a cyber attack.

IoT devices are constantly collecting data about an environment or individuals, which can be potentially shared with third parties compromising privacy. It can range from personal preferences of web-browsing habits, TV channels selection, or images from home security cameras. In addition, there are security concerns if access controls to these IoT devices are compromised. An example is of someone hacking into a home control system to open garage doors or alter air-conditioning settings. While the latter may represent a minor inconvenience for a homeowner, if done for many homes at once can result in an overload of the local electric grid. Furthermore, if these devices connect to a service provider then its servers can be accessed via the devices to compromise its security. If IoT devices are located in a factory then an unauthorized access can be used to harm the equipment or products being manufactured. If these IoT devices are deployed in a hospital, then patient care can be compromised. At an individual level, it may mean incorrect readings from a blood sugar monitor resulting in inappropriate dosage of insulin, potentially with fatal consequences.

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 157-167, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90913

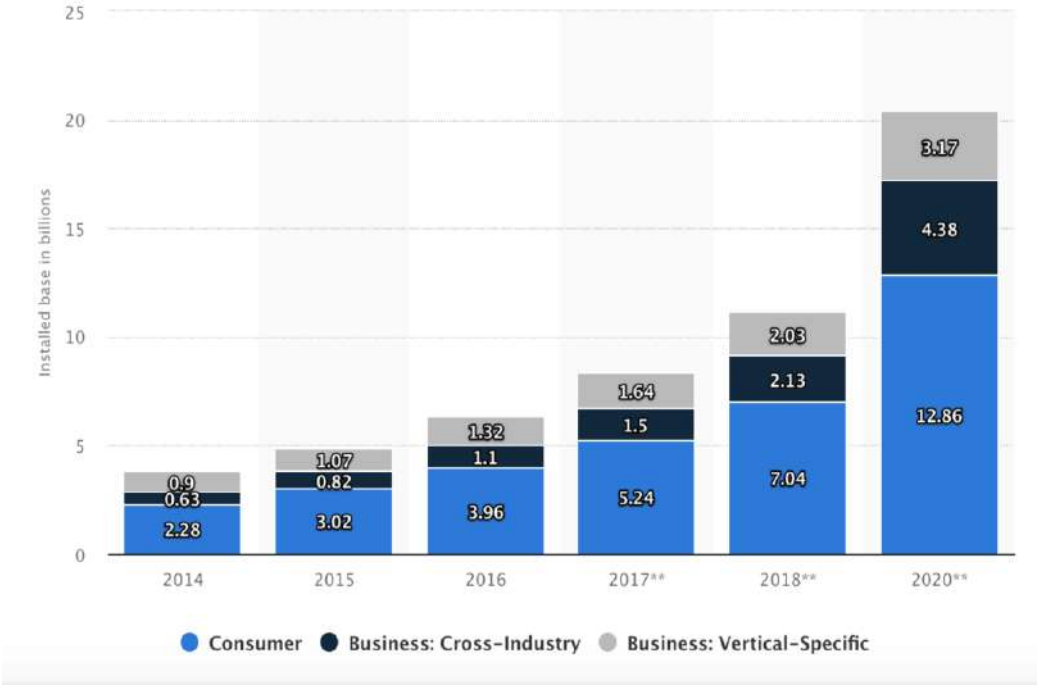


Fig 1: Growth in IoT devices over the years [2]

2. BACKGROUND

Another emerging trend is a Cloud driven by things vs. current Cloud Computing mostly driven by people, as cameras and wireless sensors are becoming pervasive [2]. Growth of IOT devices, and distribution between consumers and business are shown in Figure 1. Their applications include Retail Solutions, Home, Transportation and Automotive, Industrial and Energy etc. An example of retail industry is Amazon's user-facing portals where customers can visualize things and transact them. An example of Transportation and Automotive is a Software Defined Cockpit in a commercial aircraft, or an autonomous vehicle. An example of manufacturing is a smart factory with robots or energy savings in a building. Lastly, additional market segments such as health, print imaging, gaming and education are being digitized at an unprecedented rate. The phrase "Internet of things" was first used by British technology visionary Kevin Aston in 1999. His perception was to think of "objects in physical world connected by sensors". Internet Architecture Board (IAB) RFC 7452 provides the definition of IoT, as follows:

"Internet of Things" (IoT) denotes a trend where a large number of embedded devices employ communication services offered by Internet protocols. Many of these devices, often called "smart objects,'' are not directly operated by humans, but exist as components in buildings or vehicles, or are spread out in the environment. Four basic communication models for IoT are:

1. Device to device
2. Device to cloud
3. Device to gateway
4. Backend data sharing model

We are more interested in #2 and #4, as both involve Cloud services. An example is shown in figure 2, of home appliances such as a thermostat controlled A/C connected to Cloud for better energy management [3]

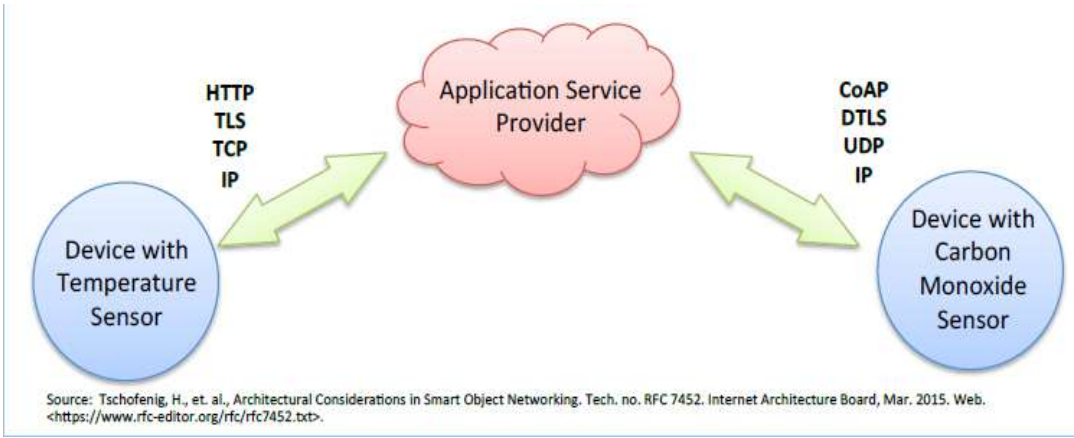


Fig 2: Cloud based energy management, monitoring and optimization [3]

3. SECURITY ATTACKS USING IOT DEVICES

For ensuring trust in IoT based Cloud Computing, it has to start with a trusted environment, trusted protocols and tamper proof components. Vendors need to provide "anti-tamper" solutions. Software upgrades in the field are needed for any bug fixes during the lifetime of an IoT device. A secure channel must exist to provide signed data that are transmitted and installed in the field, e.g., on a car or TV at home. In our door example, the vendor needs to provide an anti-tamper solution, to prevent someone locally changing the firmware or settings in an unauthorized manner. Even remote software upgrades are authenticated, as unprotected home appliances can be used to launch cyber attacks, e.g., someone using a collection of botnets to launch a DDOS attack on a Cloud server, where a botnet refers to one or more IoT devices being remotely controlled like a robotic army. Besides security, there are privacy concerns, as home sensors are collecting data about individuals that can be shared with third parties for commercial and political purposes.

Undesirable consequence may emerge if a third party can remotely gain control, e.g., of a self-driven car causing an accident on the road, or someone with malice can access the medicine drip-meters in a hospital with fatal consequences for the patients. This can be avoided with a balanced approach to interoperability and access control. This needs to be addressed at different layers of architecture, and within the protocol stacks between the devices. Standardization and adoption of communication protocols should specify when it is optimal to have standards. Some vendors like to create a proprietary ecosystem of compatible IoT products. This creates user lock-in to their particular ecosystem, which from a vendor's point of view is desirable because a closed ecosystem approach can offer benefits of security and reduces costs. However, from a user's point of view, such practices can create interoperability problems with solutions from other vendors, thereby limiting user's choices in case of upgrades or future system expansion.

As the frontiers of Cloud computing are expanding beyond the walls of a datacenter to the extremes of a network, a new term called Edge Computing is emerging. It refers to the data analytics occurring at the sources of data generation. This is bringing forth both new and existing security challenges, Following classifications describe the types of security issues as related to the Edge Computing, with a few examples:

1) **Identity authentication:** By definition, the number of players in Edge Computing is large and these may not belong to the same organization. It is infeasible to verify their

identity in a foolproof manner. Trust needs to be extended, as new customers buy their devices, such as security cameras, and bring these online with a remote registration. Central authority then must depend on the ability of these remote customers to protect their own devices.

2) **Unauthorized access:** Depending on the nature of devices at the Edge, their access into data-center may be bi-directional in nature. If someone hacks into a trusted remote device, and retrieves its authentication certificates to configure their own devices, then it will be nearly impossible to differentiate between genuine or fake users. Similarly, someone pretending to act as a central computer can access the remote devices and get critical user-data, such as on remote medical devices.

3) **Denial of service attacks:** An attack launched by hijacking multiple remote devices and simultaneously contacting the central server. This will cause the server to be overloaded, denying access to genuine users in a timely manner.

4) **Data theft:** Depending on where data is stored and for how long opens the possibility of it being stolen. An example is a security camera at home with local storage. In event of a theft, it may be possible for an intruder to simply remove the local storage, thus circumventing the purpose of a security camera. However, if camera immediately uploads an image to Cloud upon detecting a motion, then any physical tampering will not alter the images of intruders.

5) **Data integrity and falsification:** A key difference between confidentiality and integrity is that in the latter case, an attacker doesn't need to read the protected data, but merely modify it, e.g., with a buffer overflow, rendering it useless. This system level attack can happen if multiple devices from different sources are writing back to a central server database.

6) **Invasion of privacy:** Since multiple players may combine their data inputs from different sources to arrive at a desired conclusion, e.g., for real-time traffic updates, their identities need to be protected. This may include an individual's location, movements and any other aspects of personal nature.

7) **Activity monitoring:** A cell phone that constantly pings the signal tower, is sufficient for someone to monitor the location of aphone's owner, their movements etc. Furthermore, if a remote app can turn on the microphone or camera in a phone, then additional information and activities can be monitored in an illegal manner. Similar effects can be achieved with fixed cameras at commercial or public locations, e.g., in a shopping center.

8) **Rooting of devices**: Additional software can be installed in the IoT devices without users' permission. The software can 'root' the device preventing detection and have full access. There is no universal virus or malware scanner for IoT.

Some devices can be programmed to selectively transmit data to a cloud service for processing, e.g., a security camera which has a buffer of 15 seconds, but records and transmits a 30 seconds of clip only if any motion is detected, for 15 seconds before and 15 seconds after the motion is detected. This reduces storage requirements but increases chances of a missed detection. Such devices are designed to render service with minimal intervention, and yet they need to be directed using voice activation or image recognition.

These and other devices can be used to conduct a DDOS attack on the backend server, even in a serverless architecture [4]. The attacker simply hijacks one or more devices, and uses them to inundate the backend services. This can be done by sending more data, and more often, from the camera even when there is no motion detected.

4. SECURITY SOLUTIONS FOR IOT DEVICES

Solution level cost considerations involve technical factors such as limited internal processing, memory resources or power consumption demands. Vendors try to reduce the unit cost of devices by minimizing parts and product design costs. It is more expensive to design interoperability features into a product and test for compliance with a standards specification. A non-interoperable device may lack in standards and the documented best practices. It may limit the potential use of IoT device, and absence of these standards can result in deviant behavior by IoT devices.

It is recognized that traditional Trusted Compute Boundary (TCB) expands with Edge Computing to include domains that are physically outside the control of remote device or central data-center owners. The best they can do is to monitor/track a threat, identify an attacker, launch a recovery and prevent false positives. These steps are outlined below:

1) **Monitor/track a Threat:** This is possible by establishing a normal usage pattern for the IoTdevice, an example is a security camera at home, which uploads data whenever any motion is detected, e.g., whenever people go in and out. If the regular pattern for a home is no more than a couple of dozen data uploads during a day, then hundreds of data loads to the central server within a few minutes may indicate that the device has been compromised. It could be an attempt to cause a DOS attack.

2) **Identifying attackers:** Once a threat is detected, then attackers need to be identified. These could take the form of an IP address of the IoT that is repeatedly pinging the central server, to launch a denial of service attack.

3) **Attack recovery:** This can take the form of blocking the offending IP address. However, an attacker can corrupt the critical data before the attacker's presence is detected. In such a case, frequent checkpoints must be taken to do a rollback to the known good state.

4) **Accidental and unintentional failures confused with security attacks:** Any detection method suffers from the risks of false positives, e.g., mistaken flagging of genuine access as a potential threat. An example of this is a stock market trading computer that detects unusual activity, which is genuine yet may flag a false alarm. Similar situation can happen with security alarms due to false sensor activity data etc. This calls for a learning system that becomes smarter over time.

5) **Data Integrity Protection:** We previously described a system level attack if multiple devices from different sources are writing back to a central server database. This can be protected by assigning a virtual partition or container to the data coming from each distinct source, and checking the address range of each access to prevent data integrity of other users on the same server.

Internet Engineering Task Force (IETF) has identified the problem of Interoperability, as many suppliers build "walled gardens" that limit users to interoperate with a curated subset of component providers, applications and services.

Interoperability solutions between IoT devices and backend systems can exist at different layers of the architecture, and at different levels within protocol stack between the devices. Key is the standardization and adoption of protocols, which should specify when and where it is optimal to use standards. More work is needed to ensure interoperability within the cost constraints for Edge Computing to become pervasive.

There are other regulatory and policy issues at play, such as device data being collected and stored in a Cloud may cross-jurisdictional boundaries, raising liability issues if the data leaks. This is especially important if data is of personal nature, e.g., related to shopping patterns or patient health records.

5. TRUST MODELS FOR IOT DEVICES

Attacks have been made exploiting a component level vulnerability. Most security systems are designed using Capability models. A capability model usually takes into account how various services are utilized. For example, we can start with a multi-dimensional structure, composed of:

1) Hardware: An ASIC or programmable microcontroller.
2) Operating System: Windows, Linux, Android etc.
3) Applications: nature of application, and its privilege level.
4) Manner in which various components, services and utilities are deployed:

    a) e.g., kernel, library services, files accesses,
    b) Manner in which objects (username, application, function) get authenticated,
    c) What kind of cryptography is utilized, e.g., strength of MD5 vs. SHA256.

We propose to evaluate a given HW and SW solution components composed of one or more IOT devices connected to a Cloud server, based on the robustness and trustworthiness of this entire solution stack, with a multiplicative serialized model, e.g., in the following order:

1. Native compiled code is trusted more
2. Then anything using an external library
3. Lastly, any third party SW attempting to integrate

Using the above method, it is possible for us to evaluate trust of different operating systems with applications from diverse fields. Goal is to create a framework for evaluating and assigning a security score to each layer and then compute a composite score. A given application can be disassembled to see whether it is using a kernel service, or a utility in the user-space, or a built-in-library etc.

For each component in the stack, a list of orthogonal properties are established followed by an objective scoring system for each property. Numerical score for a utility function depends on the manner in which it is accessed, e.g., read (as a call by value), or a write (call by reference). A Security Score can computed by answering a set of questions by a user or automatically computed by a testing tool. Example of questions include:

- Whether a salt is used hash passwords?
- Which algorithm is used for hashing: MD5 or SHA256?
- Does the communication channel use SSL and which version of TLS is being used?
- What is the version of MYSQL in operation?

Another Security Score determination method: Whether port 3306 used by MySQL is open to the world or just to the application servers that use the MySQL database. This score can be continuously updated during the operations. More importantly, it needs to be updated after a maintenance or upgrade action is completed.

Security Score questionnaire may focus on the best practices during development. Automated score calculation focuses on the system operations. An OS without the latest patch can be at a security risk.

Security Score computations has two outputs:

1. **Probability of a successful attack:** What is the probability that an attack on this device will succeed?
2. **Probable Impact of a successful attack:** What is the probable impact if the attack succeeds?

The Security Score (S) can be computed as follows:
S = 1 - Pa * Pi
Where:
Pa - Probability of the attack in the range 0 to 1
Pi - Probable impact if the attack succeeds in the range 0 to 1
Pa * Pi - is the expected loss

This score is for a single component. By describing the security-wise relationship among the different components and their individual security scores, the whole system security score can be computed.

The factors that affect the probability of attack include:

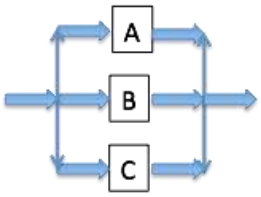
- Presence of a vulnerability existing and known to attackers
- Level of focus on products of this type by hackers
- History of exploitation of this product type

Probable impact of a security attack is defined as the sum of any regulatory fines, reputational damage and operational loss. This represents the resulting loss of trust in product and services. This needs constant monitoring for security breaches and policy updating [5].

The first step in the modelling is describe the whole system in terms of its components hierarchically organized and security-wise connections between the components could be serial or parallel.

The direction lines in figure 3 represent the security-wise relationship between the blocks in a system. In figure 3(a), to all the blocks should be secure for system to be secure and provide the required functionality. In figure 3(b), any one of the blocks should be secure for the system to provide the required functionality. The composite Security Score can be computed by applying the series-parallel reliability rules [6], as shown in Figure 3.

$S_S = S_A * S_B * S_C$



$$S_S = 1 - (1-S_A)^* (1-S_B)^* (1-S_C)$$

Figure 3: Risk levels of series-parallel systems

6. AN EXAMPLE STUDY OF TRUST SCORING

Raspberry PI is the de facto choice and starting point for many IoT devices. This choice is driven by its ubiquity and low price, making it a popular controller for many home and entry level appliances. An higher installed base also makes it an attractive target for hackers, therefore we evaluated it for our IoT trust model. For our sample system, we restricted probability values to High (0.9), Medium (0.6) and Low (0.3). Similarly, the impact values were also High (0.9), Medium (0.6) and Low (0.3).

We took an implementation of a Raspberry Pi Model 3B with Raspbian OS Ver 4.14 released on 2018-4-18 as a reference system for trust scoring [7]. The base Raspberry Pi system comes with a microSD card, which holds the OS and can be used to install additional software. The factory settings and factory shipped software packages for the OS were used for trust scoring. No packages were updated. Once the basic model trust scoring was complete, we proceeded to complete the Raspberry Pi based Security Camera setup [8]. Following additional software components were installed, as depicted in Figure 4:

1. MongoDB
2. Rabbit MQ
3. AWS IOT client
4. MotionPie software

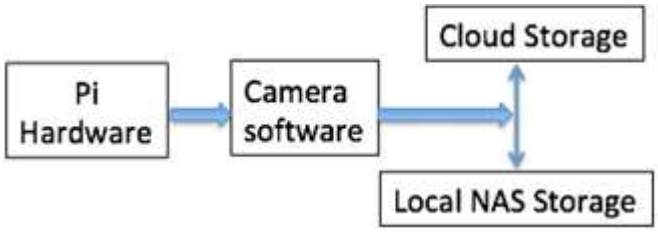


Figure 4: Series-parallel implementation of our Prototype

We use Mongo DB to have a NAS (Network Attached storage) of images, and the AWS IoT client to connect with Amazon's backend service for cloud storage. MotionPie is an image processing software to detect motion, and then decide which video clips need to be saved or discarded.

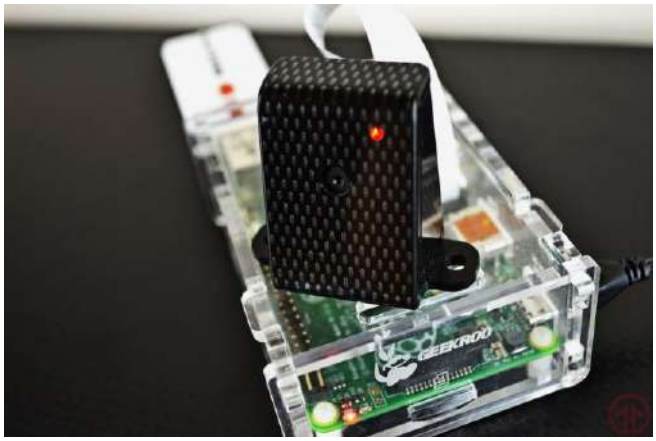


Fig 3: A simple Raspberry Pi based Camera system [6]

A problem with this security camera prototype is that someone with a physical access to local system can easily switch the software. There is no method to check if the system software is authenticated at boot time, so the base hardware setup has a high probability (0.9) of an attack. The impact probability of such attack is also high (0.9) as the base system can be fully compromised.

In the default setup, the user name is "admin", and password is blank. It is easy for someone to remotely hijack and use this camera in a Mirai botnet attack [9]. After the password has been changed, and if the camera is installed behind a secure firewall, the probability of such an attack is medium (0.6). However, the impact probability is high (0.9). Our proposed system uses AWS IOT security model [10], with X.509 certification with asymmetric keys [8]. On the backend, where the images are stored, the security is high so probability of an attack is low (0.3) and impact probability is also low (0.3), since the images have a local storage as we as well cloud based storage. Even though the local system can be attacked with a higher probability (0.9) and medium impact (0.6).

Overall, we have the Raspberry hardware and software components in series security-wise, which itself is in series with two parallel storage systems security-wise. At component level, here is what we have so far:

$$Sc = 1 - 0.9 * 0.9 = 1 - 0.81 = 0.19$$
$$Ss = 1 - 0.6 * 0.9 = 1 - 0.54 = 0.46$$

and for the storage systems,

$$Sgc = 1 - 0.3 * 0.3 = 0.91$$
$$Sgl = 1 - 0.9 * 0.6 = 0.46$$

Where, Sc is the security of camera, Ssis the security of software, Sgc is the security of cloud storage, and Sgl is the security of local storage. As cloud storage and local storage are in parallel providing redundant functionality, the security score can be computed using reliability parallel chaining rule:

$$Sg = 1 - (1 - Sgc) * (1- Sgl)$$
$$= 1 - (1 - 0.91) * (1 - 0.46)$$
$$= 1 - (0.09 * 0.54) = 0.9514$$

Finally, the end-to-end system level security protection score for an attack is a composite of three scores = 0.19 * 0.46 * 0.9514 = 0.07which is only 7% or very low. This means that the entire camera system is prone to attacks. However, we can still use it due to our added security measures of a strengthened password, dual storage in the local and cloud based databases etc. Thus, one of the two paths needs to be secured to continue the required functionality: Path (a) Camera → Software → Local NAS, or Path (b) Camera → Software → Cloud Storage. Note that all past images will still be preserved even if the system is compromised up to the point of intrusion, e.g., if someone physically removes the microSD card on a security camera. If a home or business uses such a system, it may need multiple cameras so if one of them is compromised, others will continue the surveillance. An example is of 5 Pi cameras, with a shared local NAS and common cloud storages. The Security Score for the camera and software part is computed as 1 - (1 - 0.19*.46)^5 =0.36. The entire system security will be 0.36*0.9514 = 0.34 or 34%. This improves the total system security by almost 5X. Another way to achieve a better security is by making it harder to compromise a single camera system, e.g., by putting it in a cage so its microSD card can't be easily replaced. Then the probability of a physical attack goes from high to low, such that Sc = 1 - 0.3 * 0.9 = 1 - 0.27 = 0.73. The overall score for such a single camera system would be 0.73*0.46*0.9514 = 0.32, or 32%, which is almost same as our 5 parallel cameras system, albeit at a much cheaper cost. However, it also represents a single point of failure, so the real choice may be a combination of both. This can be achieved by using two secure camera systems in parallel, as redundancy is important to improve security.

7. SUMMARY

In this paper we review the scope of various IoT (Internet of Things) devices in the field that are bi-directionally connected to data-centers (in-house or cloud) via various networks. Then we look at the nature of security issues, and mechanisms to quantify risk associated with the complete hardware and software stack, with an example of a typical surveillance camera system. We calculated system security, and suggested ways to improve it. Our proposed method can be extended to evaluate any IoT system, and improve its end-to-end security profile.

8. ACKNOWLEDGEMENT

We wish to acknowledge help from Prof.Pramod Chandra P. Bhatt for giving the initial idea of a quantitative composite Trust Model for IoT devices. He has been a constant source of inspiration for this work, guiding us to completion. Prof. Bhatt can be reached at bhatt_pcp@consultant.com.

REFRENCES:

[1] N. K. Sehgal, S. Sohoni, Y. Xiong, D. Fritz, W. Mulia, and J. M. Acken, "A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing," IETE Technical Review, Volume 28, Issue 4 [p. 279-291], 2011

[2] https://www.statista.com/statistics/370350/internet-of-things-installed-base-by-category/

[3] N. K. Sehgal, PCP. Bhatt, " Cloud Computing: Concepts and Practices," Springer Publications© 2018, ISBN 978-3-319-77839-6

[4] https://medium.com/@MarutiTech/what-is-serverless-architecture-what-are-its-criticisms-and-drawbacks-928659f9899a

[5] R. Sandhu, A.S. Sohal and S. K. Sood, "Identification of malicious Edge Devices in fog computing Environments," Information Security Journal: A Global Perspective, Volume 26, 2017, Issue 5.

[6] http://web4.uwindsor.ca/users/f/fbaki/85-222.nsf/0/b7d85091e772a10185256f84007be5c1/$FILE/Lecture_07_ch6_222_w05_s5.pdf

[7] https://www.raspberrypi.org/downloads/raspbian/

[8] https://pimylifeup.com/raspberry-pi-security-camera/

[9] https://www.sentinelone.com/blog/iot-botnet-attacks-mirai-source-code/

[10] https://aws.amazon.com/blogs/iot/understanding-the-aws-iot-security-model/

AUTHORS

NARESH is the Data-center Security and Privacy Director at Intel Corp. He has been with Intel for 28 years in various roles, including EDA development, Silicon Design Automation, Intel-HP Alliance management and for launching Virtualization technology on all Intel platforms. Naresh holds a PhD in Computer Engineering from Syracuse Univ., and MBA from Santa Clara Univ. He holds 5 patents and authored 30+ publications in the CAD domain.

SHIV SHANKAR is the founder of mapshalli.org, a social organization helping citizens and governments with technology. He was the Director of Enterprise Software Technology in Intel. He has a Master's degree in Mechanical Engineering from IIT, Madras, India.

JOHN M. ACKEN is a faculty member in the Electrical and Computer Engineering Department, Portland State University, Portland, OR. John received his BS and MS in Electrical Engineering from Oklahoma State University and Ph. D. in Electrical Engineering from Stanford University. He projects include technology and devices for information security and identity authentication. John has worked as an Electrical Engineer and Manager at several companies, including the US Army, Sandia National Labs in Albuquerque, New Mexico and Intel in Santa Clara, CA. John's time in the US Army was in the Army Security Agency, a branch of NSA during the Vietnam War.

INTENTIONAL BLANK

VIRTUAL ENTERPRISE ARCHITECTURE SUPPLY CHAIN (VEASC) MODEL ON CLOUD COMPUTING: A SIMULATION-BASED STUDY THROUGH OPNET MODELLING

Tlamelo Phetlhu and Sam Lubbe

Faculty of Commerce, Administration and Law, University of Zululand, Kwa-Zulu Natal, South Africa

ABSTRACT

The traditional models of electronic data interchange (EDI) and out-of-application methods for messaging and collaborations are not suitable to achieve the full benefits of VEASC because of multiple limitations. The limitations are: multiple human interventions, lack of real time visibility into the supply chain flows, inability to accurately synchronise the demand and supply-side information, and inability to build dynamic capabilities required for facing supply chain dynamics. The existing studies about deploying supply chain applications on cloud computing are focussed on overcoming these limitations through service-oriented architectures and their components. However, their focus needs to be expanded to virtual enterprise architecture modelling to overcome the limitations of EDI and out-of-application methods effectively. The virtual enterprise architecture supply chain (VEASC) model has been studied in this research employing Optimised Networking (OPNET) modelling and simulations of a commercial application called INTEND. The simulation results reflect a potential to overcome the limitations of traditional EDI and out-of-application methods. However, the true potential of the proposed system and the changes needed to automatically recover from failures can be determined after testing actual transactions in a real world VEASC implementation.

KEYWORDS

Supply chain, enterprise architecture, integration, collaboration, communications, strategic partnership, cloud computing, Optimised Networking (OPNET), modelling, simulations, simple object access protocol (SOAP), eXtensible Markup Language (XML)

1. INTRODUCTION

Strategic supplier management is possible on the foundations of coordination, collaboration, timely and accurate information sharing and communications between all the supplier echelons and the company managing them [1,2,3]. In its simplest representation, a supply chain may be viewed as a chain connecting three broad stages: raw materials acquisition, raw materials transformed into finished goods, and productions and services distribution and delivery to clients [2].

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 169-186, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90914

The value-chain model of supply chain (Figure 1) presents the bigger picture of integration, coordination, collaboration, and communications for enhancing effectiveness and efficiency of operations [1]. In the value-chain model, the supply chain may be viewed as a chain of stages between the suppliers and the customers [1,2,3]. The operations have their own cycles of processes and their underlying tasks that take inputs from the previous stage and feeding output to the next stage [1,2,3]. Hence, this model may also be viewed as the chain of cycles of operations [1,2,3]. The entire chain is supported by organisational support functions [1,2]. If the span of support by the support functions is extended to suppliers upstream and the customers downstream through the same system, the entire supply chain becomes a virtual enterprise [1,2]. The effectiveness of the operations of the stages is related to accuracy of their desired outcomes for meeting the customer demands, and the efficiency of the operations is related to responsiveness of the processes to the customer demands [2][4]. Hence, accuracy and responsiveness are the two fundamental targets for enhanced performance of a supply chain [2]. They are dependent upon an effective orchestration among the structural and functional units of a supply chain, achievable through the virtual enterprise model [4][5][6][7].

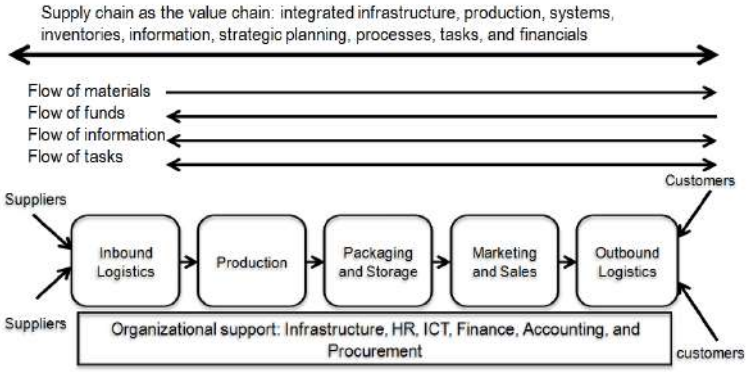


Figure 1: Value chain model of a supply chain (Source: Christopher, 2011, p. 14)

The effectiveness in orchestration of the structural and functional units of a supply chain are governed by strategic advanced planning and orientation of processes in accordance with the planning [4][8,9], strategic relationships management with the suppliers and customers [1][10,11,12], information systems and sharing framework with desired capabilities [13,14], strategic integration of the operations cycles of all the stages and their support functions (including suppliers and customers) [15,16,17], and effective collaboration, cooperation, and communications among the supply chain agents working in the echelons on their respective assignments [17,18,19]. An example of effective orchestration of structural and function units if a supply chain is found in the strategic market networks in which, the suppliers and the production companies integrate their structural assets and function units through cross-border integration of processes, collaboration and communication channels, and information sharing [12][20]. This form of integration can integrate diverse competencies, and innovations of different organisations to form an agile, flexible, and responsive supply chain for the customers that offers enhanced value and trust to the end-customers [10][12][20,21].

Modern supply chains are heavily dependent on information and communication technologies (ICT) for not only information sharing, but also in executing collaborations, communications, co-ordinations, managing operations processes and their tasks [14][22]. A properly design ICT

infrastructure with hardware, operating software, applications, workflows, and Internet integration is essential for managing and operating the virtual enterprise model [14][22]. An effective ICT infrastructure should also have ubiquitous access, platform independence, rapid and dynamic configurations, integration of multiple data sources [23,24]. The cloud computing is emerging as a platform for strategic market networking bringing together multiple suppliers and customers through an exchange facilitating exchange of funds with goods and services [24]. It is an enhanced form of the traditional electronic data interchange (EDI) and messaging and collaboration through out-of-application methods (like, e-mails and chat boards) carried out between self-hosted ICT infrastructures of suppliers and customers [23,24]. EDI and out-of-application methods require multiple manual interventions, lack real time supply chain visibility, and lacks synchronisation of demand and supply side information. Cloud computing in supply chains eliminates many delays that occur because of lack of integrated information sources and related manual processes required [23,24].

The virtual enterprise model of supply chain can be implemented highly effectively through cloud computing because the applications, their underlying workflow engines, and the databases are integrated with consolidated records stored by multiple supply chain agents [23,24]. Achieving highly integrated supply chain virtual enterprise with high levels of accuracy and responsiveness (linked with effectiveness and efficiency, respectively) is a new research area and is currently at conceptual stage. There are few research studies on how this can be implemented practically. Hence, currently the knowledge about supply chain virtual enterprise through cloud computing is not standardised amidst lack of actionable designs, approaches, and implementation planning. The existing studies have focussed on service-orientation concepts of supply chain applications and their components on the cloud computing. As reviewed in the next section, the concept of virtual enterprise and its realisation on cloud computing through web 2.0 service-oriented architecture and integrated processes, databases, and cloud tasks have been presented by the existing studies. However, existing studies on cloud-based enterprise architectures have not yet integrated these concepts for a realisable empirical design. Simply stated, existing studies have not investigated an actual framework of integration if virtual enterprise on cloud computing is extended to supply chains. In the absence of this framework, the limitations of traditional EDI and out-of-application methods cannot be eliminated effectively. This is justified as the following:

In absence of virtual enterprise architecture, suppliers and buyers will continue to operate as standalone virtual entities on the cloud computing. While their internal processes will be improved, collaboration and communications among them will require manual interventions. Perhaps, they may need EDI and out-of-application methods on the clouds. Their databases will be distributed and hence will lack an integrated real time visibility into the supply chain flows. The information units cannot be synchronised effectively between the suppliers and the buyers. Above all, there will be a very serious limitation. Because of disintegrated application processes and databases, the suppliers and buyers will lack dynamic abilities to quickly respond to dynamics and risks in their supply chains.

To extend the concept of virtual enterprise architecture to supply chains, it is important that the suppliers and buyers should form an integrated virtual organisation through a complex framework of strategic agreements (framework agreements) enabling them to operate as a single virtual entity. This is itself a complex phenomenon and requires separate studies. Assuming that the framework of agreements is already in place, some studies need to delve deep into how their

application processes and tasks will interact to truly enact the virtual enterprise on cloud computing. This is another focus area lacking in existing studies.

This study has been designed to model architecture of a virtual enterprise architecture supply chain (VEASC) on cloud computing. To study the model, multiple transactions have been configured and simulated in accordance with an application called INTEND. The overall performance levels studied through simulations reflect how a supply chain virtual enterprise can ensure high accuracy and responsiveness through cloud computing for the VEASC model. The next section presents a review of supply chains on the clouds.

2. SUPPLY CHAINS AND CLOUD COMPUTING

2.1. Introducing Cloud Computing

Cloud computing systems are consolidated architectures comprising thousands of servers, storage, and network systems interconnected through services oriented infrastructures, mostly run by service providers [25, 26]. Service orientation is achieved through virtualisation of servers and networking and through orchestration of computing, storage, and networking resources [25, 26]. Services are delivered through web services aggregators, service allocators, and dispatchers [25, 26]. The users are connected to applications through software as a service (SaaS) and the developers are connected to platforms through platforms as a service (PaaS). Both SaaS and PaaS systems run on infrastructure as a service (IaaS) [25, 26].

The services are offered to subscribers of cloud services through restricted access controls and security controls [27,28]. The subscription data is stored in cloud-based registries that comprise of the details of cloud subscribers and their access permissions [27,28]. The services contributors to the cloud offer Java or XML (extensible mark-up language) based interfaces to their application services [27,28]. The details of all such service interfaces on the cloud are stored in the service registries maintained under the service aggregators [27,28]. More details of such service-oriented applications are presented in the Section 3.

2.2. Enterprise Architecture on Cloud Computing

Before entering the next level of review about deploying enterprise architecture supply chains on the clouds, a brief review of enterprise architecture on cloud computing is presented. Cloud computing may be viewed as a service-oriented clustered and homogeneous platform that can be used as a foundation of the original enterprise architecture design [29]. The ICT infrastructure on cloud computing is elastic, dynamic, adaptive, lean, agile, optimised, and always available [29]. It can enable the enterprise architecture design because it is suitable for integrating business, data, technology, and application architectures on the same platform [29]. The processes on clouds are continuous and parallel as they need not be broken into individual discrete threads running on multiple self-hosted ICT systems and executed separately [29]. Cloud computing can run data intensive applications ubiquitously from laptops, computers, mobile devices, and pervasive devices, and query massive and distributed databases through concurrent distributed XML query threads [30].

2.3. Supply Chains on Cloud Computing

Supply chain echelons are integrated through cloud computing using specially designed applications that use web services and virtualisation [24][26,27]. Cloud computing enables the virtual enterprise model of supply chains in which, suppliers and manufacturers can form strategic arrangements with profit sharing, benefits sharing, innovations sharing, resources sharing, and risks sharing for shared access to the markets [31][38]. The workflow applications systems of multiple suppliers can be integrated through PaaS application development and delivery of runtimes [31]. The inter-systems communications are facilitated through standard XML and the users to systems communications are facilitated through Web 2.0 interfaces programmed on HTML 5.0 [25][32].

Integration through virtual enterprise requires extensive collaborations and communications among all the supply chain echelons and the support functions supporting them [1]. For ensuring long-term strategic relationships among supply chain partners, communications and collaborations need to penetrate through the organisational boundaries at all the levels of the organisational hierarchies [33]. The processes and their tasks among the supply chain partners are executed the way a massive single business enterprise operates [33]. The integration is required at the strategic level among the top management groups, at the tactical level among the middle management groups, and at the operations level at the lower management groups [34]. The entire framework should be globally operated and accessible [34].

Web services through clouds facilitate global integration of all participating organisations in the virtual enterprise and facilitate a single, large, and centralised platform for information entry and management, information processing, and information sharing [35,36,37]. The suppliers and manufacturers can use the global Inter-enabled platform for enhancing competitive value, innovation value, learning value, knowledge value, and financial value [38].

In the past, Internet has helped in establishing and integrating major workflows of a supply chain in the areas of materials requirements planning, procurements, scheduling of production and post-production tasks, strategic supplier relationships, and inventory control. Traditionally, electronic data interchange (EDI) between the suppliers' ICT systems and manufacturers' production and materials planning systems over private links or Internet has been the established system for information sharing [39]. Cloud computing is the next step when real-time transactions, collaborations, and communications have replaced EDI [40]. EDI required integration with internal and external applications for automating the transactions and enabling real-time visibility into the supply chain events [23] [40]. Further, EDI required to break the strong hierarchical boundaries of information domains and was operated at individual systems level rather than enterprise level [23] [40].

The review in this section reflects that existing studies have recognised the limitations of traditional methods and the value of virtual enterprise integration on cloud computing to eliminate those limitations. However, an empirical framework for achieving it in real world supply chains has not evolved. The technical knowledge is already formed in the cloud computing literature. A researcher needs to extend this knowledge in forming an empirical model of virtual enterprise architecture for supply chains by exploiting the integration abilities of cloud computing. A practical insight is needed into the service-oriented designs for achieving a virtual enterprise of integrated suppliers and buyers. To gain a better understanding, a review of service-

oriented applications integration on cloud computing is presented in the next section. This part of the review has also helped in modelling a multi-party supply chain application in OPNET.

3. SERVICE-ORIENTED APPLICATIONS INTEGRATION ON THE CLOUD COMPUTING

Service-orientation in supply chain can help in requesting a service offered by any participating organisation on the cloud and the cloud system ensures that the service is searched and delivered to the requester [31]. For example, by simply executing queries written in XML web services description language, a procurement manager can fetch information on current products in the catalogue, their availability in the inventories of the connected suppliers, prices and discounts offered by the suppliers offering the product, location of the products, and expected lead time of delivery [28][31]. Cloud computing is a virtualised ICT infrastructure having multiple virtual domains each owned by a participating organisation [41]. The databases managed by the participating organisation can be deployed on the cloud as a public service or run within the virtual domains of the respective owners [41]. In either scenario, the databases can run on multiple servers in parallel through parallel processing [41]. Hence, real time queries can be run on them without conducting EDI between the servers and the users [41]. For example, the product master databases, price master databases, ordering databases, and invoicing transactions databases managed by multiple organisations can be deployed on the same cloud [41]. An integrated XML query can be used to run on multiple databases in parallel and provide the output into a temporary data view space provided to the requester [41].

The applications, collaborations, and communications workflows can be integrated on cloud computing [42]. For example, collaborations can be designed on schedules, events, marketing, budgets and expenses, financial statements, presentations, task managers and monitors, web databases and spreadsheets, web apps, file sharing, web mails, web conferencing, online groupware, wikis, blogs, and social networking [42]. Hence, when a process task is in progress, all participants related to the task can have real time access to all resources and data to execute it [42]. Participants in the task can be hooked in real time irrespective of their location [42]. Natural language processing and time-zone management can break the barriers of multilingual and multicultural international integration [42]. This model may be viewed as value focussed process engineering, which integrates business constructs, risk management, business objectives, and objectives hierarchy of multiple organisations while a common task is being processed [43]. The integration comprises inter and intra-organisational process integration, operations integration, online cognitive integration, and collaborative integration [43]. This is like integrating physical, spatial, and temporal flows in the supply chain [43].

The choice of XML for processing, storing, and querying information is to ensure loose connections between the information presentation and the databases [28]. Many databases are stored in the form of XML data files, which have relational capabilities and supports parallel processing [28]. Data tables in modern databases can be exported into XML data files [44]. The XML data files are used in mobile data views as they can be fast and easily accessible through mobile apps running SOAP (simple object access protocol) engine [45]. SOAP can directly query XML data files [45]. SOAP can facilitate distributed and concurrent execution of XML scripts, XML threads, and execution libraries [25]. The applications hosted by contributing organisations to the web services infrastructure can have their XML data files spread across the cloud with

executions confined within the virtual boundaries [45]. These data files can be accessed through an SOAP apps-based light weight query execution from mobile phones [46], and also from desktop computers with SOAP engine deployed [47]. A user can query data files of multiple contributing organisations concurrently and quickly gain consolidated data views presenting integration information from multiple parties as needed in the task under process [42].

The database objects on the cloud computing are distributed among the server arrays spread across the world [48,49,50]. The locations of the database objects and their ownership details are allocated by the cloud resource manager and their details are stored in cloud objects registries [48,49,50]. The service allocation and dispatching agents can query the registries for identifying the locations of the database objects such that the queries can be broken into threads and sent to the objects for parallel query processing [48,49,50]. The registries also are XML DTD files with hierarchical structures, which help in identifying the objects against user requests and also help in negotiating access levels and service levels based on the subscription details of the users [48,49,50]. The runtime environments of the databases are allocated to users through their respective virtual machines, which comprises tools for building queries and data views generated after the queries are run in parallel on all the database objects throughout the cloud [48,49,50].

The concepts of technical design of a virtual enterprise using service-oriented architecture are adequately established in cloud computing literature. Assuming that a framework of integration agreements among multiple buyers and suppliers has been formed, a deeper view into the actual interactions of virtual enterprise applications is investigated in this research. The interactions should be planned carefully to ensure that there is no need for EDI and out-of-application methods within the framework such that their limitations stated in Section 1 are fully eliminated in the design.

With the above theoretical background, a cloud has been modelled in OPNET tool with some of the supply chain transactional processing in a commercial application, called INTEND, were modelled. The model is described in Section 5. The next section (Section 4) presents the research approach used in this research.

4. THE RESEARCH APPROACH

The research approach used in this research is modelling and simulations. The workflow for data collection and analysis used for this research is presented in Figure 2:

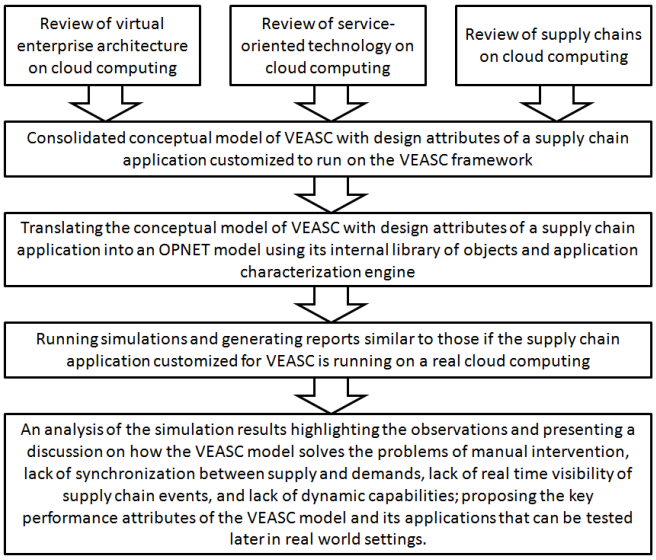


Figure 2: Workflow for data collection and analysis

The tool chosen for the research is OPNET, which is suitable for creating virtual test bed environment for ICT infrastructures and the applications running on them [51,52]. The tool is primarily a commercial network analytics engine used for designing, testing, and optimizing ICT infrastructures [51,52]. The academic version is available through OPNET university program, which limits simulation to 50 million events. The academic version contains most of the libraries of the commercial version and has features suitable for virtual test beds for academic applications. The libraries comprise of generalised objects supporting all technological attributes needed to model an ICT infrastructure, and also comprise of common commercial vendor model of products that can be configured the way the vendors have designed them.

In this research, a cloud comprising suppliers and procurement groups have been designed. More supply chain agents could have been modelled, but this design is sufficient to present the concept presented in this study. The server model objects are chosen from the OPNET library and interconnected through advanced switches to form the cloud. The supply chain applications and databases have been configured using the application and profile configuration objects and the supply chain transactions are configured using the custom application configuration object. The simulation span is 12 hours and the report comprises a number of parameters chosen. The traffic has been configured as exponential with standard predefined mean values as suggested by OPNET depending upon the loading profile selected in the application configuration object. By default the loading is chosen as high on all the databases supporting the application. Some deliberate delays have been introduced between two types of transactions. For example, the delay between delivery and invoicing has been configured as a minimum of one hour. The actual results depend upon the way the network is behaving while the transactions by all agents are in progress.

OPNET generates hundreds of reports after simulation. Given the limited space in this report, only the most relevant reports are shown. Given that reports related to all the devices on the cloud cannot be shown in the limited space on this document, only some samples have chosen. The full set of reports can be presented on request. The reports reflect the internal interactions between the supply chain agents through the applications and the databases.

5. MODELLING STRATEGIC SUPPLIER CONTRACTS ON THE CLOUD

The cloud model for virtual enterprise supply chain is as presented in Figure 2. This cloud is formed by Cisco Cat 6000 enterprise class switches and Compaq GS 320 enterprise class servers. In real world, these are high-end machines and hence have been perceived to be suitable for building a high performing cloud. The links are gigabit Ethernet links that can carry up to 1000 Mbps of data traffic. The capacity can be increased by adding more connections or using other faster technologies (like 10G and ATM). These links are available in OPNET objects library.

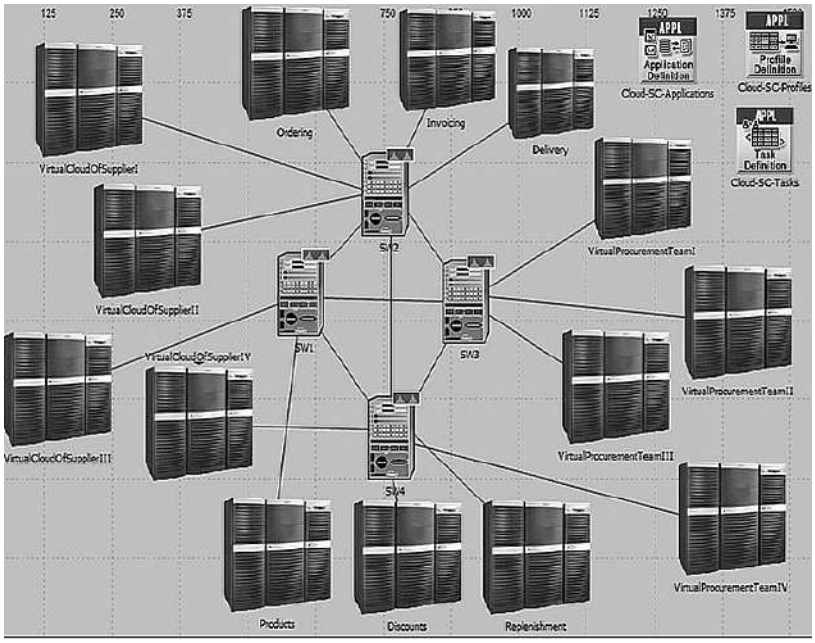


Figure 3: Cloud model for virtual enterprise supply chain designed in OPNET

The supply chain application modelled in this cloud is related to strategic supplier management in a virtual enterprise model. In the model four groups of suppliers (Virtual Cloud of Supplier I to Virtual Cloud of Supplier IV) and four groups of procurement teams (Virtual Procurement Team I to Virtual Procurement Team IV) are created. Each of the supplier group and procurement team is allocated one Compaq GS 320 server. In real clouds, there may be hundreds of servers allocated to them for running their applications. In addition to the suppliers and the procurement teams, one Compaq GS 320 server each is allocated to databases of ordering, invoicing, delivery, products, discounts, and replenishment.

A common application system is configured on the cloud. This application is called Procurement Process. It has a workflow comprising multiple phases of activities as described in Table 1. This workflow is configured using the custom application object in OPNET. OPNET has a process engine built within the custom application tool that can be used to configure significantly large workflows. For each phase of the workflow, a task is defined. The action taken on model (during simulations) is based on the tasks and also the design. For example, the database object named products DB is configured on the ordering server and the client runtime is configured on the servers for the procurement officers' and suppliers' groups. The cloud should be able to identify this server when the query executions on products DB are requested. In OPNET modelling, the

identification is carried out through a destination preferences setting in each of the requesting server. This object configuration comprises records of all the application components and their respective destination servers. This may be viewed as similar to the services registry on cloud computing.

Table 1: The process for operating the framework agreement

Phase no.	**Task Description**	**Action on the cloud**
1	The procurement team retrieves details and identification of the products that they planned to order. The service request is made to the products database.	The cloud dispatcher identifies the database objects pertaining to products DB and allocates the query to them. The query enters a queue waiting for its turn before other queries are executed.
2	The products DB replies to the service request.	All the details of the products requested by the procurement team are displayed on the application screen (example, an ordering form).
3	The procurement team retrieves details and identification of the products' prices and discounts that they planned to order. The service request is made to the discounts database.	The cloud dispatcher identifies the database objects pertaining to discounts DB and allocates the query to them. The query enters a queue waiting for its turn before other queries are executed.
4	The discounts DB replies to the service request.	All the details of the products' prices and discounts requested by the procurement team are displayed on the application screen (example, an ordering form).
5	The procurement team retrieves details and identification of the products' stocks that they planned to order. The service request is made to the replenishment database.	The cloud dispatcher identifies the database objects pertaining to replenishment DB and allocates the query to them. The query enters a queue waiting for its turn before other queries are executed.
6	The replenishment DB replies to the service request.	All the details of the products' stocks requested by the procurement team are displayed on the application screen (example, an ordering form).
7	The procurement team retrieves details and identification of the products' delivery lead times that they planned to order. The service request is made to the delivery database.	The cloud dispatcher identifies the database objects pertaining to delivery DB and allocates the query to them. The query enters a queue waiting for its turn before other queries are executed.
8	The delivery DB replies to the service request.	All the details of the products' delivery lead times requested by the procurement team are displayed on the application screen (example, an ordering form).
9	The procurement team now completes the first order and saves in the ordering database. This is called PO1.	The cloud dispatcher identifies the database objects pertaining to ordering DB and sends the PO1 data to be saved in the objects.
10	The procurement team now completes the second order and saves in the ordering database. This is called PO2.	The cloud dispatcher identifies the database objects pertaining to ordering DB and sends the PO2 data to be saved in the

Phase no.	Task Description	Action on the cloud
		objects.
The subsequent transactions are carried out by the suppliers' group.		
11	The supplier team gets access to the order details by running a query on the ordering DB.	The cloud dispatcher identifies the database objects pertaining to ordering DB and allocates the query to them. The query enters a queue waiting for its turn before other queries are executed.
12	The ordering DB replies to the service request.	All the details of the orders placed by the procurement team are displayed on the application screen (example, an order execution form).
13	Supplier group issues delivery instructions that are saved in the delivery DB. This is Delivery 1 against PO 1.	The cloud dispatcher identifies the database objects pertaining to delivery DB and sends the Delivery 1 data to be saved in the objects.
14	Supplier group issues delivery instructions that are saved in the delivery DB. This is Delivery 2 against PO 2.	The cloud dispatcher identifies the database objects pertaining to delivery DB and sends the Delivery 2 data to be saved in the objects.
15	Once the dispatch is confirmed (an automatic notification about Delivery 1 from the delivery team; not modelled in this workflow), the Invoice 1 is generated.	The cloud dispatcher identifies the database objects pertaining to Invoicing DB and sends the Invoicing 1 data to be saved in the objects.
16	Once the dispatch is confirmed (an automatic notification about Delivery 2 from the delivery team; not modelled in this workflow), the Invoice 2 is generated.	The cloud dispatcher identifies the database objects pertaining to Invoicing DB and sends the Invoicing 2 data to be saved in the objects.
The subsequent transactions are carried out by the procurement team		
17	The procurement team runs a query on the replenishment database to know the change in stocks of the products at the buyers end and also at the suppliers end. This is done to plan for the next ordering cycle.	The cloud dispatcher identifies the database objects pertaining to replenishment DB and allocates the query to them. The query enters a queue waiting for its turn before other queries are executed.
18	The replenishment DB replies to the service request.	The details of stocks at the buyers' and customers' ends are displayed on the screen (like, replenishment form).

This workflow is formed with the help of a running procurement application named INTEND in the researcher's organisation. For modelling this application, some of the steps in the original application have been eliminated to make it simple and relevant. In real world, the workflow will be much more advanced and complex. For example, the workflows of packaging, transportation, materials inspection reporting, and later running a forecasting module for replenishment can be added in this workflow. However, the purpose of this study is to investigate how an integrated workflow for integrated suppliers and procurement teams of multiple organisations on the cloud works for the VEASC model. Hence, the workflow has been kept shorter than the original application. In the next section, the simulation results have been presented and analysed.

6. SIMULATION RESULTS

The workflow is simulated with 100 users load on each cloud server (400 users in suppliers' groups and 400 users in the procurement teams). The model is simulated assuming that all the users are online on the cloud operating their transactions. The simulation screenshot in Figure 3 shows the results of three phases of the procurement process cloud application: ordering, delivery, and invoicing.

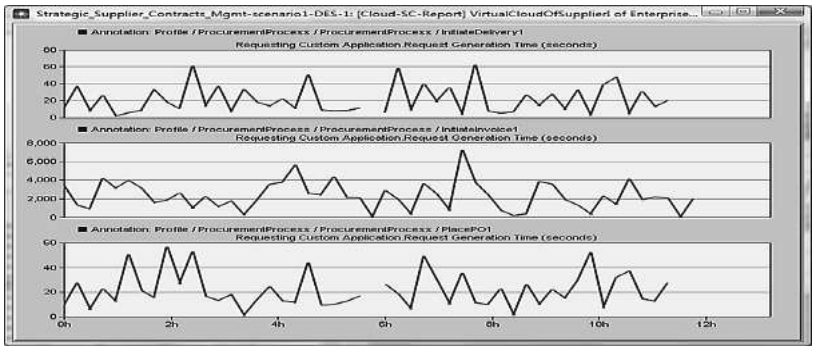


Figure 4: Simulation results of three phases of the cloud application for the first servers of suppliers and procurement groups

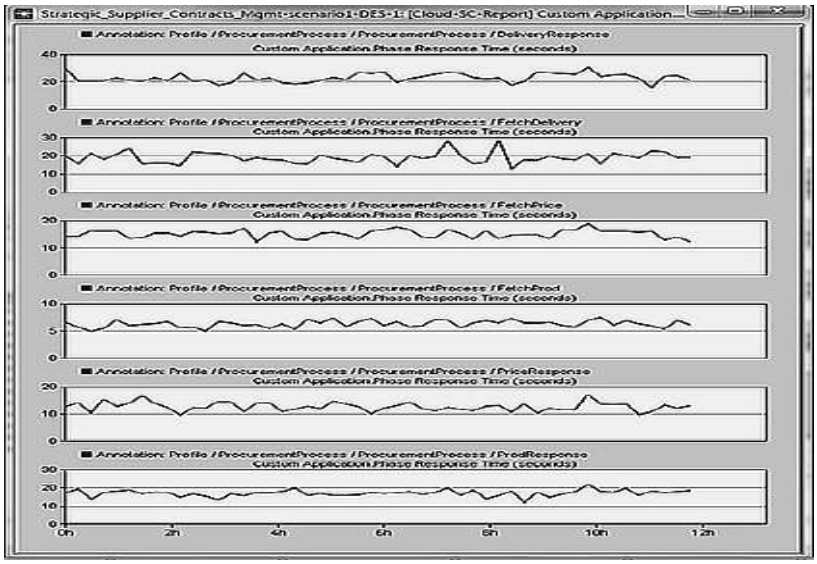


Figure 5: Simulation results of some of the process threads comprising query initiations and query responses

The delivery initiation transactions are occurring almost concurrently with the ordering initiation transactions (Figure 4). The invoice initiation transactions are occurring within couple of hours assuming that the stock verification and delivery instructions are issued within this period. The phases of packaging, transportation, delivery, and materials inspection are present in the INTEND application but eliminated here because they will require a few days of simulations, which is not possible in the academic edition (the academic edition of OPNET allows 50 million events in the simulation). In this research, the simulation carried out is of about 12 hours. The process names

(like, FetchProd, FetchDelivery, PriceResponse, and ProdResponse) have been taken from the INTEND application. The results show concurrency of transactions executing all phases within the range of zero to 40 seconds. This performance is evident while there are four supplier organisations and four buying organisations collaborating and coordinating through this cloud.

While the phases of the strategic supplier management are executing for eight organisations comprising hundred users each, there have not been any stress on the databases. Simulation results of databases revealed that the average load is mostly in a few hundred milliseconds. How are these observations relevant to VEASC? A discussion and analysis in this context has been presented in the next section (Section 7).

7. DISCUSSION AND ANALYSIS

The VEASC model requires integration of all supply chain agents to a common synchronised framework of coordination, collaboration, and communications. Traditionally, the framework has been unsynchronised because of methods like EDI, e-mailing, posting updates, and live communications needing human interventions for completing all the phases of the supply chain processes. This may cause lower effectiveness and efficiency because of high dependence on speed of human responses. This problem has been reduced in cloud-based VEASC as the transactions are interconnected through the cloud without any manual system needed. Figure 5 shows almost continuous execution of tasks through integrated application instances and databases. There is no manual information sharing because the databases are relational and interconnected. For example, as soon as the suppliers update the stocks details, they are accessible to the procurement managers. There is no need for an EDI to share this information.

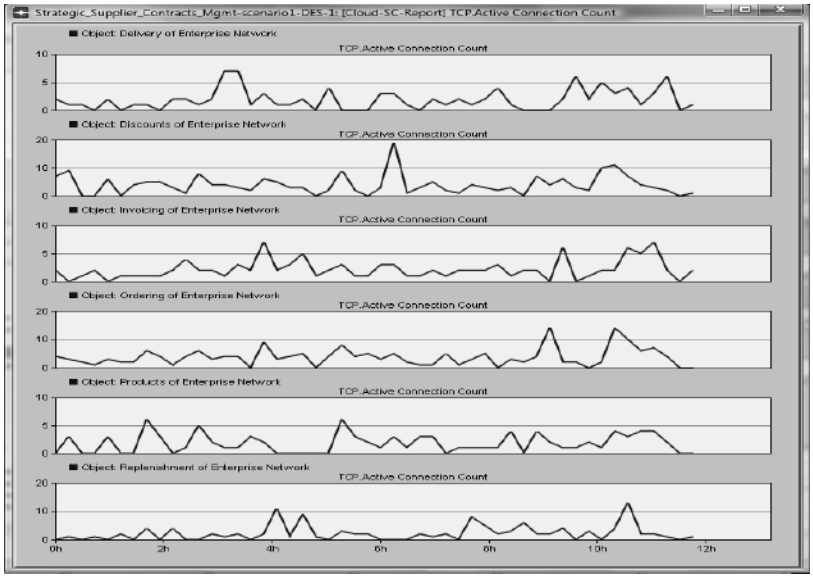


Figure 6: Number of active TCP sessions reflecting the active concurrent transactions occurring on the cloud databases

Figure 6 presents how the ordering application can access multiple databases simultaneously. The objects of these databases are in reality maintained by multiple organisations. In real clouds, they will be dynamically updating XML data files spread across thousands of servers on the cloud.

The transactions shown in Figure 7 are merely queries and data commits through SOAP. In the real world VEASC, all the supply chain functions can have their respective XML data files accessible to other agents. Separate XML data files may be used for collaboration and communications having records integrated with the integrated cloud views. Free text records, images, voice, and video files can be a part of the records presented in the data views. For example, while approving a payment an agent can view the order, the invoice, the delivery report, the inspection report with a video showing the inspections, and free text records entered by all supply agents involved in that order.

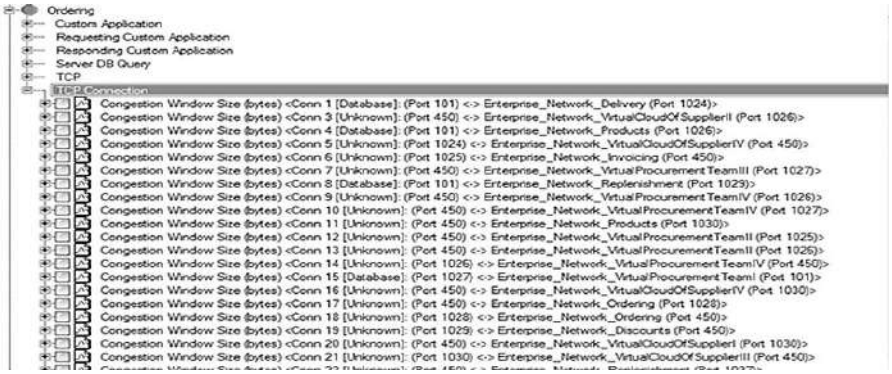


Figure 7: A screen shot showing part of all the TCP connections occurring on the cloud

The INTEND application modelled in this report currently lacks these features because it is not cloud-enabled. Hence, many out-of-application collaboration tools are needed (like e-mails and chat boards). The records of such collaborations and communications are not recorded within INTEND because of lack of integration such tools. This gap can lead to communication gaps while the content is available somewhere else but not readily accessible. The proposed model of cloud application can support VEASC because every possible transaction and collaboration/communication record can be accessible through the same record ID. This model makes every supply chain agent integrated and synchronised. There is little scope for manual intervention by individuals as the system integration is driving the transactions. The agents need to simply keep clearing their transactional queues as a routine. The participating agents can benefit from the shared values of the VEASC model. In this model every agent can avail repeatability, commonality, proportionality, value-sharing, shared risk management, shared advancements, and shared innovations. These are performance attributes projected for the proposed VEASC model, as explained below:

(a) Repeatability: The business processes and their tasks are closely integrated through shared cloud objects such that the results of committed transactions become shared knowledge entities. The knowledge and experience in handling them can be reused by all the members of the virtual enterprise thus enabling a gradual path of maturity.

(b) Commonality: The business processes and tasks can be standardised by establishing common conventions, codes, methods, and protocols (within the shared cloud objects) followed by each member of the virtual enterprise. No delays shall occur in translations or transformations of processes and tasks between any two entities.

(c) Proportionality: The volumes of transactions shall be proportionately distributed among the participating members depending upon their partnership share translating into proportionately shared benefits.

(d) Value-sharing: The value streams generated by this system shall be shared by all members as they are using a common service-oriented structure comprising shared cloud objects.

(e) Shared risk management: All members in the virtual enterprise will share common risks, as they are operating common business processes and sharing their cloud objects and databases on a common cloud platform. For example, if the application tasks listed in Table 1 are exploited by an attacker, or certain application processes fail, every member will face the resulting impacts.

(f) Shared advancements: Advancements in this system will benefit all members because of shared business processes and tasks.

(g) Shared innovations: The members of the virtual enterprise can jointly evolve new innovations in this system through shared research and development.

It is projected that this system is capable of automation, real time visibility into the supply chain events, close synchronisation of data generated by suppliers and buyers (as they are integrated within the virtual enterprise), and is capable of developing dynamic capabilities (quick response and agility) to face supply chain dynamism and uncertainties. Integrated cloud objects do not leave any room for delays in business processes, as reflected in Figures 4 and 5. In a traditional supply chain, the transactions of ordering and delivery initiation may be days apart. In this system, a delivery initiation occurs within a few seconds after order confirmation because of tightly integrated cloud objects. Further, there are no manual processes of negotiations, ordering, order confirmation, stock checking, and such other interactions requiring human intervention. With these projected claims, it is hereby suggested that simulations may not be a true reflection of actual performance of this system. There may be multiple practical challenges in operating the VEASC model in real supply chains. The simulation results have not highlighted such challenges in this study, because all transactions are modelled to be successful in their first instances. In real cloud applications, there may be chances of exclusive locks in databases, object corruptions, data corruptions, failure of certain threads, or even failure of hardware. The changes needed in the process flow to quickly detect such failures and activate remedies should be investigated further. In a fully automated system, instant identification of errors and failures and activation of quick remedies are highly critical.

8. CONCLUSIONS

In this study, a cloud computing model for enabling VEASC model of supply chain has been studied with the help of modulation and simulations in OPNET. The simulations revealed close synchronisation of all the phases of a procurement process because the application seamlessly interacts with the databases contributed by all the suppliers and buyers connected to the cloud. The model ensures full automation with human tasks directed by systemic integration rather than individual interventions. This architecture can be suitable for strategic integration of all the echelons of a supply chains extended to all suppliers and customers. The transactions flow

automatically both ways without any manual interventions. This cloud-enabled VEASC model of supply chain can be used for strategic market integration with every contributing agent sharing all the benefits of the collaboration. This model can enable competitiveness among suppliers, collaboration among multiple suppliers for serving common customers, auctions, online tendering, automated volume commitments based on replenishment records and forecasting, and such other functions. It can potentially enable automation, real time visibility into the supply chain events, synchronisation of demand and supply side data, and dynamic capabilities to face supply chain dynamics and uncertainties. The model reflects possibility of repeatability, commonality, proportionality, value-sharing, risk management, advancements, and innovations for all the contributing members. However, given that this research was simulation-based, all these projected possibilities need to be tested in a real world supply chain.

REFERENCES

[1] Christopher, M.: Logistics & Supply Chain Management, 4th Edition, Prentice Hall Global (2011)
[2] Chopra, S. & Meindl, P.: Supply Chain Management – Strategy, Planning, and Operation, Fourth Pearson International Edition, Worldwide: Pearson (2010)
[3] Cousins, P., Lamming, R., Lawson, B., & Squire, B.: Strategic Supply Management: Principles, Theories, & Practices, London: Pearson (2008)
[4] Surie, C. & Wagner, M.: Supply Chain Analysis, p. 37-64, Book Chapter: Supply Chain Management and Advanced Planning, 3rd Edition, Stadtler, H. & Kilger, C (Eds), Springer, Heidelberg (2005)
[5] Meyr, H. &Stadtler, H.: Types of supply chains, p. 65-80, Book Chapter: Supply Chain Management and Advanced Planning, 3rd Edition, Stadtler, H. & Kilger, C (Eds), Springer, Heidelberg (2005)
[6] Gunasekaran, A., Lai, K., & Cheng, T. C. E.: Responsive supply chain:A competitive strategy in a networked economy, Omega, Vol. 36, p. 549-564, Elsevier (2008)
[7] Jeschonowski, D. P., Schmitz., Wallenburg, C. M., & Weber, J.: Management control systems in logistics and supply chain management: a literature review, Logistics Research, 1, p. 113-127, Springer, Heidelberg (2009)
[8] Fleischmann, B. Meyr, H., & Wagner, M.: Advanced Planning, p. 81-108, Book Chapter: Supply Chain Management and Advanced Planning, 3rd Edition, Stadtler, H. & Kilger, C (Eds), Springer, Heidelberg (2005)
[9] Lambert, D. M., Garcia-Dastugue, S. J., & Croxton, K. L.: An evaluation of process-oriented supply chain management frameworks, Journal of Business Logistics, 26 (1), p. 25-51 (2005)
[10] Eggert, A. & Ulaga, W.: Managing customer share in key supplier relationships, Industrial Marketing Management, Vol. 39: p. 1346–1355, Elsevier (2010)
[11] Mena, C., Humphries, A., & Choi, T. Y.: Toward a theory of multi-tier supply chain management, Journal of Supply Chain Management, 49 (2), p. 58-77, Wiley (2013)
[12] Piercy, N. F.: Strategic relationships between boundary-spanning functions: Aligning customer relationship management with supplier relationship management, Industrial Marketing Management, 38: p. 857–864, Elsevier (2009)
[13] Kim, D., Cavusgil, S. T., & Calantone, R. J.: Information System Innovations and Supply Chain Management: Channel Relationships and Firm Performance, Journal of the Academy of Marketing Science, 34 (1), p. 40-54, Sage (2006)
[14] Qrunfleh, S. & Tarafdar, M.: Supply chain information systems strategy:Impacts on supply chain performance and firm performance, International Journal of Production Economics, 147: p. 340-350, Elsevier (2014)
[15] Kim, S. W.: An investigation on the direct and indirect effect of supply chain integration on firm performance, International Journal of Production Economics, 119, p. 328-346, Elsevier (2009)
[16] Kim, D.: Relationship between supply chain integration and performance, Operations Management Research, Vol. 6, p. 74-90, Springer (2013)

[17] Kim, D., Cavusgil, S. T., & Calantone, R. J.: Information System Innovations and Supply Chain Management: Channel Relationships and Firm Performance, Journal of the Academy of Marketing Science, 34 (1): p. 40-54, Sage (2006)
[18] Samaranayake, P.: A conceptual framework for supply chain management: a structural integration, Supply Chain Management: An International Journal, 10 (1), p. 47–59, Emerald (2005)
[19] Attaran, M. & Attaran, S.: Collaborative Supply Chain Management: The Most Promising Practice for Building Efficient and Sustainable Supply Chains, Business Process Management Journal, 13 (3): p. 390-404, Emerald (2007)
[20] Holweg, M., Disney, S., Holmstrom, J., & Smaros, J.: Supply Chain Collaboration: Making Sense of the Strategy Continuum, European Management Journal, 23 (2), p. 170-181, Elsevier (2005)
[21] Simatupang, T. M. & Sridharan, R.: Design for supply chain collaboration, Business Process Management Journal, 14 (3): p. 401-418, Emerald (2008)
[22] Jitpaiboon, T.: The Roles of Information Systems Integration in the Supply Chain Integration Context - Firm Perspective, Published Doctor of Philosophy thesis, p. 1-279, The University of Toledo, UMI Microform 3188242, ProQuest Information and Learning (2005)
[23] Cegielski, C. G., Jones-Farmer, L. A., Wu, Y., & Hazen, B. T.: Adoption of cloud computing technologies in supply chains: An organizational information processing theory approach, The International Journal of Logistics Management, 23 (2), p. 184-211, Emerald (2012)
[24] Jun, C. & Wei, M. Y.: The Research of Supply Chain Information Collaboration Based on Cloud Computing, Procedia Environmental Sciences, 10: p. 875–880, Elsevier (2011)
[25] Buyya, R., Vecchiola, C., & Selvi, S. T.: Mastering Cloud Computing Foundations and Applications Programming, Worldwide: Elsevier (2013)
[26] Barry, D. K. & Dick, D.: Web Services, Service-Oriented Architectures, and Cloud Computing, 2nd Edition, Worldwide: Elsevier (2013)
[27] Ouzzani, M. & Bouguettaya, A.: Efficient Access to Web Services, IEEE Internet Computing: p. 34-44.
[28] Srinivasan, L. & Treadwell, J. (2005), "An Overview of Service-oriented Architecture, Web Services and Grid Computing", p. 1-13, HP Research (2004)
[29] Raj, P. & Periasamy, M.: The convergence of enterprise architecture (EA) and cloud computing, p. 61-90, Book Chapter: Cloud Computing for Enterprise Architectures, Mahmood, Z. & Hill, R. (Eds.), Springer, Heidelberg (2011)
[30] Rao, N. R.: The convergence of enterprise architecture (EA) and cloud computing, p. 159-172, Book Chapter: Cloud Computing for Enterprise Architectures", Mahmood, Z. & Hill, R. (Eds.), Springer, Heidelberg (2011)
[31] Grilo, A, & Jardim-Gonclaves, R.: Cloud-Marketplaces: distributed e-procurement for the AEC sector, Advanced Engineering Informatics, vol. 27, p. 160-172, (2013)
[32] Ferguson, D. F. & Hadar, E.: Optimizing the IT business supply chain utilizing cloud computing, In 2011 8th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT), 2-3 Nov. 2011, New York, p. 1-6, IEEE (2011)
[33] Jun, C & Wei, M. Y.: The research of supply chain information collaboration based on cloud computing, 3rd International Conference on Environmental Science and Information Application Technology (ESIAT 2011), Procedia Environmental Sciences, 10, pp. 875-880 (2011)
[34] Prajago, D & Olhager, J.: Supply chain integration and performance: the effects of long-term relationships, information technology and sharing, and logistics integration, International Journal of Production Economics, 135, p. 514-522 (2012)
[35] Wu, I, Chuang, C, & Hsu, C.: Information sharing and collaborative behaviors in enabling supply chain performance: a social exchange perspective, International Journal of Production Economics, 148, p. 122-132 (2014)
[36] Monczka, R. M., Handfield, R. B., Giunipero, L. C. & Patterson, J. L.:, Purchasing and Supply Chain Management, 4th Edition, Cengage Learning Canada (2009)
[37] Meixell, M. J. & Gargeya, V. B.: Global supply chain design: A literature review and critique, Transportation Research Part E, 41, p. 531–550 (2005)

[38] Walters, P. G. P.: Adding value in global B2B supply chains: Strategic directions and the role of the Internet as a driver of competitive advantage, Industrial Marketing Management, 37, p. 59–68, Elsevier (2008)
[39] Lancioni, R. A., Smith, M. F., & Oliva, T. A.: The Role of the Internet in Supply Chain Management, Industrial Marketing Management, 29, 45–56, Elsevier (2000)
[40] Ranganathan, C., Teo, T. S. H., & Dhaliwal, J.: Web-enabled supply chain management: Key antecedents and performance impacts, International Journal of Information Management, 31: p. 533–545, Elsevier (2011)
[41] Kiroski, K., Gusev, M., & Ristov, S: IaaS Cloud Model for e-Ordering and e-Invoicing, In 2013 Federated Conference on Computer Science and Information Systems (FedCSIS), 8 - 11 September, 2013, Kraków, Poland, PTI, p. 105–110 (2013)
[42] Miller, M.: Cloud computing: web-based applications that change the way you work and collaborate online, IN: Que Publishing (2009)
[43] Nieger, D., Rotaru, K., & Churilov, L.: Supply chain risk identification with value-focused process engineering, Journal of Operations Management, 27, p. 154–168, Elsevier (2009)
[44] Lee, D., Kwon, J., Lee, S., Park, S., & Hong, B.: Scalable and efficient web services composition based on a relational database, The Journal of Systems and Software, 84: p. 2139– 2155, Elsevier (2011)
[45] Zhang, Q., Cheng, L. & Boutaba, R.: Cloud computing: state-of-the-art and research challenges, Journal of Internet Services and Applications, 11 (1), p. 7-18 (2010)
[46] Zhang, J., Levy, D., Chen, S., & Zic, J.: mBOSSS+: A Mobile Web Services Framework, IEEE Computer Society, p. 91-96, IEEE (2010)
[47] Wang, X.: Analysis on cloud computing-based logistics information network mode, IEEE Computer Society, IEEE, p. 1286-1289, IEEE (2011)
[48] Buyya, R., Ranjan, R., & Calheiros, R. N.: InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services, Hsu, C. H. et al. (Eds.), In ICA3PP 2010 – Part I, LNCS 6081, p. 13-31, Springer, Heidelberg (2010)
[49] Sakr, S.: Cloud-hosted databases: technologies, challenges and opportunities, Cluster Computing, Digital Objects Identifier: 10.1007/s10586-013-0290-7, p. 1-16, Springer, Heidelberg (2013)
[50] Grossniklaus, M.: The Case for Object Databases in Cloud Data Management, In ICOODB 2010, LNCS 6348, p. 25–39, Springer-Verlag Berlin Heidelberg (2010)
[51] Svensson, T. & Popescu, A.: Development of laboratory exercises based on OPNET Modeler, Published Master Thesis, Blekinge Institute of Technology, Sweden, p. 2-268 (2003)
[52] Dunaytsev, R.: Network Simulators: OPNET Overview and Examples, Department of Communications Engineering, Tampere University of Technology, p. 1-69 (2010)

SECURITY CONSIDERATIONS FOR EDGE COMPUTING

John M. Acken[1] and Naresh K. Sehgal[2]

[1]ECE Department, Portland State University, Portland, OR
[2]Data Centre Group, Intel Corp, Santa Clara, CA

ABSTRACT

Present state of edge computing is an environment of different computing capabilities connecting via a wide variety of communication paths. This situation creates both great operational capability opportunities and unimaginable security problems. This paper emphasizes that the traditional approaches to security of identifying a security threat and developing the technology and policies to defend against that threat are no longer adequate. The wide variety of security levels, computational capabilities, and communication channels requires a learning, responsive, varied, and individualized approach to information security. We describe a classification of the nature of transactions with respect to security based upon relationships, history, trust status, requested actions and resulting response choices. Problem is that the trust evaluation has to be individualized between each pair of devices participating in edge computing. We propose that each element in the edge computing world utilizes a localized ability to establish an adaptive learning trust model with each entity that communicates with the element. Specifically, the model we propose increments or decrements the value of trust score based upon each interaction.

KEYWORDS

Edge Computing, Security, Adaptive learning, Trust model, Threats, Cloud Computing, Information Security

1. INTRODUCTION

Edge Computing represents a combination of distributed computing connected to centralized servers. Historically, centralized versus distributed models have alternated as computing and communication capabilities have grown, while the limiting factor has alternated between computational capability and communication capacity. The present environment of cloud and edge computing is a complex mixture of computing capability, communication capacity, and security considerations. In this paper, we will focus on the security aspects of edge computing. Any such investigation must include multiple subtopics, e.g., protecting information content from observation and alteration, protection of operational capability from unauthorized access, protection of normal operation in the presence of malicious overloaded requests etc. Solution components need to consider prevention from and response to any security threats [1]. Examples of prevention include encryption to protect content from observation and alteration, access checking protocols to prevent unauthorized accesses, tracking mechanisms to identify attempted attacks, and blocking messages except from trusted devices.

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 187-194, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90915

2. BACKGROUND

Today's information technology environment contains a wide variety of computing resources and a multiplicity of communication channels between the various computing resources. Economics drove creation of large datacenters, and Cloud computing was born to utilize this enormous computing power. As capability of inexpensive computing continued ahead of the communications capabilities, computational power moved back to the end nodes of a system. The age of IoT (Internet of Things) arrived a decade ago as demonstrated by the fact that more things were connected to the internet than people in the world [2]. The "things" connected to Internet include sensors, controllers, and intelligent devices [3]. These devices have limited power to create security problems but they have even more limited ability to provide security solutions. To date the biggest security breaches in the IoT world have been instructions sent to the IoT devices, which then launched massive denial of service attacks on central servers. The top three examples are Mirai, Hajime and Persirai codes [4].

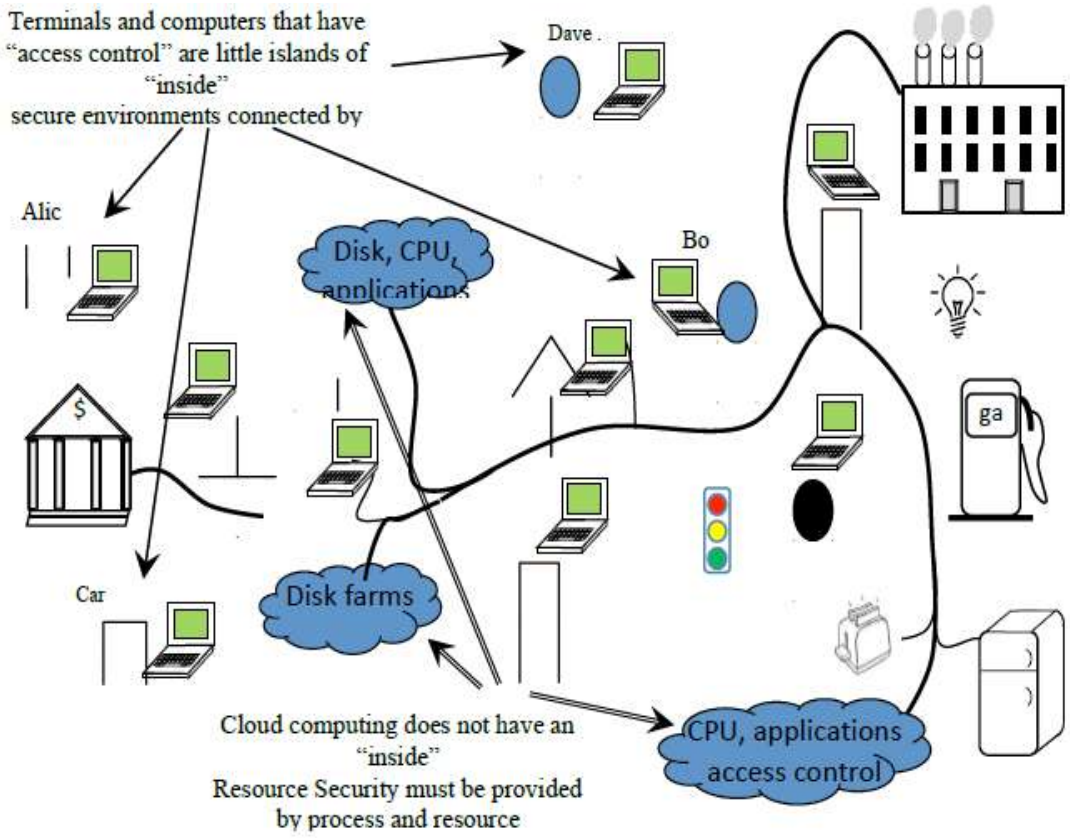


Figure 1. Variety of elements connected in the IoT world demonstrates security challenges, especially with a wide range of security requirements.

To visualize a wide variety of elements and security requirements in the IoT domain, consider Figure 1. The standard internet communication security approach (including virtual private networks, i.e., VPN) is to establish a link between Alice and Bob using access control to identify the authorized individuals and then to use encryption for information exchange between the "islands" of security containing Alice and Bob. Alternatively, Dave may want to do a transaction with his bank. Dave's transaction requires a higher level of security than Dave's normal activities. Carol may want to turn on her light bulbs at home since she will be arriving after dark. While this does not require a high level of security, Carol certainly does not want some random person

turning her lights on and off. Other examples of low levels of security are the household appliances, such as a toaster or a refrigerator. The high levels of security examples include opening a home garage, accessing banks or operating factories.

3. EMERGENCE OF EDGE COMPUTING

In the era of edge computing another consideration is due to multiple connection paths for each device. Each element on the edge can connect using a choice of paths or even multiple paths between the same endpoints. Specifically, any computing element on the edge can connect via the internet, telephone lines, cell phone connections, wireless local area service networks (WiFi), or local wireless point-to-point connects such as Bluetooth or NFC (Near Field Communication) etc. See figure 2 for multiple paths from Alice to Bob, to a local server hub, to the internet, or to the house alarm system. Edge computing continues to mature and encompass more of our world. Standards are being created such as Waggle [5], which is an open sensor platform for edge computing, has been introduced to reduce some of the foreseen compatibility problems.Edge computing security issues encompass end-to-end devices and the networks in between.

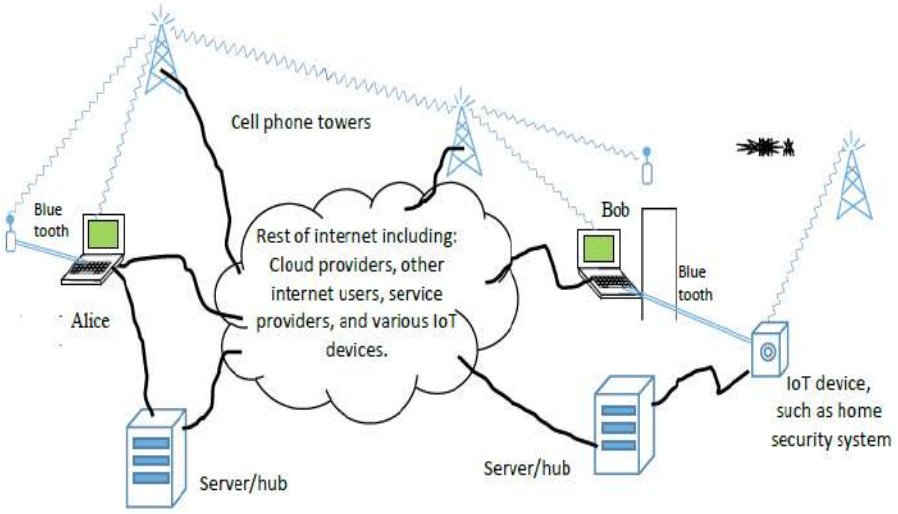


Figure 2. Communication connectivity from the edge

4. STATUS OF EDGE COMPUTING SECURITY AND RECENT BREACHES

The security issues for Edge computing often overlap with existing security problems. Access control using identity authentication is especially difficult in the IoT environment. Edge computing greatly increases the number of devices that need authentication. The pairwise authentication problem increases faster than exponentially (specifically the increase is N! where N is the number pairs) with increase in possible paths between the devices that need authentication. Added to the authentication problem, the problem of corrective action when unauthorized access is detected.

One of the largest attacks that Internet has ever experienced was recently launched using unsecure routers, digital video recorders (DVRs) and online surveillance cameras [6]. A collection of devices called botnet (an army of infected devices) was used to launch a Distributed Denial of Service (DDoS) attack on KrebsOnSecurity.com, the website of a Security journalist who had previously exposed cybercriminals. This attack generated > 660 Gbps of traffic, making it the largest attack on record in terms of data volume. In another case, a pair of researchers showed

that they could remotely hijack a Jeep's digital systems over the Internet. It led to a recall of 1.4 million vehicles [7], which required a costly fix after it was shown that a moving Jeep's steering wheel could be turned, unintended acceleration caused and brakes disabled remotely. Many homes have Internet enabled devices including thermostats, garage door openers, smart TVs etc. Such devices may contain vulnerabilities, enabling hackers to compromise a home, including changing the heating or cooling settings, opening garage doors and use TVs to connect with PCs on the home networks for stealing personal data [8].

Threat tracking and tracing are difficult for the IoT environment, but there are only a few channels through which an attack may travel. With Edge computing, definition and enforcement of the virtual protection boundary is difficult. Therefore, monitoring and responding to threats is the key. Fortunately, the increased computational ability of the elements at the edge also offers the potential for increasing the sophistication of the security monitoring and corrective responses.

5. SECURITY MODELLING TARGETING EDGE COMPUTING

Perimeter defence has long been insufficient for IoT security. Fixed protocols for boundaries of security with individual devices' security implementations will fail, because devices can have multiple channels of communications across boundaries.Each of these can be configured dynamically bypassing the fixed protocols. In addition, a fixed universal security policy is inadequate.However, components throughout the Edge computing environment must be adaptive in the sense that each device builds an individual trust model with the other devices to which it connects. This model must include monitoring to determine the level of trust applied to each individual connection between devices. The source device's trust (which sets the specific security policies and actions) increases based upon a history of successful connections and transactions with the responding devices. The source device's trust decreases based upon measured or detected failures for connections and transactions with the responding device. The decreased trust invokes increased security measures as will be described in a later section. Therefore, each device must learn who to trust and what level of trust to extend to other individuals and devices.

Each device may be part of the community of edge devices and cloud services. This community is similar to online communities of individuals and Hamilton et al describe the trust in an online community as a function of loyalty to the community [9]. Each edge device evaluates its trusted partners based upon preference, commitment, consistency vs surprise, and decisions or actions to be taken. The preference and commitment is established by the quantity and time spread of past communications. The measure of trust from one edge device to other entities is either increased by exchanges consistent with past exchanges or decreased by any surprisingly different exchanges. Thus, consistency increases trust and inconsistency decreases trust. The level of trust (based upon the past) and the immediate request drives a decision or action on the part of either the edge device or the cloud service component. A key to the success is the ability of each entity to learn and improve the measurement of trust.

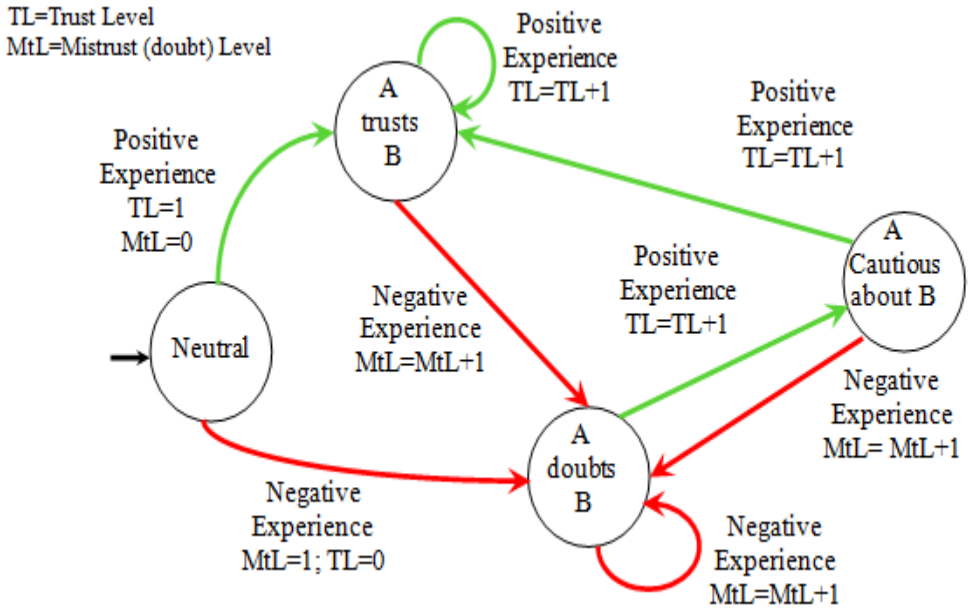


Figure 3. Element A's State of Trust Level of element B.

Table 1. Categories of Security Considerations for connection from A to B

Length and frequency of relationship	Purpose of relationship	History	Action Request	Severity and Urgency	Status of Trust	Response
New, first contact _ _ _ _ _ _ _ Short term many contacts _ _ _ _ _ _ _ Short term, few contacts _ _ _ _ _ _ _ Medium term many contacts _ _ _ _ _ _ _ Medium term, few contacts _ _ _ _ _ _ _ Long term	Casual _ _ _ _ _ _ _ Medical _ _ _ _ _ _ _ Legal _ _ _ _ _ _ _ Financial _ _ _ _ _ _ _ Schedule or calendar _ _ _ _ _ _ _ Employment _ _ _ _ _ _ _ Political _ _ _ _ _ _ _ Religious _ _ _ _ _ _ _ Ownership/ Property _ _ _ _ _ _ _ None/just Information _ _ _ _ _ _ _ National Security	Neutral _ _ _ _ _ _ _ Successful _ _ _ _ _ _ _ Failure _ _ _ _ _ _ _ Mixed successes _ _ _ _ _ _ _ Past success, recent failure _ _ _ _ _ _ _ Past failure, recent success _ _ _ _ _ _ _ Relationship change	Data or message delivery _ _ _ _ _ _ _ Data or message request or exchange _ _ _ _ _ _ _ Monetary transfer _ _ _ _ _ _ _ Physical Action _ _ _ _ _ _ _ Verification _ _ _ _ _ _ _ Open connection_ _ _ _ _ _ _ _ Attestation	Emergency _ _ _ _ _ _ Critical _ _ _ _ _ _ Casual _ _ _ _ _ _ Serious _ _ _ _ _ _ Unclear _ _ _ _ _ _	Mutual trust _ _ _ _ _ _ A trusts B _ _ _ _ _ _ B trusts A _ _ _ _ _ _ Mutual doubt _ _ _ _ _ _ A doubts B _ _ _ _ _ _ B doubts A _ _ _ _ _ _ Neutral	Ignore _ _ _ _ _ Store _ _ _ _ _ Respond _ _ _ _ _ Forward request _ _ _ _ _ Alert _ _ _ _ _ Perform action
	Multiple Possible		Multiple Possible			Multiple possible

The previous discussion proposes that information security is far more complex in the current computing environment. Not only does each participant (device, element, or person) require different security considerations, but each relationship between each pair of participants requires different security considerations. Additionally these security considerations change over time based on the past actions and new information. Table 1 summarizes the categories of considerations. It shows that each element in edge computing world needs a localized ability to establish an adaptive learning trust model with each entity that communicates with the element. Our proposed model limits and prevents the spread of a device failure from contaminating the whole system. As a consequence, the trust score of the compromised device shall be lowered.

Let us consider some examples of applying Table 1 and Figure 3. First, consider the case of a patient and physician. For our example: the first column is long term, the second column is both Medical and financial, the third column is successful. The action requested is to renew a prescription which is "data or message request or exchange" in column four. The severity in column 5 is Serious, and the Status of Trust in column 6 is Mutual trust. Therefore, the Doctor's response in column 7 is "Forward Request" to Pharmacy. The level of Trust in the state diagram remains B trusts A and the positive experience raises the Trust Level (TL). Secondly, consider that the patient's friend contacts the physician requesting medical history. This is a new, first contact, and column 2 is medical, History is neutral, action request is data request, Severity is serious but the status is neutral. Now for medical requests the response is multiple in both responding to the requester that this is protected information and alerting the patient that the request was made. The level of trust in the state diagram moves to mistrust because this was an unexpected and not previously authorized request resulting in negative experience. This will be modified with the patient's response to the notification from the physician.

Finally, consider interactions between two devices, for example, a connected car and a cloud computing resource. Specifically, the car's computer contacts the automotive maintenance centre to schedule a regular maintenance. From Table 1, column 1 we see this is a medium term relationship with few contacts. From column 2 we see it is both scheduling and financial. From column 3 we have successful. Therefore, from state diagram 3 we have a positive trust level for between both the car and the maintenance shop. The Action Request column is for data message exchange of data, time, and financial commitment. From column 5, the severity is Casual as it is not urgent or serious. As mentioned before, in column 6 we have mutual trust based upon the history and the state diagram. The action is to respond. Now consider that the car maintenance shop attempts to contact the car and drive it. The first column is still a medium term relationship with few contacts. However, in column two the purpose of the relationship does not match the action request from column 5. Because column 3 and 6 point to some level of trust, but the severity of the action from column 5 leads to a response of "Alert" and "Forward request" but not perform action.

The previous discussions concentrates on trust levels between two entities. However, in reality there are multiple entities involved in some trust relationships. As an example, some security protocols include a third party security certification. In addition, there are some security situations where a third party monitors or records transactions. These considerations will be explored in future work.

The application of Deep Learning for speech recognition is advancing [10], and it could be applied for speaker recognition for authentication and other security evaluations. The concept is to push some of the security decisions to the edge computing devices. The additional compute power at the edge is already being applied for decision-making using machine learning [11][12]. The future of security with edge computing and the cloud is a mix of central protocols in the cloud [13], decision making at the edge based upon machine learning, monitoring and analysing

communication activity[14]. A Machine Learning (ML) environment may allow the identification and defence against unexpected and unpredictable security challenges [15].However, ML is a double edged sword as hackers with access to training data can corrupt the learning process, or alter their attack code to specifically bypass a pre-determined security model [16]. There is a no silver bullet to ensure the security for all devices participating in Edge Computing, so a community based adaptive trust model may present an optimal solution.

6. SUMMARY

The present state of edge computing is an environment of vastly different computing capabilities connecting via a wide variety of communication paths. This situation creates both great operational capability opportunities and unimaginable security problems. This paper emphasizes that the traditional approaches to security of identifying a security threat and developing the technology and policies to defend against that threat are no longer adequate. The wide variety of security levels, computational capabilities, and communication channels require a learning, responsive, varied, and individualized approach to information security. We propose that each element in the edge computing world utilizes a localized ability to establish an adaptive learning trust model with each entity that communicates with that element.

REFERENCES

[1] N. K.. Sehgal, S. Sohoni, Y. Xiong, D. Fritz, W. Mulia, and J. M. Acken, “A cross section of the issues and research activities related to both information security and cloud computing,” IETE Technical Review, Volume 28, Issue 4 [p. 279-291], 2011.

[2] https://www.postscapes.com/internet-of-things-history/

[3] J. Ashton, "That 'Internet of Things' Thing", RFID Journal, Jun 22, 2009.

[4] http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

[5] P. Beckman, R. Sankaran, C. Catlett, N. Ferrier, R. Jacob and M. Papka , "Waggle: An open sensor platform for edge computing," 2016 IEEE SENSORS, Orlando, FL, 2016, pp. 1-3. doi: 10.1109/ICSENS.2016.7808975

[6] https://motherboard.vice.com/en_us/article/15-million-connected-cameras-ddos-botnet-brian-krebs

[7] https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[8] http://abc7chicago.com/technology/home-hackers-digital-invaders-a-threat-to-your-house/515520/

[9] W. L. Hamilton, et al., “Loyalty in Online Communities,” Proceedings of the Eleventh International AAAI Conference on Web and Social Media (ICWSM 2017). Pp 540-543.

[10] L. Deng et al., "Recent advances in deep learning for speech research at Microsoft," 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, 2013, pp. 8604-8608. doi: 10.1109/ICASSP.2013.6639345

[11] R. Nelson, “Smart factories leverage cloud, edge computing,” Evaluation Engineering, Vol. 56, No. 6, June 2017.b

[12] https://www.kdnuggets.com/2017/01/machine-learning-cyber-security.html

[13] Wei Li, "An adaptive security model for communication on cloud," Proceedings of 2011 International Conference on Computer Science and Network Technology, 24-26 Dec, 2011.

[14] R. Sommer, V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection" 2010 IEEE Symposium on Security and Privacy, May, 2010.

[15] https://www.information-age.com/machine-learning-cyber-security-123475346/

[16] https://www.technologyreview.com/s/611860/ai-for-cybersecurity-is-a-hot-new-thing-and-a-dangerous-gamble/

AUTHORS

JOHN M. ACKEN is a faculty member in the Electrical and Computer Engineering Department, Portland State University, Portland, OR. John received his BS and MS in Electrical Engineering from Oklahoma State University and Ph. D. in Electrical Engineering from Stanford University. He projects include technology and devices for information security and identity authentication. John has worked as an Electrical Engineer and Manager at several companies, including the US Army, Sandia National Labs in Albuquerque, New Mexico and Intel in Santa Clara, CA. John's time in the US Army was in the Army Security Agency, a branch of NSA during the Vietnam War.

NARESH is the Data-center Security Director at Intel Corp. He has been with Intel for over 30 years in various roles, including EDA development, Silicon Design Automation, Intel-HP Alliance management, and for launching Virtualization technology on all Intel platforms. Naresh holds a Ph.D. in Computer Engineering from Syracuse Univ. and MBA from Santa Clara Univ. He holds 5 patents and has authored 30+ publications in the CAD domain. He has co-authored a book on Cloud Computing published by Springer in 2018.

A MAPREDUCE BASED ALGORITHM FOR DATA MIGRATION IN A PRIVATE CLOUD ENVIRONMENT

Anurag Kumar Pandey, Ruppa K. Thulasiram, and A. Thavaneswaran*

Department of Computer Science, University of Manitoba, Winnipeg, Canada
*Department of Statistics, University of Manitoba, Winnipeg, Canada

ABSTRACT

When a resource in a data center reaches its end-of-life, instead of investing in upgrading, it is possibly the time to decommission such a resource and migrate workloads to other resources in the data center. Data migration between different cloud servers is risky due to the possibility of data loss. The current studies in the literature do not optimize the data before migration, which could avoid data loss. MapReduce is a software framework for distributed processing of large data sets with reduced overhead of migrating data. For this study, we design a MapReduce based algorithm and introduce a few metrics to test and evaluate our proposed framework. We deploy an architecture for creating an Apache Hadoop environment for our experiments. We show that our algorithm for data migration works efficiently for text, image, audio and video files with minimum data loss and scale well for large files as well.

KEYWORDS:

Cloud Computing, Private Cloud, Data Migration, MapReduce, Data Loss, Cost

1. INTRODUCTION

Cloud computing is an environment that enables resource sharing irrespective of the location of the user. Virtualization is the key to cloud computing, since it allows us to create multiple simulated environments or dedicated resources from a single, physical hardware system. A hypervisor is a software that connects directly to that hardware and allows to split one system into separate, distinct, and secure environments known as virtual machines (VMs). Thus cloud computing is used to provisioning of various services like Infrastructure as a Service, (IaaS), Software as a Service (SaaS) , Platform as a Service (PaaS) or Anything as a Service (XaaS) being offered to an individual organization. The above classification is based on the type of service, while public, private, hybrid or community cloud are cloud classification based on its deployment model [1].

There are multiple benefits of cloud [2] such as Elasticity, Cost Saving, Accessibility and Reliability. The public cloud, for example, represents a set of standard resources of varying types that can be combined to build applications [3] and the services are offered to clients for different purposes such as storage of files, etc. Cloud enables users to get computing resources/services over the internet irrespective of the location from a remote network of servers [4].

The significance of a private cloud over the public cloud is that important data can be stored with the minimum fear of it getting leaked over the internet. A private cloud can be maintained

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 195-212, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90916

anytime if organization(s) require it without depending on the cloud providers. However, there is a disadvantage in using a private cloud. If even a small portion of a server gets corrupted, it may lead to the data loss [5].

To address this problem, additional servers need to be installed in the private cloud to keep multiple copies of the same data, which can be used for data recovery. The additional server should function continuously without any hindrance and should always contain the up to date copies of the files present in the original server. Hence, any file that is added to the original server in the private cloud should be copied to additional servers. During server maintenance, the data may have to be migrated to different sets of servers. The data should also be deleted from the server initiating the migration because the data may be sensitive and should be avoided falling into wrong hands within the organization.

There are multiple approaches discussed in literature as presented later in the related work section. All these approaches focus on various aspects and issues of data migration. The major problem with these approaches is not having a generic solution to data migration problem. Each approach is best suited for a specific scenario or a particular data set. There is a need for building a framework that can efficiently migrate the data and calculate the data loss as well.

There might be data loses happening during migration. The few data migration approaches discussed above, do not compute the data loss accurately or may not even consider such loss. These existing approaches migrate data without any optimizing tools like MapReduce. This makes it difficult to compute the data loss during the transfer. Hence, there is a need for creating a novel framework that can efficiently migrate data without any data loss or minimal data loss. We are building such a framework that can efficiently migrate the data using MapReduce and also help in computing the data loss, if any. The overall objective and contribution from this research is:

1) Migrating the data efficiently without any loss in the data or minimum loss of data.
2) Designing an algorithm to reduce the time taken to migrate the data between the servers over the cloud.
3) Studying the scale effect by migrating a large amount of data in a short span of time.

1.1 Data Migration

Data migration refers to the process of moving data, applications or other business elements from an organization's onsite systems to the cloud, or moving them from one cloud environment to another system. There are different categories of data migrations in an organization through cloud computing. One of the most common category of data migration is the transfer of data and applications from a client's server to the public cloud. Another common category of data migration is the data migration between two servers of the same organization located in different locations. They can be located even in different continents but are transferred over the internet. The transfer may also be performed between two different platforms of a cloud and this is known as cloud to cloud migration. Data migration might also takes place from a cloud server to a local server or data center.

1.1.1. Types of Data Migration

There are various types of data migration that takes place over a cloud system. Most important types are briefly described below.

Storage migration is the process of migrating data from existing drives and locations into state-of-the-art drives elsewhere. This will provide more significant and faster performance, providing more scaling with more cost effectiveness [6]. This requires data management characteristics like cloning, backup and disaster recovery, snapshots, etc. The process takes time to perform validation and optimization of data and to identify outdated or corrupted data. It also involves migrating blocks of files and storage from a system storage to another irrespective of whether it is drive, disk or in the cloud. There are multiple storage migration techniques and tools which helps in smoother transition of the process. It also increases the chance of modernizing the storages and stop inefficient drives.

Database migration is the process of migrating data from one database to another. This is performed at times where there may be a necessity to shift from one database vendors to another, upgrading the software of the database or move the database to the cloud [7]. In this type of migration, the basic data may change, that may affect the application layer when there is a shift in protocols or data. This technique deals with modifying the data without altering the structure. A few key tasks include calculating the size of database for determining the amount of storage required, testing applications and making sure that the data will be confidential. There may be compatibility problems that may occur at the time of migration process, hence it is necessary to test the process first.

Application migration is the process of migrating an application from an environment or storage to another. This may include migrating the whole application or a part of it from a storage to cloud or between different clouds [8]. It may also include migrating the applications' main data to a newer form of application that is used by another provider. It is mostly used when an organization switches to another vendor platform or application. There are complexities associated with the process since the applications might interact with other applications, and every migration has its own data model. Usually, applications are not migrated since tools in the management and configuration in the virtual machines might change between different environments and due to change in operating system. Migration of applications may need other middle ware tools to bridge the gap in technology.

There are challenges associated with migration in the cloud. A lot of enterprises do not have the technical experience required for transferring between cloud systems or between servers over the cloud, which causes lots of disadvantages. A solution would be to outsource the work, which may lead to data theft or loss. Protection of sensitive data is important in cloud environment.

1.1.2. Lack of Migration Progress Management

Live data migration in cloud computing has uncovered major weaknesses in existing solutions that lacks progress management in the migration, the ability to predict and control the time of migration [9]. With no capability to control and predict the migration time control, the management tasks will not be able to attain the expected performance. If a system administrator requires to take down a physical machine for maintenance or for migrating the contents of the system to the cloud, the time management cannot be guaranteed and may disrupt the process and may lead to disruption of productive time in the business. The failure prediction systems that are applied may not detect the abnormal activities in the servers during the data migration. The migration is also be performed to balance the load [10]. These scenarios reveal the weaknesses in current live migration. Hence, the system administrator has to analyze and predict the time taken to complete the migration and ensure that the migration process is managed efficiently. In general, data migration seems simple and hence, managers, do not pay much attention on it, care less about the migration and maintenance of servers. However, there are huge implications [11]. The bandwidth is one of the major implications among those. The authors [11] also discuss

reducing the cost of processing the geographically distributed big data. The data that is transferred between the servers is usually huge and entire data may not reach the other server. A small corrupted block in the server (original/additional) may lead to a big failure. Addressing the problem of migration is complex and a separate industry has been booming and growing at a rapid pace. According to the reports by Thalheim et al. [12], in the past only 16% of the data migration projects had been completed successfully without any error. These authors have also mentioned that since the migration takes significant time, only 64% of the data migration project had a timely delivery.

1.2 Hadoop MapReduce

According to Apache Hadoop project, Hadoop MapReduce is a software framework for distributed processing of large data sets on compute clusters of commodity hardware [13]. The framework takes care of scheduling tasks, monitoring them and re-executing any unsuccessful tasks. According to the Apache Software Foundation [13], the primary objective of MapReduce is to split the input data set into independent chunks that are processed in a completely parallel manner.

From Figure 1, it can be seen that MapReduce contains two main functions known as Map and Reduce. The Map function converts the input data into intermediate Key / Value Pairs (KVP) format by grouping the data. A KVP contains data of two linked items which is a Key and a Value. The Key assigns a unique identity for the group of data, whereas the Value contains a pointer that points to the location of the data. The Map now has data in a structured manner along with the Key and Value assigned to it. This output is used as an input to the Reduce task. In the reduce task, it obtains the structured data i.e. intermediate KVP's and converts them into smaller structures. The KVP data for each group is stored in the Hadoop distributed file system (HDFS).

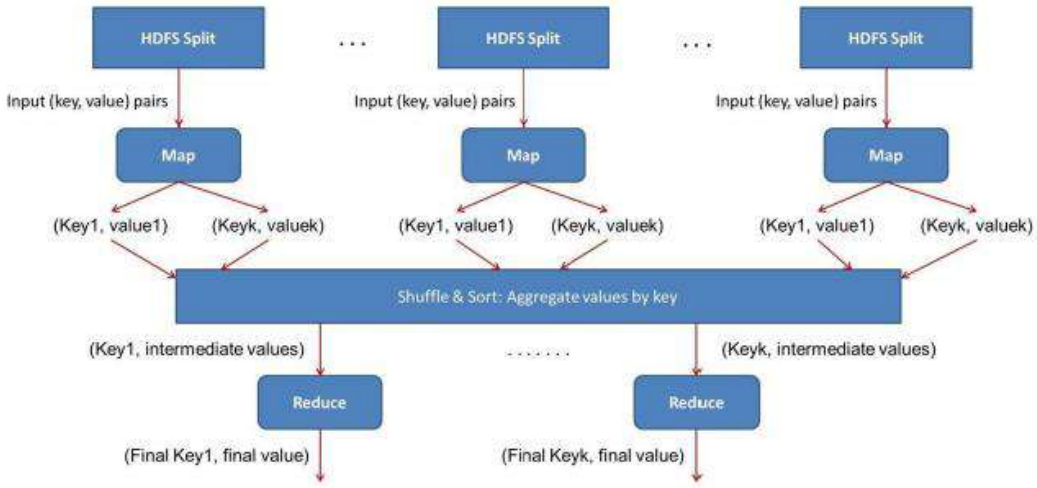


Figure 1: Basic functionality of MapReduce [14]

A MapReduce functionality is a type of work that consists of input data, MapReduce functionalities and the details of the configuration. Hadoop works by dividing the job into tasks as map tasks or reduce tasks. Two different types of nodes that control the job execution are a tracker node and multiple task trackers. These task trackers run the tasks allocated to them and send reports to the Job Tracker since it preserves the whole progress of every task.

The input to the MapReduce task is divided into fixed size pieces known as chunks or splits (64 MB chunks) [15]. It assigns a map task for each split when functions related to the users are recorded for every split. Having a lot of split means that the time taken to process every split is smaller while comparing to the time taken to process whole input at once. Hence, if the splits are processed in parallel, it will be faster when the splits are small, since system can perform the processing more quickly. Even though the machines are identical, failed processes or other tasks that run simultaneously makes load balancing desirable, and the nature of the load balancing increases as the chunks become more fine grained. On the contrary, if the chunks are too small, the overhead of dealing with the chunks and of map tasks creation starts to dominate the execution time of the overall tasks. For most tasks, a good chunk size will in general be the measure of a HDFS block, which is 64 MB as a standard.

Map jobs compile their output to the localized disk, not to HDFS. This is on the grounds that the output of the map is the intermediate output. It is handled by reduce function to deliver the final output and once the activity is finished the output from the map can be disposed of. Hence, storing the map output in HDFS with copies would be unnecessary. For each HDFS block from the output of the reduce, the primary copy is saved on a localized node, with different copies being saved on other data nodes. In this way, writing the output of the reduce task consumes bandwidth of the network.

The number of reduce jobs is not controlled by the input size. When there are more than one reducer, mapper partition's the output, each making one section for each reduce task. There can be multiple keys per partition, however, the records for any given key are all in a single partition. The partitioning may be controlled by a partitioning function as defined by the user, however the default partitioner works well by utilizing a hash function which stores keys.

Rest of the paper is organized as follows: In Section 2 we discuss some of the closely related works. We describe our architecture and experimental set up in Section 3. In Section 4 we explain our algorithm and MapReduce implementation flow. We introduce three metrics for performance of our MapReduce alogithm and analyze our results in Section 5. We conclude our study in Section 6.

2. RELATED WORK

In this section, we discuss some of the approaches related to the data migration. The literature consists of various approaches such as DCTCP [16], D2TCP [17] and D3 [18] that are used for minimizing the cost of data movement inside the data center. These approaches focus on data transfer within a single geographical location. The paper by Cho and Gupta [19] presents a system named Pandora that gives optimal cost solution for transferring a significant amount of data from one data center to another data center located around the globe. This approach finds the optimal cost using the physical shipment of disks as well as online data transfer. The problem with this approach is the conventional physical shipment is not an efficient solution to transfer large volume of data.

Various technologies like elastic optical networks and DC networks have been discussed by Lu et al. [20] for migrating data efficiently and creating backups for use in big data. The authors have described the impacts of applications of big data on the existing network. After this, authors have made a model for the data migration over the network. They have proposed efficient algorithms with respect to BL-Anycast-KSP-Single-DC algorithm. A joint resource defragmentation has been discussed in [20] for improving the performance of the network and a mutual backup model has also been proposed for better data backup. However, the efficiency of data migration is very less for elastic optical inter-DC networks and it is difficult to control and manage the network.

2.1 Hadoop MapReduce based approaches

Efficient migration of data has been studied under different contexts. We have discussed in this section briefly about Hadoop, geo distributed data centers and energy efficiency. Liu et al. [21] used Hadoop clusters to implement the MapReduce for cloud computing applications. According to these authors, when the data size grows, the performance of MapReduce is reduced. They introduced a performance rating scheme to analyze this phenomenon. Principle Component Analysis method was used to fill out the critical Hadoop configuration metrics that strongly impact the workload performance from excessive configuration items [21].

HadoopDB: There has been a lot of research studying correlating (related) data into similar nodes. HadoopDB saves information in a localized database management system and hence interrupts the dynamic scheduling and fault tolerance of Hadoop. According to Dittrich et al. [22], the two input files are grouped in Hadoop by creating a unique file with the specifications of a Trojan Index. Trojan Index is a solution to integrate indexing capability into Hadoop to provide index that can help in executing the MapReduce jobs.

Despite the fact that this methodology does not require an alteration of Hadoop, it is a static solution that expects users to rearrange their input data. Newer benchmarks have distinguished a gap in the performance among Hadoop and parallel databases. There has been considerable interest in advancing Hadoop with methods from other databases, while retaining the flexibility of Hadoop. A serious analytical benchmark study of different parts of the process pipeline of Hadoop was been led by Jiang et al. [23]. It was discovered that indexing the map significantly enhanced Hadoop's execution.

GridBatch [24] is another expansion to Hadoop with a few new administrators, and in addition another record type, which is divided by a partitioning function as defined by the user. It enables applications to determine documents that should be co-put too. Their answer intermixes the partitions at the record framework level, though this strategy decouples them with the goal that diverse applications can utilize distinctive strategies to characterize related documents. In further developed apportioning highlights of parallel database frameworks e.g. IBM DB2, TeraData, and Aster Data tables are co-divided, and the inquiry analyzer abuses this reality to create proficient question designs. This methodology adjusts these plans to the MapReduce framework, while holding Hadoop's dynamicity and adaptability. To accomplish this, proposed approach varies from parallel databases in that proposed framework performs co-position at the record framework level and in a best-exertion way: When constraints in the space or failures prevent co-situation, high accessibility and adaptation to internal failure are given higher need.

Programming Models: There have been multiple programming models that has provided restricted programming and utilizes restrictions for parallel computation automatically. An associated functionality can be used for the prefixes using parallel prefix computations [25]. These models can be simplified using MapReduce based on real world computations. An implementation that is tolerant on fault that scales to thousands of processors has been provided.

Conversely, a large portion of the parallel preparing frameworks have just been executed on little scales and leave the points of interest of taking care of machine failures to the developer. Higher levels of abstraction is provided by bulk synchronous programming [26] and some MPI primitives [27] that make it easier for programmers to code simultaneous programs. A prime distinction between these frameworks and MapReduce is that MapReduce misuses a limited programming model to use the client program in parallel and to give straightforward adaptation of the fault tolerance. The locality optimization draws its motivation from techniques such as active

disks [28], where computation is pushed onto processing elements that are close to local disks, to reduce the amount of data sent across I/O subsystems or the network.

Scheduling: Commodity processors are utilized where a small amount of disks are directly associated instead of running directly on disk controller processors, but the general methodology is similar. The backup task techniques are like the eager scheduling techniques used in the Charlotte System [29]. The main weakness of a simple enthusiastic scheduling is that if a given task causes failures repeatedly, the whole processing fails to complete. Few instances of this problem have been fixed in this technique to skip the bad records. The MapReduce execution depends on an in-house cluster management framework which is responsible for distributing and running user tasks on a large number of common systems. Even though it is not the focus of this work, the cluster management technique is similar to other techniques like Condor [38]. The data sorting which is a part of the MapReduce library is similar to the operation of Now-Sort [30]. The source machines segment the information to be arranged and sends it to the reduce tasks. The reduce task arranges the information in a local storage. It is known that Now-Sort is not very user friendly and cannot be defined by the user.

BAD-FS is an altogether different programming model from MapReduce that has been proposed by Bent et al. [31] for targeting the tasks across a wide area network. However, there are two main similarities: (1) Both frameworks utilize excess execution to recuperate from data losses that is caused by failures; (2) Both utilize a similar type of planning to diminish the amount of information sent through dense networks. TACC framework has been designed for simplifying the creation of services within a network is given by Fox et al. [32]. Like MapReduce, it depends on re-execution as a system for actualizing adaptation to internal failure

Geo-distributed cloud services contain many data centers spread across different locations. They can provide larger capacities to the end users and they are mainly used for social media applications [33]. According to [33], there are challenges like storing and migrating the data over long distances. An efficient framework has been proposed by Microsoft Team [33], which provides a solution to data placement. This solution helps to reduce the data movement between geo-distributed data centers. The effectiveness of the proposed framework has been verified by comparing to offline transfers. However, in this model [33], storage limits are not considered for every cloud location, and only the predicted data is sent.

An energy efficient tool has been developed in Li et al. [34] for migrating data in a virtual machine. It is an emulator where it provides functionality of an actual computer. A double threshold model with multiple resource utilization has been designed to migrate in the virtual machine [34]. The proposed algorithm by Li et al. [34] has shown better energy efficiency in cloud data center. To transfer data over the cloud efficiently, a cost effective data migration technique has been proposed by Zhang et al. [35] using a framework similar to MapReduce. Online lazy migration (OLM) and randomized fixed horizon control (RFHC) algorithms have been proposed by these authors to transfer the data efficiently. The performance of the online algorithms has been shown to improve when compared to optimal offline algorithm such as Smith Waterman alignment algorithm.

Each of these approaches is best suited for a specific scenario or a particular data set. There is a need for building a framework that can efficiently migrate the data and calculate the data loss as well. Our focus and objective is to build such a system framework that would efficiently migrate data using Map Reduce and avoid data loss.

3. EXPERIMENTAL SETUP AND ARCHITECTURE

We describe in this Section various modules of our architecture depicted in Figure 2.

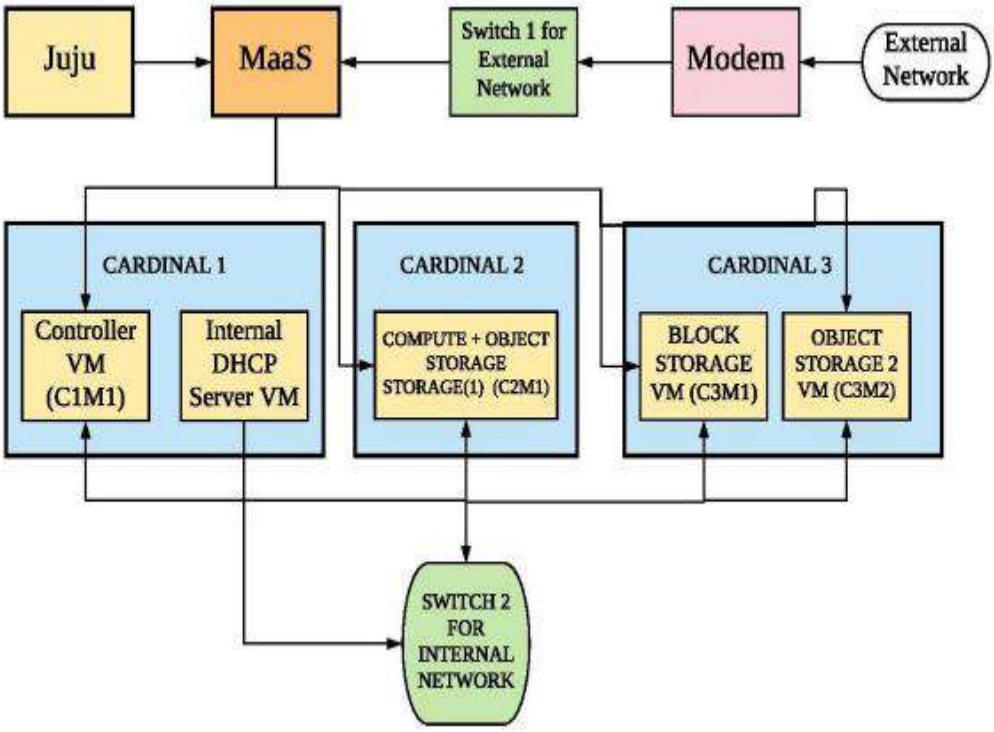


Figure 2. Cloud Architecture

3.1 OpenStack

The OpenStack project is an open source cloud computing platform for all types of clouds [36]. The purpose of using this open source software is that it is simple to implement, highly scalable, and feature rich. It is one of the widely used cloud computing platforms among developers and cloud computing technologists.

OpenStack basically provide IaaS solution through a group of associated services [36]. Each service provides an application programming interface (API) to facilitate this integration. According to the needs, one can install the required services. OpenStack has gained a lot of popularity due to its flexibility and ability to provide a virtualized infrastructure as it provides multiple hypervisors such as Kernel Virtual Machine (KVM), Qemu and Hyperv. KVM is a Linux kernel module that allows a user space program to utilize the hardware virtualization features of various processors [37]. Today, it supports recent Intel and AMD processors (x86 and x86/64). Qemu can make use of KVM when running a target architecture that is the same as the host architecture [37].

Several components contribute in building an OpenStack based Cloud. For this experiment, we have installed Nova compute, Glace, Cinder, Swift, Horizon, Keystone and Neutron.

3.2 MAAS

Metal as a Service (MAAS) treats physical servers like virtual machines in the cloud. It turns bare metal into an elastic cloud-like resource so we don't have to manage each server individually. Machines can be quickly provisioned using MAAS. MAAS can also destroy instances easily as similar to instances in a public cloud like Amazon AWS, Google GCE, and Microsoft Azure, among others. MAAS can act as a standalone PXE service. It can also be integrated with other technologies. It is basically designed to integrate well with Juju, the service and model management service. It's a perfect combinations as MAAS manages the machines and Juju manages the services running on those machines.

Minimum Requirements for MAAS

The minimum requirement for the machines that run MAAS vary widely depending on local implementation and usage.

Factors that influence hardware specifications include: a) the number of connecting clients (client activity); b) the manner in which services are distributed; c) whether high availability is used; d) whether load balancing is used; and e) the number of images that are stored.

3.3 JAAS

Juju as a Service (JAAS), is the best way to quickly model and deploy cloud-based applications. Juju is used to operate software on bare-metal servers by using Canonical's Metal as a Service (MAAS), in containers using LXD, and more. The models in Juju provide an abstraction which allows the operations know-how to be cloud agnostic. This means that Charms and Bundles in Juju can help in operating the same software with the same tool on a public cloud, private cloud, or a local laptop.

3.4 Building a Testbed

There are various ways of deploying the cloud. We have deployed a version of Openstack Pike using MAAS and JAAS as shown in Figure 2.

To build a private Cloud, we used three Dell R420 servers with multiple Ethernet ports. These servers are named as Cardinal 1, Cardinal 2 and Cardinal 3. All servers have 20 GB RAM and 8 Intel Xeon processors on each of them. Ubuntu 18.04 LTS (Desktop Version) was used as the operating system running on each of them. We have two different desktops with 8 GB RAM and Ubuntu 18.04 LTS version to install MAAS and JAAS separately. MAAS is also acting as DHCP server for external network providing Management IP’s. A VM is created on Cardinal 1 which is working as internal DHCP server to allocate Provider IP’s. We have used OpenStack Pike to create a private Cloud environment for these machines. OpenStack is a Cloud software platform with a three node architecture [36] as shown in Figure 2. OpenStack should have minimum three nodes to implement Cloud but to get more resources more number of compute nodes can be added. There can be only one controller and network nodes each in OpenStack setup. These three node are setup on three Dell servers using Qemu-KVM. These nodes are created as VMs on those servers to support the networking required while setting up OpenStack.

In this figure 2, (a) MaaS is acting as DHCP server for external network; (b) MaaS provides management IPs; (c) Switch 2 provides IPs for internal network; (d) all cardinals have Ubuntu 18.04 LTS; (e) All VM’s have Ubuntu 16.04 LTS.

3.5 Hadoop MapReduce Implementation

Data migration being a complex function, the data has to be optimized to make the process simpler. Hence, we use MapReduce, a model that optimizes the data, for my experiment. It is a programming model that processes big data sets. We have made two VMs on the compute nodes in our testbed. These VMs are used for demonstrating the migration for different types of files like csv, image, pdf and audio files. The data migration is done based on IP of these VMs. We have made this environment to run the MapReduce code because MapReduce requires the HDFS for running and executing the jobs. These codes of MapReduce are written using MATLAB environment. The Mapper and Reducer functions are implemented separately for different types of files. With the help of data migration, we show that using MapReduce for migration, reduces data loss as well as improves the efficiency of the migration.

4. EXPERIMENTS

4.1 Implementation Flow

Figure 3 presents the implementation process, and is explained below.

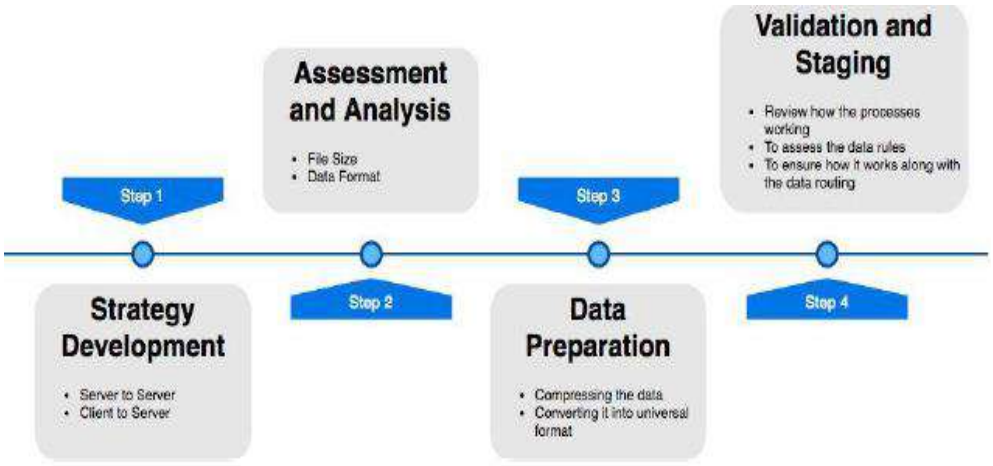


Figure 3. Implementation Flow

4.1.1.Strategy Development

The strategy development process for data migration can be chosen from different strategies based on the needs and available processing windows. The strategy depends on the following two criteria:

1) Data migration from server to server (with administrative permission): in this process, the data is migrated of one server platform to another (such as moving from server A to server B in Cloud environment), also our servers will have root or administrator access, which will allow to have full control over the setup and configuration of the server.

2) Data migration from client to server (With administrative permission): in this process, the data will be migrated from one client platform to another (such as moving from client A to server B in Cloud environment), also our client as well as server will have root or administrator access, which will allow to have full control over the setup and configuration of the server.

4.1.2. Assessment and Analysis

Two important parameters for a file are its size and format. We assessed and analyzed the performance of our MapReduce algorithm based on these two input parameters. The file size helps in computing data loss. In order to assess the performance of the migration process, different files of sizes (in MB) were considered. The data format help us in identifying what type of data is to be transferred during migration. For our experiments, the data file format is in csv, excel, images, audio, or video.

4.1.3. Data Preparation

During data migration from one server to another, a large amount of data is transferred, in general. In our experiment, data is transferred from Server A to Server B. If any data gets corrupted during the transfer, it is difficult to identify the location and directory of the corrupted file. Hence, prior to migration the data must be optimized for easier transfer of data. For this optimization process, we used the MapReduce framework. The final output (.mat file) is converted into PDF or another universal format (.rar) to ensure the security and privacy level of data.

4.1.4 Validation

The migration process performance is validated for ensuring the requirements and customized settings function. The validation and performance analysis process covers the following features: (a) review the process flow; (b) assess the data rules; (c) to ensure proper working of the process along with the data routing. The following parameter setting were used to achieve these features.

Parameter	Description
Schedule ID	Migration Schedule ID
Server	Primary file system's server
Files Migrated	The number of files that were migrated
Status	Migration completion status
Start Time	Date and time when the migration began
End Time	Date and time when the migration ended
Rules used	Rules used by the policy
Pre-Migration File System Space Used	File system size, total used space before the migration
Post-Migration File System Space Used	File system size and the total used space after the migration
File System Capacity	File system's total capacity

The efficiency and total execution cost are computed based on the above parameters to determine the performance of the algorithm, which we discuss later in the results section.

4.2 MapReduce Implementation

Our aim is to migrate data between two servers and compute if there is any data loss during the transfer. The proposed framework combines data migration and MapReduce. Apache Hadoop is the most commonly used MapReduce tool since it is open source tool and easily available and hence, we use this for our study.

For data migration, we have written a script in Matlab that replicates the data from Server A to Server B and will delete the data in Server A after MapReduce is performed. MapReduce model

comprises of three stages, the map stage and the reduce stage. The Map function optimizes the data and converts it into structured data. Mapping is performed in parallel on multiple nodes or groups of data.

After completion of Map stage, intermediate KVPs are sent to reduce function where the different mapping steps are combined. The reducer takes all the values associated with a single key k and outputs any number of KVPs. The data will be saved in the KVP, where the Key is an integer data assigned to each group of data. The Value in KVP is a floating-point type and contains the corresponding data. The Key and Value are stored as an array for each group of data. There might be more than one data with the same Key, however, the Value will be different. These Keys that have similar data are combined by merging the data sizes in the Value and storing it in a single array. Since, the KVP might have more than one row or column, it will be stored as a 2D array.

Algorithm: MAPRDUCE DATA MIGRATION

Input: Image, Audio, Video, Excel files
Output: (Key, Value) Pairs
Initialization:
  Mapper (INP, INF_VL, IN_K_VL)
    IMV = Data Fragmentation Condition (INP)
    Add IMV to IN_K_VL
Return IN_K_VL
Reducer (KY_VL, INT_VLTR, OT_K_VL)
  While HASNEXT (INT_VLTR)
    OT= GETNEXT (INT_VLTR)
  End While
  Add OT to OT_K_VL
Return OT_K_VL
Migrate (Server 1 ⟶ Server 2)
  Server 1:
  MIG_D_V= TCPIP (Server 2 IP Address, Port, Client)
  Mapping Rule:
    Set (MIG_D_V, Output Buffer Size, Output Bytes)
    Fopen (MIG_D_V)
  Data Recovery:
    Fwrite (MIG_D_V, Input);
    Fclose (MIG_D_V);
Server 2:
  SVR_END= TCPIP (Server 1 IP Address, Port, SERVER)
    Set (SVR_END, InputBufferSize, Input Bytes);
  Set (SVR_END, Timeout, 30);
  Fopen (SVR_END);
  Act_D = fread (SVR_END, INPUT PORT);
  Fclose (SVR_END);
End

The Map Reduce data migration algorithm takes different types of input such as audio, video, images and csv files. The first step is to create datastore for the data set. This datastore works as an input for MapReduce allowing MapReduce to process data in chunks. The input to the map function is data (INP), information (INF_VL) and intermediate Key Value store (IN_K_VL). The INP and INF_VL are the result of the call function made to the datastore. The map function adds the KVPs to the IN_K_VL object.

The inputs to the reduce function is intermediate key (KY_VL), value iterator (INT_VLTR) and final key value store (OT_K_VL). The KY_VL is the active key added by map function.

Whenever there is a call made to reduce function, map reduces provides a new key from intermediate Key Value store (IN_K_VL). The INT_VLTR objects contains all the values associated with KY_VL. The HASNEXT and GETNEXT functions are used to scroll through the values. OT_K_VL is the final key value store where the reducer functions has added the KVPs. MapReduce takes all the KVPs from OT_K_VL and returns to the output datastore.

After MapReduce function, the migration takes place. The migration process has an important condition that both the servers should have the same version of Matlab environment. The migration is done based on the IP address of the sender and receiver. The sender defines the address of receiver in TCPIP function and the port. Similarly the receiver defines the IP address and port of the sender.

5. RESULTS AND DISCUSSIONS

After MapReduce step, the data is transferred from Server A to Server B in the private cloud environment. The KVP is obtained from the data that is now in the Server B. This new KVP is compared with the previous KVP to find if the values are same. Any mismatch would mean that there is some loss in the transferred data. If the matching of data takes place well without any error, it means that there is no loss in data.

The size of the groups where the data loss has taken place is used to compute the total data loss during the transfer. This will be done by computing the difference between the total amount of data before the migration and total amount of data after the migration.

Data Loss: D_L

Total amount of data before migration: D_{BM}
Total amount of data after migration: D_{AM}

$$D_L = D_{BM} - D_{AM}$$

We have performed the experiments and various performance evaluation to check the effectiveness of the proposed method that combines the data migration method using MapReduce with input parameters such as number of files, file size, output parameters such as accuracy and the cost of the transfer.

The energy consumption of the servers is generally high, which accounts for the high data migration cost. The cost of migration has to be low in any framework in order to be efficient. We evaluated the cost of migration for the proposed model and also evaluated the cost for migrating data without using MapReduce. Execution cost was calculated by adding the cost incurred during the idle time with the cost incurred to execute the work flow schema.

Total Execution Cost: E_C

Idle Time: I_T
Busy Time: B_T
Information that is stored after transfer: λ
Data that is transferred over the network: γ

$$E_c = \frac{(\lambda * I_t) + (\gamma * B_t)}{\lambda + \gamma}$$

Efficiency: E

Efficiency is another major important metric for performance evaluation. It can be defined as the percentage of data that is transferred without any data loss.

Total Data Transferred: DT
Data Re-transferred: DRT

$$E = \frac{DT - DRT}{DT} * 100$$

TABLE 1 : INPUT FILE FORMAT: Audio and Video Files (.wav, .mp4)			
File Size (In MB)	Total Execution Cost (In second)	Data Loss (In MB)	Efficiency
10	9.789856	1.07	90.674%
100	41.099143	6.98	91.986%
400	90.371984	19.91	94.793%
700	159.12896	34.08	95.168%
1100	242.95312	41.09	96.023%

Table 1 captures various results for the performance of data migration of audio video data files. The algorithm working behind these files need to run an additional function as audio datastore.

Due to this, there is a delay, which leads to addition of few seconds to the total execution cost. The total execution cost keeps decreasing with respect to the size of data transfer. The efficiency improves as it can be seen in the table showing that for big data sets, the algorithm performs better. The data loss also reduces with increasing size. This concludes that our algorithm performs efficiently in case of audio video migration for scaled data size.

Table 2 presents the performance of our algorithm on image data files. The Map and Reduce function for image migration uses contrast and saturation as key values. The total execution cost keeps decreasing with respect to the size of image transferred. The efficiency improves as it can be seen in the table showing that for big data sets, the algorithm performs better. The image being static (still), performs better than audio video files. The data loss is low with increasing size. Hence it can be conclude that the algorithm performs well in case of image migration also with respect to scaling data sizes.

TABLE 2: INPUT FILE FORMAT: Image Files (.png, .jpg, .tif)			
File Size (In MB)	Total Execution Cost (In second)	Data Loss (In MB)	Efficiency
10	8.132984	0.99	92.147%
100	39.227144	5.20	93.997%
400	87.994872	17.80	17.80
700	146.297184	20.73	95.778%
1100	223.224165	28.07	96.814%

TABLE 3: INPUT FILE FORMAT: Excel Files (.csv, .xlsx)			
File Size (In MB)	Total Execution Cost (In second)	Data Loss (In MB)	Efficiency
10	7.193986	0.93	93.674%
100	33.938971	3.71	94.986%
400	71.392817	13.77	94.793%
700	138.029641	20.73	96.168%
1100	194.837194	28.07	97.023%

Table 3 presents the performance of our algorithm for textual data files in csv or xlsx format. The Map and Reduce function for document migration uses keywords as key values. This performs better than other data formats mentioned before. The total execution cost is very low in comparison to other data format with same amount of data size. The total execution cost keeps decreasing with respect to the size of documents transferred. The efficiency improves as it can be seen in the table showing that for big data sets, the algorithm performs well. Due to data being present in row-column format, we can separate the data easily based on key values. Hence, the performance improves with respect to other file format such as image, audio and video files. The data loss is low with increasing size. With this we can conclude that our algorithm performs better in case of document migration with respect to increasing size of file.Analyzing the results in Figure 4, we can observe that the efficiency is best for textual data in csv or xlsx format. It can be seen that with increasing size of data, the efficiency increases irrespective of the data format. This shows that algorithm works better providing a high efficiency for bigger data sets. The goal was to minimize the data loss and it decreases with respect to the size of the data migrated. The datastore functionality provide by Matlab is a benefit over other programming languages as it helped in optimizing the datasets.

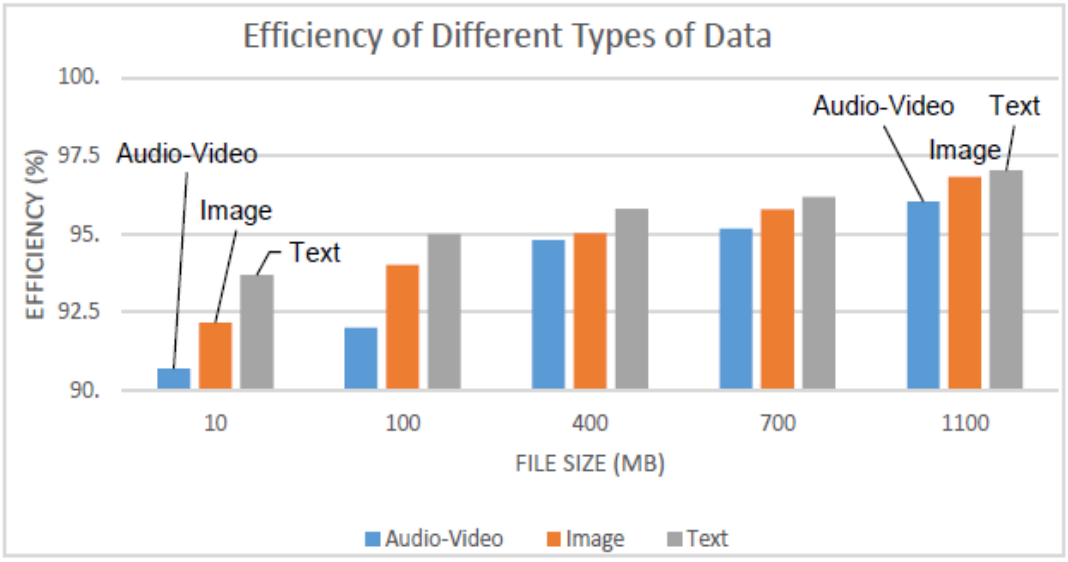


Figure 4. Efficiency Analysis

6. CONCLUSIONS

A migration technique has been discussed in this study that can efficiently transfer the data between the servers using MapReduce. The framework that has been developed for migrating the data has reduced the data loss. The MapReduce has efficiently optimized the data migration code when large data sets are considered for migration. The performance metrics introduced have been

validated by computing the efficiency and the cost for migration. From the results, it can be seen that the efficiency of the proposed algorithm increases with the increasing file size, that is, we established the scalability of the proposed algorithm. Also, the cost of the transfer is shown to be reduced.

The data migration technique used for the experiment performs faster than the previously available work in cloud computing. The work has been performed using image files like png, jpeg and tiff, audio files like wav, video files like mp4 and documents like xls and csv. While performing the simulation, internet interruptions, failure of a server, less bandwidth and less frequency have been the issues for data loss in the experimental results reported. With stable network connectivity, we expect that the data loss could be avoided.

Larger heterogeneous files (text, images, audio and videos) have been migrated by our algorithm for execution time and efficiency. The execution cost can further be reduced if the files formats were homogeneous while also decreasing the data loss.

With the limited resources used for the current study, the size of files migrated were bounded due to system limitations and also data loss could not be avoided. By improving the configuration of the system architecture and physical servers we might expect to improve the performance further. The efficiency of our algorithm cannot be guaranteed for input files with complex data (features of the input files) and other file formats, hence, improving the algorithm for such input files is left as future work.

ACKNOWLEDGEMENT

The last two authors acknowledge the partial funding from the Faculty of Science Inter-disciplinary research collaboration initiation grant and discovery grant from Natural Sciences and Engineering Research Council (NSERC).

REFERENCES

[1] N. Subramanian and A. Jeyaraj, “Recent security challenges in cloud computing,” Computers and Electrical Engineering, Elsevier, vol. 71, pp. 28–42, 2018.

[2] M. Younas, D. N. Jawawi, I. Ghani, T. Fries, and R. Kazmi, “Agile development in the cloud computing environment: A systematic review,” Information and Software Technology, 2018

[3] P. Hofmann and D. Woods, “Cloud computing: the limits of public clouds for business applications,” IEEE Internet Computing, vol. 14, no. 6, pp. 90–93, 2010

[4] C. Rong, S. Nguyen, and M. Jaatun, “Beyond lightning: A survey on security challenges in cloud computing,” Computers and Electrical Engineering, vol. 39, no. 1, pp. 47–54, 2013.

[5] T. Laszewski and P. Nauduri, “Migrating applications to the cloud,” in Migrating to the cloud: Oracle client/server modernization. Elsevier, 2011, ch. 8, pp. 181–208.

[6] L. Zhang, C. Wu, Z. Li, C. Guo, M. Chen, and F. C. Lau, “Moving big data to the cloud: An online cost-minimizing approach,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 12, pp. 2710–2721, 2013

[7] T. Laszewski and P. Nauduri, “Migrating applications to the cloud,” in Migrating to the cloud: Oracle client/server modernization. Elsevier, 2011, ch. 7, pp. 155–179

[8] E. Ahmed, A. Akhunzada, M. Whaiduzzaman, A. Gani, S. H. Ab Hamid, and R. Buyya,“Network-centric performance analysis of runtime application migration in mobile cloud computing,” Simulation Modelling Practice and Theory, vol. 50, pp. 42–56, 2015

[9] U. Deshpande and K. Keahey, “Traffic-sensitive live migration of virtual machines,” Future Generation Computer Systems, vol. 72, pp. 118–128, 2017.

[10] T. Wood, “Improving data center resource management, deployment, and availability with virtualization,” Ph.D. dissertation, University of Massachusetts Amherst, 2011, open Access Dissertations.

[11] P. Teli, M. V. Thomas, and K. Chandrasekaran, "Big data migration between datacenters in online cloud environment," Procedia Technology, Elsevier, vol. 24, pp. 1558–1565, 2016.
[12] B. Thalheim and Q. Wang, "Data migration: A theoretical perspective," Data and Knowledge Engineering, Elsevier, vol. 87, pp. 260–278, 2013.
[13] Apache Software. (2013) Mapreduce tutorial. Accessed: 2018-08-23. [Online]. Available:https://hadoop.apache.org/docs/r1.2.1/mapredtutorial.html#MapReduce+-+User+Interfaces
[14] S.Kumar. (2018) What is Hadoop map reduce and how does it work? Accessed: 2018-08-22. [Online]. Available: https://qph.fs.quoracdn.net/main-qimg-82813242aa853b91a91b96134f0c5c13-c
[15] Apache Software Foundation. (2018) Hadoop cluster. Accessed: 2018-12-17 [Online]. Available:https://hadoop.apache.org/docs/stable/hadoop-project-dist/hadoop-common/SingleCluster.html
[16] M. Alizadeh, A. Greenberg, D. A. Maltz, J. Padhye, P. Patel, B. Prabhakar, S. Sengupta,and M. Sridharan, "Data center tcp (dctcp),"ACM SIGCOMM computer communication review, vol. 41, no. 4, pp. 63–74, 2011.
[17] B. Vamanan, J. Hasan, and T. Vijaykumar, "Deadline-aware datacenter tcp (d2tcp),"ACM SIGCOMM Computer Communication Review, vol. 42, no. 4, pp. 115–126, 2012.
[18] C. Wilson, H. Ballani, T. Karagiannis, and A. Rowtron, "Better never than late: Meeting deadlines in datacenter networks," ACM SIGCOMM Computer Communication Review, vol. 41, no. 4, pp. 50–61, 2011.
[19] B. Cho and I. Gupta, "Budget-constrained bulk data transfer via internet and shipping networks," in Proceedings of the 8th ACM international conference on Autonomic computing, 2011, pp. 71–80.
[20] P. Lu, L. Zhang, X. Liu, J. Yao, and Z. Zhu, "Highly efficient data migration and backup for big data applications in elastic optical inter-data-center networks," IEEE Network, vol. 29, no. 5, pp. 36–42, 2015.
[21] F.-H. Liu, Y.-R. Liou, H.-F. Lo, K.-C. Chang, and W.-T. Lee, "The comprehensive performance rating for hadoop clusters on cloud computing platform," International Journal of Information and Electronics Engineering, vol. 4, no. 6, p. 480, 2014.
[22] J. Dittrich, J.-A. Quian´e-Ruiz, A. Jindal, Y. Kargin, V. Setty, and J. Schad,"Hadoop++: making a yellow elephant run like a cheetah (without it even noticing),"Proceedings of the VLDB Endowment, vol. 3, no. 1-2, pp. 515–529, 2010
[23] D. Jiang, A. K. Tung, and G. Chen, "Map-join-reduce: Toward scalable and efficient data analysis on large clusters," IEEE transactions on knowledge and data engineering, vol. 23, no. 9, pp. 1299–1311, 2011.
[24] H. Liu and D. Orban, "Gridbatch: Cloud computing for large-scale data-intensive batch applications," in Cluster Computing and the Grid, (CCGRID). 8th IEEE Intl. Symposium on. IEEE, 2008, pp. 295–305.
[25] R. Ladner and M. Fischer, "Parallel prefix computation," Journal of the ACM (JACM),vol. 27, no. 4, pp. 831–838, 1980.
[26] L. G. Valiant, "A bridging model for parallel computation," Communications of the ACM, vol. 33, no. 8, pp. 103–111, 1990.
[27] W. D. Gropp, E. Lusk, A. Skjellum, and A. Lusk, Using MPI: portable parallel programming with the message-passing interface. MIT press, 1999, vol. 1
[28] E. Riedel, C. Faloutsos, G. A. Gibson, and D. Nagle, "Active disks for large-scale data processing," Computer, vol. 34, no. 6, pp. 68–74, 2001
[29] J. Dean and S. Ghemawat, "Mapreduce: simplified data processing on large clusters," Communications of the ACM, vol. 51, no. 1, pp. 107–113, 2008.
[30] K. Shvachko, H. Kuang, S. Radia, and R. Chansler, "The hadoop distributed file system." IEEE 26th Symposium on Mass Storage Systems and Technologies, 2010, pp. 1–10.
[31] J. Bent, D. Thain, A. C. Arpaci-Dusseau, R. H. Arpaci-Dusseau, and M. Livny, "Explicit control in the batch-aware distributed file system." In Networked System Design & Implementation, vol. 4, 2004, pp. 365–378
[32] A. Fox, S. Gribble, Y. Chawathe, E. Brewer, and P. Gauthier, "Cluster-based scalable network services," in Proceedings of the sixteenth ACM symposium on operating systems principles, ser. SOSP '97. ACM, 1997, pp. 78–91.
[33] S. Agarwal, J. Dunagan, N. Jain, S. Saroiu, A. Wolman, and H. Bhogan, "Volley: Automated data placement for geo-distributed cloud services," Proceedings (CD-ROM) of the 7th USENIX conference on Networked systems design and implementation, 2010

[34] H. Li, G. Zhu, C. Cui, H. Tang, Y. Dou, and C. He, "Energy-efficient migration and consolidation algorithm of virtual machines in data centers for cloud computing," Computing, Springer, vol. 98, no. 3, pp. 303–317, 2016.
[35] L. Zhang, C. Wu, Z. Li, C. Guo, M. Chen, and F. C. Lau, "Moving big data to the cloud: An online cost-minimizing approach," IEEE J. on Selected Areas in Communications, vol. 31, no. 12, pp. 2710–2721, 2013.
[36] OpenStack. (2018) Get started with openstack. Accessed: 2018-11-22. [Online].Available: https://docs.openstack.org/install-guide/get-started-with-openstack.html
[37] QEMU. (2017) Features/kvm Accessed: 2019-01-21. [Online]. Available: https://wiki.qemu.org/Features/KVM
[38] D. Thain, T. Tannenbaum, and M. Livny, "Condor and the grid," Grid computing: Making the global infrastructure a reality, pp. 299–335, 2003.

AUTHORS

Mr. Anurag Pandey is a graduate student with the Department of Computer Science, University of Manitoba, Winnipeg, Manitoba. He is currently completing his MSc program. He has previously worked as a Software Engineer. His research interests include Cloud Computing, Amazon Web Services, and Big Data (Infrastructure).

Dr. Ruppa K. Thulasiram (Tulsi) is a Professor with the Department of Computer Science, University of Manitoba, Winnipeg, Manitoba. He received his Ph.D., from Indian Institute of Science, Bangalore, India and spent years at Concordia University, Montreal, Canada; Georgia Institute of Technology, Atlanta; and University of Delaware as Post-doc, Research Staff and Research Faculty respectively before taking up a position at University of Manitoba. Tulsi's current research interests include Computational Finance, Cloud Computing, Blockchain Technology for Financial Applications and related areas. He has written many papers in the areas of High Temperature Physics, Gas Dynamics, Computational Finance, Grid/Cloud computing, Computational Intelligence and Blockchain Applications research areas. He has supervised many MSc and PhD theses and graduated many students. He has also received many best paper awards in reputed conferences. He holds a patent for true random generators along with students and colleagues. Tulsi has developed a curriculum for cross-disciplinary computational finance area as well as on Cloud Computing at University of Manitoba for both graduate and senior undergraduate level and has been teaching for the past several years. Tulsi has organized many conferences and has been editor and guest editor with many journals. He is associated with many professional societies such as IEEE, ACM, ASAC etc.

Dr. Aerambamoorthy Thavaneswaran (Thava) is a Professor with the Department of Statistics, University of Manitoba, Winnipeg, Manitoba. He received his M.Math. and Ph.D.in statistics from University of Waterloo. Thava's research interests include Inference for stochastic processes, Estimating Functions, Nonlinear Time Series, Filtering, Smoothing, Empirical Financial Time series modelling, Mathematical Finance: option pricing/bond pricing, Fuzzy Methods in Finance and Financial Risk Forecasting. He has supervised many MSc and PhD theses and graduated many students at University of Manitoba, Temple University and University of Malaya. He has also published more than 100 papers having more than 1000 citations. Thava has been an associate editor and guest editor with many journals. He is associated with statistical society of Canada and International Statistical Institute (ISI) as an elected member.

INTEGRATING CLOUD COMPUTING TO SOLVE ERP COST CHALLENGE

Amal Alhosban and Anvitha Akurathi

Department of Computer Science, Engineering and Physics
University of Michigan-Flint, MI, USA

ABSTRACT

Enterprise Resource Planning (ERP) is a popular business management tool used by almost all companies these days to organize their business. In-spite of the challenges faced by ERP; before, during and after its implementation into the Enterprise, it fetches greater profits to the organization. This paper deals with the challenges faced by ERP with a complete literature overview of the challenges from earlier authors. Then after a brief visit of these factors, a very essential topic to the Enterprises i.e., Costs are discussed. The costs that are incurred in the project, some unknown or hidden costs are dealt with. A solution is proposed to solve this cost problem of ERP and to improve the profit margins to the companies. The solution is Cloud ERP. The latter part deals with the benefits of Cloud ERP in general and with respect to costs along with the concerns of cloud ERP, the major issue among all the concerns and few proposed solutions of solving this problem in the cloud ERP.

KEYWORDS

ERP, Cost, Cloud ERP, Security

1. INTRODUCTION

ERP (Enterprise Resource Planning) is a bunch of modules that form a suite to support the business activities of an Enterprise or an organization. It plays a very crucial role in the profit gains and the maintenance of standards in any organization. In the initial stages of ERP, it was all on-premise which means that the company or the organization has to bear the cost of infrastructure, hardware, electrical equipment, systems, and employees to manage them to house an on-premise ERP. Along with all these, there were many potential challenges of ERP in an Enterprise. Our paper discusses very briefly in section 3 all the challenges of ERP by performing an overview on existing literature work (section 2) on the factors affecting ERP and the crucial factor of ERP for any company – Costs is discussed. We talk on the budget, the hidden and underestimated costs and the mistakes that give rise to such costs. A small case study is provided to show how the budget problem can affect a project and can create havoc to it. In section 4, we discuss the best possible solution to the cost problem, its benefits, concerns and other details relating to it. This solution is Cloud ERP and we discuss in detail about the benefits and concerns of it. Section 5 discusses the workflow of the research. Section 6 concludes the work with a proposal on future work.

2. RELATED WORK

Implementing ERP is a very challenging task. It has many factors that affect it. Most of these factors have been discussed by many authors in their literature. In this section of the paper, let us look in detail what all the authors have in their work about the factors affecting ERP. Parijat and

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 213-219, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90917

Pranab said that the factors of ERP are business process restructuring, change management, users' attitude, training, project management, top management support, vendor support, project sponsorship (budget) and proper communication [4]. In [5], the authors mentioned some other general factors as inadequate clients' willingness to participate, need for vast clients and relevant personnel involved [6], too broad coverage of business, lacking clear targets, shortage of support and experience, technological or cost-profit problems. Inadequate training, not enough experts, lacking analysis of flow and technology, failure of synergizing inside and outside expertise, [8] business plans incompatible with ERP functions, and separation from certain ready systems are risk factors for the success of ERP. The major challenges of ERP implementation in Business [11] [19] are Lack of senior management commitment, [20] ineffective communication with users, insufficient training of end-users, failure to get user support, [16] lack of effective project management [11] methodology, [12] [13] underestimating the legacy systems, conflict between the user departments, composition of project team members, change management, training to users, communication, failure to redesign business processes and the misunderstandings of change requirements. For an ERP project to succeed, you must prevent problems in the following high-priority areas which [14] are e-business strategy, project management approaches, complex technology and systems, and [17] End-user resistance.

Process knowledge, customization and contextualization knowledge, management support, change management, and training have been identified as key components of this dimension [15] [21]. The major success factors of an ERP system are [3] [9] top-management support, training [15], team contributions, consulting capability, and support. Employee skills [18] and project knowledge [21] play an important role in the success of any project. Employees should be well trained in using the system and be fully aware of the system's advantages and capabilities. Technical competence factors do play a very important role in the ERP system. [24] The implementation team should have the ability to implement, [23] maintain and upgrade the ERP system, actively builds relationships with business managers [22], responsive to the endusers and check for proper data integrity.

As mentioned in [18] ERP should be a well-planned and accurate budget covering all the costs needed [15] in terms of training certificates, employees' motivations, system upgrades in the post-implementation phase, and any costs due to recruitment and training of new staff to replace those leaving and to cope with potential increases in turnover[23]. ERP systems simply can't handle complex transactions and therefore limit the success of channel partners, negatively impact margins, and ultimately hurt the bottom line. Legacy systems proper planning, softwareselection efforts and information-system area participation [1] [3].

All these challenges can be broadly categorized into 4: Employee Skills (Both Technical and Non-Technical), Change Management, Costs, and Other IT factors

3. CHALLENGE IN FOCUS – COSTS

The ultimate goal of any enterprise is profits which are the result of the whole revenue generated taking out the costs incurred. The profits will be more when the costs are less. Let us now discuss One of the important challenges of ERP are 'Costs'. ERP software initiatives are complex, multifaceted undertakings making the budgeting process is one of the trickiest stages of implementation. [15] Cost is a very important factor for ERP projects. Generally, if we take 100% as our total budget for the ERP project, the hidden and unexpected costs would come up to 10% of the total estimate [27]. There are few factors that determine the ERP implementation cost such as the size of the Company, cost-involving implementation, third-party software Integration, ERP system customization, and brand factor.

While the most expensive ERP system will probably meet all or most of your company's requirements, the TCO (Total Cost of ownership) may far exceed the corporate budget. On the other hand, there can be both functionality and implementation risks associated with selecting the least expensive ERP solution.

3.1 Hidden/ Underestimated Costs

The Hidden or underestimated costs of ERP projects can be any of the following: training, unanticipated customizations, data conversion into different formats, integration and testing, data migration from legacy systems, data analysis, consultants and Infinitum, replacing the best and the brightest people, process redesign and software upgrades. All these form most of the hidden and underestimated costs of an ERP project. These are not direct and are not all the time unaware.

3.2 Mistakes that Increase the costs

There are a few mistakes that cause the project to move into over-budget. They are: improper requirements gathering, underestimating potential hidden costs, failing to buyin from the top management, frequent changing of processes to meet software's needs, over-estimating the ability to customize the system, failing to select the right person-incharge, doing too much at once, under-staffing the project, giving Inadequate training to the users and not expecting the unexpected. All these mistakes lead to more costs on an on-premise ERP. Many solutions are proposed to solve this problem of costs but only a few of them are practically feasible.

3.3 Example Case-study

While implementing an ERP system for the US Navy, the 2005 budget request for the Navy was $3.5 billion for business systems operations and upgrades, and it does include ERP. The Navy estimates the ERP will not be fully operational until 2011 at an estimated cost of $800 million. But the individual Program Managers for each of the pilots reported the following total costs of their pilot through September 2004 as $1,044,300,000. The $1 billion spent on the pilots was a waste. The best solution to the cost problem proposed so far is 'Cloud ERP' which means moving the ERP from onpremise to cloud so that all the resources are shared along with the products and services in the cloud [29].

4. CLOUD ERP

Cloud ERP is an approach to enterprise resource planning (ERP) that makes use of cloud computing platforms and services to provide a business with a more flexible business process transformation [30]. The shift to cloud-based software is being fuelled by a number of factors, including virtualization (creation of a software layer between existing computer hardware and host operating systems), which enables shared use of servers, reducing the cost of IT infrastructure and support. In addition, organizations want to adopt the latest technologies quickly to remain competitive, and increasing complexity of IT support requirements for business management applications.

4.1 Benefits of Cloud-ERP:

Movement of ERP to the cloud is new but the benefits can be reaped both from the Cloud and ERP perspectives. It gives a double advantage of using Cloud ERP. The benefits of cloud ERP can be summed up as: reduction in capital and operational costs. ensures latest updates or versions, without the necessity of companies to be involved, perfect fit for new start-ups, even if they think of going public someday, access of information throughout the globe, ease of

maintenance and ensure regular compliance, reduction in IT staffers, procurement and configuration of servers, enhanced system speed and performance, trial applications without a large capital investment and roll out new applications to groups reducing risk and spreading training costs, and can adjust users and applications up or down to meet the changing demands of your business and enhanced mobility. In most cases, cloud computing is more secure than an organization's data warehouse, businesses can focus more on their people and facilities rather than on providing infrastructure business continuity and provides an opportunity to re-architect our systems that will support new world applications

4.2 Cost cuttings through Cloud ERP:

Cloud ERP is more beneficial to save the costs for the ERP project. Some of the cost cuttings through Cloud ERP are: reduction in capital and operational costs, reduction in maintenance costs, reduction in investment and ownership costs, elimination of IT/ERP infrastructure facilities for user companies, lower Total Cost of Ownership (TCO), reduction in Resource costs due to sharing and less cost for upgrading the software. Using Cloud helps in turning down the cost of the whole ERP project to more than 50% less to the original on-premise cost. For this reason, most of the larger companies are moving their ERP to Cloud. Examples of such companies are Amazon, Qualcomm, Microsoft, and Google. Most of these concerns in cloud computing are solved by using methods and techniques in the cloud. The major concern of the present day cloud application, especially ERP is "Security".

5. METHODOLOGY OF RESEARCH

The workflow of our Research can be given in a simple flow as figure 1.

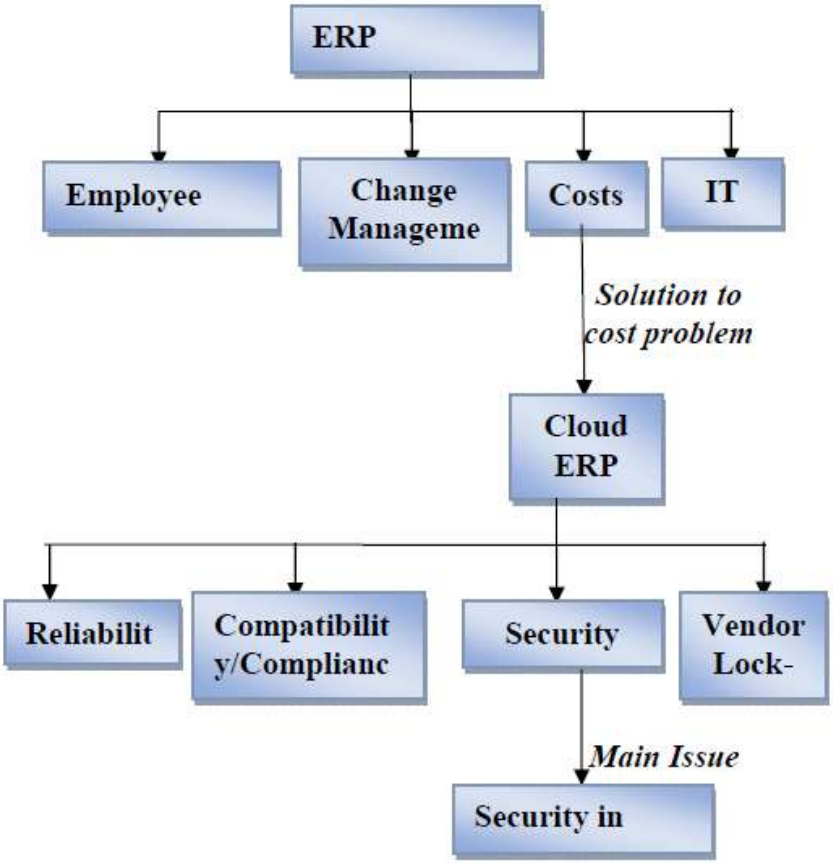


Figure 1. ERP Cloud Work Flow

6. CONCLUSIONS

ERP is an excellent tool to improve the Organization's profit margin. Providing a solution to the challenges faced by the ERP is not a huge task but implementing them at the right time in the right product provides the best results. The solution to the cost problem of ERP i.e., the Cloud ERP works amazingly for all the cost problems of the ERP software and also saves a lot of capital cost to the organization. Apart from the security concern of cloud ERP, everything else works well for any organization that would like to use ERP in the cloud without investing money on infrastructure. The Security concern of Cloud ERP has few solutions proposed but this issue is still skeptical from the view of users and the providers as well. The breaches in security will also cause violations of privacy leading to a new issue in the Cloud ERP. Hence, as the future work of this paper, a solution can be proposed to mitigate the Security issue of the Cloud ERP to a maximum level, so that the Cloud will become a safe place to work on ERP with a very less cost to the organization.

REFERENCES

[1] Joe Alphonse, "3 Reasons Your ERP System Could Hamper RevenueGrowth", Revitas, Wednesday, November 06 2013.

[2] Christopher P. Holland and Ben Light, "A Critical Success Factors Model forERP Implementation", Manchester Business School, IEEE Software, May-June 1999

[3] BooYoung Chung, "AN ANALYSIS OF SUCCESS AND FAILURE FACTORS FOR ERP SYSTEMS IN ENGINEERING AND CONSTRUCTION FIRMS", University of Maryland, College Park, 2007

[4] Parijat Upadhyay, Pranab K Dan, "An explorative study to identify the Critical Success Factors for ERP implementation in Indian small and medium scale enterprises", International Conference on Information Technology, IEEE, 2008
[5] S. Alter, "Implementation Risk Analysis", TIMS Studies in Management Science, Vol. 13,No 2, pp 103-109, 1979
[6] B. W. Boehm, "Software Risk Management: Principles and Practices", IEEE Software, Vol. 8,No. 1, pp. 32-41, 1991
[7] S. Wright and A.M. Wright, "Information System Assurance for Enterprise Resource Planning Systems: Implementation and unique Risk Considerations", Journal of Information Systems, Vol. 16, pp. 5-15, 2001
[8] S.M. Huang, Y.C. Hung, H.G Chen and C. YKu, "Transplanting the Best Practice for Implementation of An ERP System: A Structured Inductive Study of An International Company",The Journal of Computer Information Systems, Vol. 44, No. 4, pp 101,Summer 2004
[9] S. Al-Sehali, "The Factors That Affect the Implementation of Enterprise Resource Planning (ERP) in the International Arab Gulf States and United States Company with Special Emphasis on SAP Software", Dissertation, University of Northern Iowa, 2000
[10] P. S. Bingi, K. Maneesh and J. K. Godla, "Critical Issues Affecting an ERP Implementation", Information Systems Management, Vol. 16, No. 3, pp. 7-14, 1999
[11] GoeunSeo, "Challenges in Implementing Enterprise Resource Planning (ERP) system in Large Organizations: Similarities and Differences Between Corporate and University Environment", Sloan School of Management, MIT, Cambridge, May 2013
[12] Ada Wong, Harry Scarbrough, "Critical Failure Factors in ERP Implementation", University of Hong Kong, China
[13] Dr. Bernard Wong, David Tein, "Critical Success Factors for ERP Projects", Australia
[14] Herb Krasner, "Ensuring E-business Success by Learning from ERP Failures", IT Pro Magazine, January-February 2000
[15] Randa Mazzawi, "Enterprise Resource Planning Implementation Failure: A Case Study from Jordan", Journal of Business Administration and Management Sciences Research, Vol. 3(5), pp. 079- 086, May, 2014
[16] D. P. Slevin and J. K. Pinto, "Balancing Strategy and Tactics in Project Implementation," Sloan Management Review, vol. Fall, pp. 33-44, 1987.
[17] David Allen, Thomas Kern, Mark Havenhand, "ERP Critical Success Factors: an exploration of the contextual factors in public sector institutions", Proceedings of the 35th Hawaii International Conference on System Sciences – 2002
[18] ElSayed, M.S., Hubbard, N.J. and Tipi, N.S., "Evaluating Enterprise Resource Planning (ERP) Post Implementation Problems in Egypt: Findings from case studies of Governmental, Multinational and Private Egyptian Organizations", The Business School, University of Huddersfield, Queensgate Huddersfield HD1 3DH UK, September 2013
[19] Stephen C. Wingreen, Maryam Mahdavian, Hritik Gupta,"An investigation into Enterprise Resource planning implementation success: Evidence from Private and public sector Organizaions", 2013
[20] W.-H. Tsai1, W.-R.Lin1*, S.-J.Lin1, J.-L. Hsu2, "Investigation of ERP Implementation Problems in Organization Environment", Taiwan, 2009
[21] Anjali Ramburn, Lisa Seymour and Avinaash Gopaul. "Learning from a Failed ERP implementation: The Case of a Large South African Organization." University of Cape Town, Cape Town, South Africa
[22] Hsiu-Hua Chang et al. "ERP Post - Implementation Learning, ERP Usage and Individual Performance Impact."Internet: http://www.pacisnet.org/file/2011! PACIS2011-025.pdf, [Date Update: 2011], [Access Date: 2010212012]
[23] D. Aloini, R. Dulmin, V. Mininno, "Risk management in ERP project introduction: review of the literature", Information &Management, vol. 44, 2007, p547–567
[24] Arun Madapusi, Daniel A. Cernas Ortiz, "The Influence of Technical Competence Factors in ERP System Implementations", Journal of Applied Business and Economics vol. 16(2) 2014
[25] Daniel D.Pern, 15th September 2008, "How One Company Broke Down Silos and Improved Application Integration". CIO.
[26] Phil Wainewright. 16th March 2013. "Qualcomm mulls shift to cloud ERP". Diginomica. Found online at: http://diginomica.com/2013/05/16/qualcomm-mulls-shift-to-cloud-erp/

[27] "5 factors that determine the ERP implementation cost", Accendo Technologies, May 2014, http://www.accendotechnologies.com/blog/5-factors-that-determine-erp-implementation-cost/
[28] Sheldon Needle, "Calculating Total Cost of Ownership (TCO): an Important Measurement of ROI", CTS manufacturing blog, December 1, 2012 http://www.ctsguides.com/manufacturing/calculatingtotal-cost-of-ownership-tco-an-important-measurement-of-roi/
[29] Harold Carver, William Jackson, "A Case Study of the United States Navy's Enterprise Resource Planning System", Monterey, California, June 2006
[30] "35 Questions Every CFO needs To Ask About ERP Software In the Cloud", ERP Panel Papers, ERPSofwareBlog.s.com, ICAL Business Solutions Provider
[31] S hashank Bhushan Chaturvedi and Prateek.Singh. 25 December 2013. " A Framework for Security of ERP System on Cloud", International Journal of Current Engineering and Technology, Vol.3,No.5
[32] D. Johnson. 6 October 2011. "Security Issues in Cloud ERP". ERP Cloud news. Available online at: http://erpcloudnews.com/2011/10/security-issues-in-cloud-erp/
[33] Fumei Weng and Ming-Chien Hung. August 2014. "Competition and Challenge on Adopting Cloud ERP". International Journal of Innovation, Management and Technology, Vol. 5, No. 4.
[34] Year Book. 2012. Volume 1. Faculty of Computer Science. GOCE DELCEV UNIVERSITY – STIP.
[35] Matt Woodward. 21 July 2014. "Protecting Cloud ERP: 6 Security Realms Your Software Vendor Should Know". Available online at: http://offers.smbsuite.com/blog/protecting-cloud-erp-6-securityrealms- your-software-vendor-should-know.

INTENTIONAL BLANK

CHALLENGES OF BIG DATA APPLICATIONS IN CLOUD COMPUTING

Manoj Muniswamaiah, Dr. Tilak Agerwala and Dr. Charles Tappert

Seidenberg School of CSIS, Pace University, White Plains, New York

ABSTRACT

Big Data applications are used for decision making process for gaining useful insights hidden from large volume of data. They make use of cloud computing infrastructure for massive scale and complex computation which eliminates the need to maintain dedicated hardware and software resources. The relationship between big data and cloud computing is presented with focus on challenges and issues in data storage with different formats, data transformation techniques applied, data quality and business challenges associated with it. Also, some good practices which helps in big data analysis has been listed.

KEYWORDS

Big data; cloud computing; data transformation; data analysis; data warehousing

1. INTRODUCTION

The volume and information captured from devices and multimedia by organizations is increasing and has almost doubled every year. This big data generated is characterized to be huge, can be structured or unstructured which requires pre-processing and cannot be easily loaded into regular relational databases. Healthcare, finance, engineering, e-commerce and various scientific fields use these data for decision making and analysis. The advancement in data science, data storage and cloud computing has allowed for storage and mining of big data [1].

Cloud computing has resulted in increased parallel processing, scalability, virtualization of resources and integration with data storages. Cloud computing has also reduced the infrastructure cost required to maintain these resources which has resulted in the scalability of data produced and consumed by the big data applications. Cloud virtualization provides the process to share the resources and isolation of hardware to increase the access, management, analysis and computation of the data [1].

The main objective of this paper is to provide challenges and issues of big data applications in cloud computing which requires data to be processed efficiently and provide some good design principles.

2. BIG DATA

Data which is difficult to store, manage and analyse through traditional databases is termed as "Big Data". It requires integration of various technologies to discover hidden values from the data that is varied, complex and requires heavy computing. The characteristics of big data are.

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 221-232, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90918

1) Volume - Collection of data from different sources which would allow users to data mine the hidden information and patterns found in them.
2) Velocity - Data been streamed in real time from sources such as IoT devices. It is the speed at which data is transferred and consumed for collection and archiving.
3) Variety - Data collected in either structured or unstructured format from sensors and social networks. Unstructured data include text messages, audio, blogs.
4) Variability - Data flow can be highly inconsistent and varies during peak period and their ingestion into the data stores.
5) Value - Represents the hidden value discovered from the data for decision making.
6) Veracity - It refers to the reliability of the data source. Its importance is in the context and the meaning it adds to the analysis.
7) Validity - It refers to the accuracy of the data been collected for its intended use.
8) Vulnerability - It represents the security aspects of the data been collected and stored.
9) Volatility - How long the data needs to be stored historically before it is considered irrelevant.
10) Visualization - In-memory tools which are used to plot data points representing as data clusters or tree map [2].

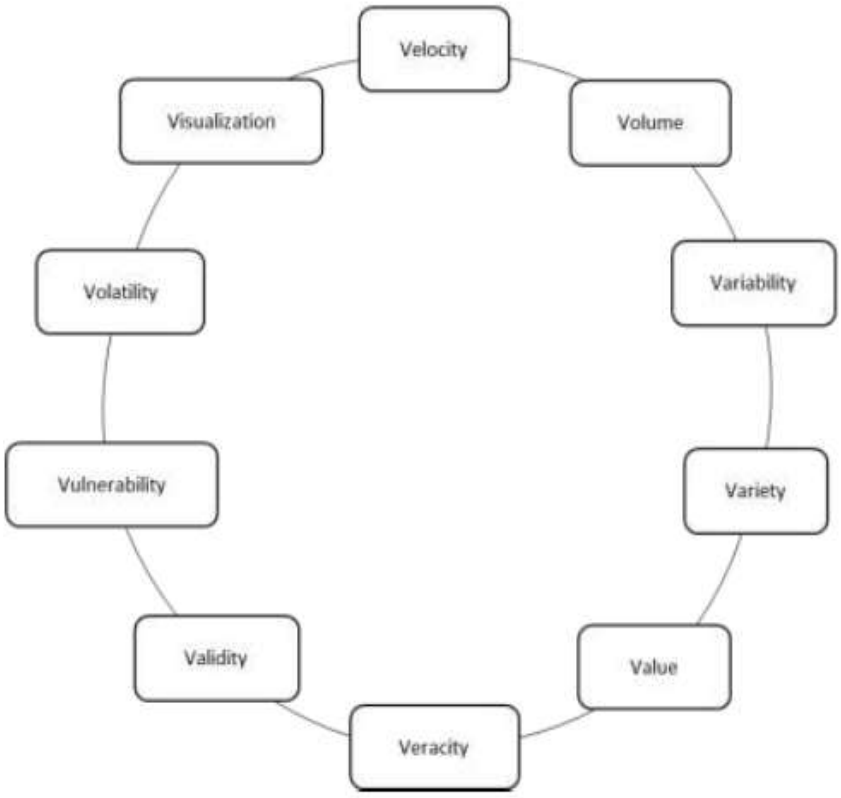


Figure 1: V's of Big Data

3. BIG DATA CLASSIFICATION

Analysis Type - Whether the data is analysed in real time or batch process. Banks use real time analysis for fraud detection whereas business strategic decisions can make use of batch process.

Processing Methodology - Business requirements determine whether predictive, ad-hoc or reporting methodology needs to be used.

Data Frequency - Determines how much of data is ingested and the rate of its arrival. Data could be continues as in real-time feeds and also time series based.

Data Type - It could be historical, transactional and real-time such as streams.

Data Format - Structured data such as transactions can be stored in relational databases.

Unstructured and semi-structured data can be stored in NoSQL data stores. Formats determine the kind of data stores to be used to store and process them.

Data Source - Determines from where the data is generated like social media, machines or human generated.

Data consumers - List of all users and applications which make use of the processed data [3].

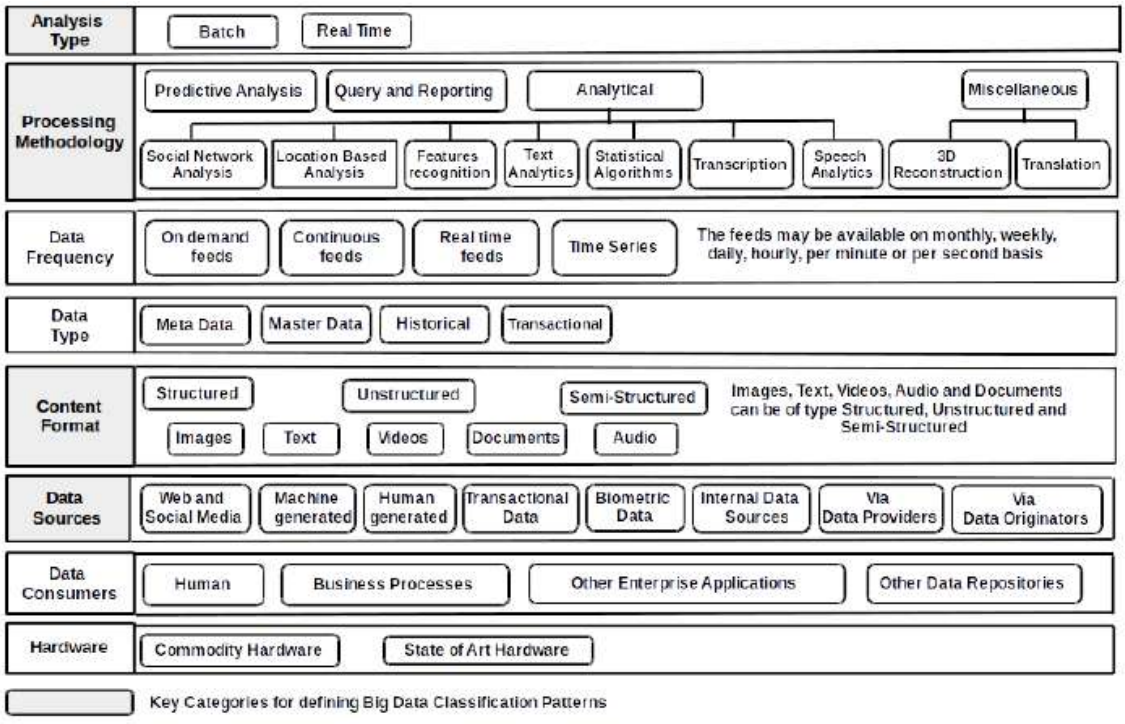


Figure 2: Big Data Classification

Big data is classified based upon its source, format, data store, frequency, processing methodology and analysis types as shown in Figure 2.

4. CLOUD COMPUTING

Cloud computing has become default platform for storage, computation, application services and parallel data processing. It allows organizations to concentrate on core business without having to worry about the infrastructure, maintenance and availability of the resources. Figure 3 shows the differences between on premise and cloud services. It shows the services offered by each computing layer and differences between them.

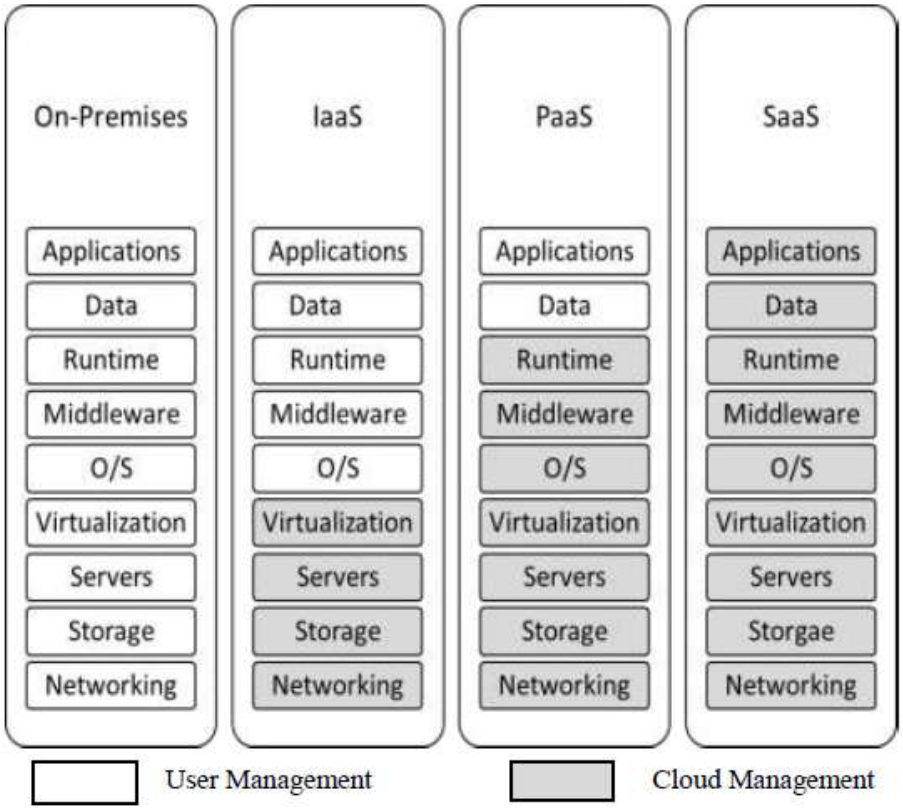


Figure 3: Summary of Key Differences

SaaS: Software as a Service

Software as a service represents the most commonly used business option in cloud services. It uses the internet to deliver applications to users. It does not require installations on client side as they run directly through web. In SaaS vendor manages all the servers, middleware and storage of the data. It eliminates users to install, manage and upgrade softwares.

PaaS: Platform as a Service

Platform as a Service model is been used by developers to build applications. It allows business to design and create applications that are integrated in to PaaS software components. These applications are scalable and highly available since they have cloud characteristics.

IaaS: Infrastructure as a Service

Infrastructure as a Service cloud computing model provides servers, storage, operating systems to organizations through virtualization technology. IaaS provides same capabilities as data centers without having to maintain them physically [4]. Figure 4 represents the different cloud computing services been offered.

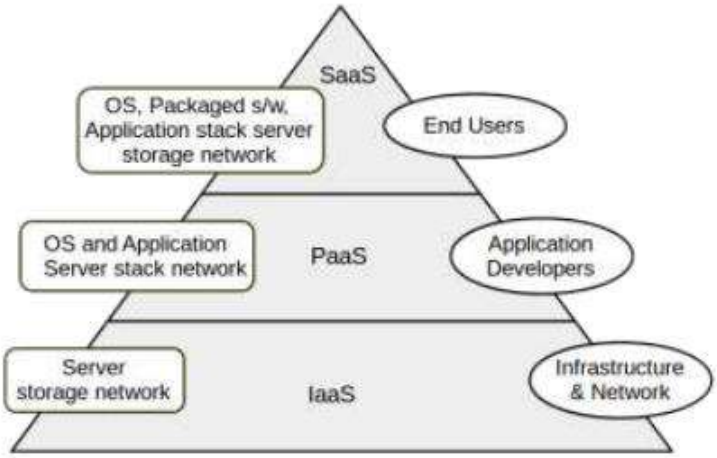


Figure 4: Primary Cloud Computing Services

5. RELATIONSHIP BETWEEN THE CLOUD AND BIG DATA

Cloud computing and big data go together, as cloud provides the required storage and computing capacity to analyse big data. Cloud computing also offers the distributed processing for scalability and also expansion through virtual machines to meet the requirements of exponential data growth. It has resulted in the expansion of analytical platforms. This has resulted in service providers like Amazon, Microsoft and Google in offering big data systems in cost efficient manner.

Cloud computing environment has several providers and user terminals. Data is collected using big data tools later it is stored and processed in cloud. Cloud provides on-demand resources and services for uninterrupted data management. The most common models for big analytics is software services such as (SaaS), Platform service like (PaaS) and Infrastructure service like (IaaS). Recently Cloud analytics and Analytics as a Service (AaaS) are provided to clients on demand. Analytics as a Service (AaaS) provides services for a fast and scalable way to integrate data in semi-structured, unstructured and structured format, transform and analyse them.

Virtualization simulates a virtual computing environment that can run operating system and applications on it. Virtualization reduces the workload and unifies them in to a physical server which helps in consolidation of multi-core CPUs in to one physical node. This reduces and improves resource utilization and power consumption as compared to the multi-node setup. Virtualized big data applications like Hadoop provide benefits which cannot be provided using physical infrastructure in terms of resources utilization, cost and data management. Virtual data includes wide range of data sources and improves the data access from heterogeneous environments. It also enables high-speed data flow over the network for faster data processing.

Information privacy and security are one of the important aspects of big data in cloud as data is hosted and processed on the third party services and infrastructure. Service level agreements must be maintained between providers and consumers in order to bring confidence in users. Security of big data in the cloud is important because data needs to be protected from malicious intruders, treats and also how the cloud providers securely maintain huge disk space [5].

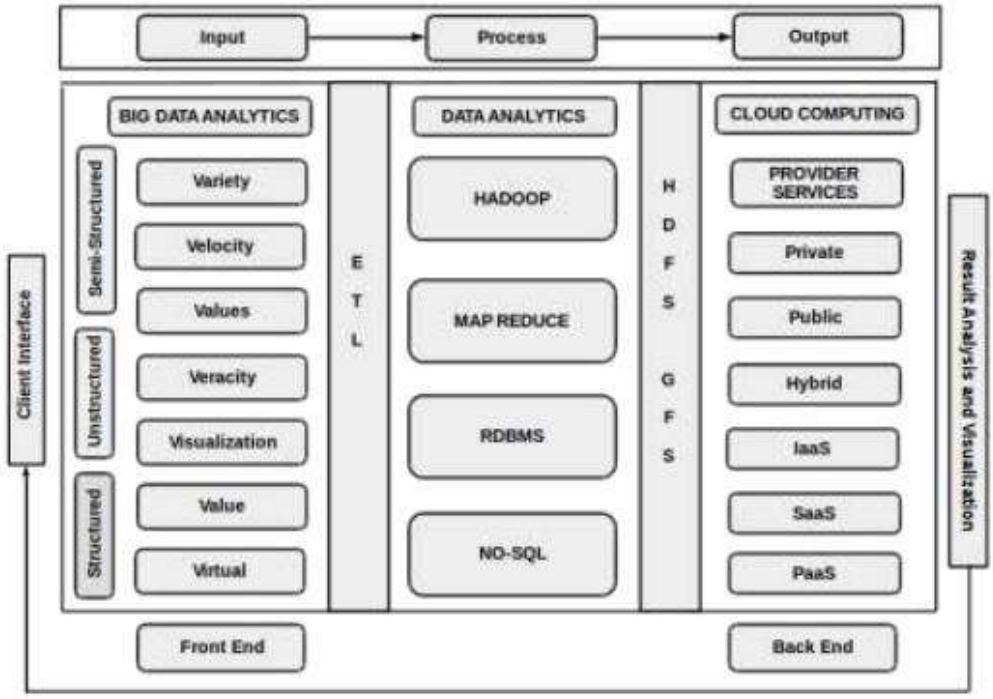


Figure 5: Big Data and Cloud Computing

The relationship between big data and cloud computing follows input, processing and output model as shown in Figure 5. The input is the data obtained from various data sources and are processed and stored using Hadoop and data stores. Processing steps includes all the tasks required to transform input data. Output is the result obtained after data been processed for analysis and visualization. Internet of Things (IoT) is one of the common factors between Cloud computing and big data. Data generated from IoT devices needs to be analysed in real time. Cloud providers allow data to be transmitted over internet or via lease lines. It provides a pathway for the data to navigate, store and be analyzed. Cloud computing provides common platform for IoT and big data. IoT is the source of the data and big data is an analytical technology platform of the data as depicted in the Figure [6].

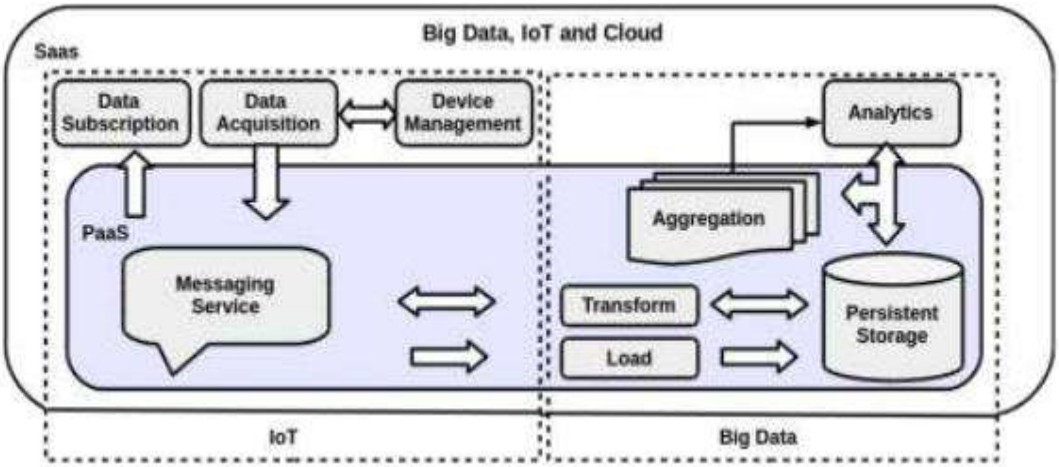


Figure 6: Overview of IoT, Big Data processing and Cloud Computing

6. CASE STUDIES

There are several case studies of big data on cloud computing.

A. Redbus

Redbus is an online travel agency for bus ticket booking in India. Redbus decided to use Google data infrastructure for data processing and analysis in order to improve customer sales and management of the ticket booking system [6].

B. Nokia mobile company

Nokia mobile phones are been used by many people for telecommunication. Nokia gathers large amount of data from mobile phones in petabyte scale for business decision strategies using Hadoop data warehouse for analytics [6].

C. Tweet Mining in Cloud

Noordhuis et al. [6] used cloud computing to gather and analyse tweets. Amazon cloud infrastructure was used to perform all the computations. Tweets were crawled and later page ranking algorithm was applied. The data crawled had nearly 50 million nodes and 1.8 billion edges.

7. DATA STORES

Modern databases needs to handle large volume and different variety of data formats. They are expected to deliver extreme performance and scale both horizontally and vertically. Database architects have produced NoSQL and NewSQL as alternatives to relational database. Below are characteristics of relational database, NoSQL and NewSQL [7].

Characteristics of Databases	Relational Database	NoSQL Database	New SQL Database
ACID property	✓	✗	✓
Analytical and OLTP support	✓	✗	✓
Data analysis	✓	✗	✓
Requires Schema	✓	✗	✗
Data format support	✗	✓	✗
Distributed parallel processing	✓	✓	✓
Scalability	✗	✓	✓

8. HADOOP TOOLS AND TECHNIQUES

Big data applications use various tools and techniques for processing and analyses of the data below table represents some of them [8].

Tools/Techniques	Description	Developed by	Written in
HDFS	Redundant and Reliable massive data storage	Introduced by Google	Java
Map Reduce	Distributed data processing framework	Introduced by Google	Java

YARN	Cluster resource management framework	Apache	Java
Storm	Stream based task parallelism	Twitter	Clojure
Spark	Stream based data parallelism	Berkeley	Scala
Map Reduce	Java API.	Introduced by Google	Java
Pig	Framework to run script language Pig Latin	Yahoo	Java
Hive	SQL-like language HiveQL	Facebook	Java
HCatalog	Relational table view of data in HDFS	Apache	Java
HBase	NoSQL column oriented Google's	BigTable	Java
Casandra	NoSQL column oriented	Facebook	Java
Flume	Import/Export unstructure or semi-structure data into HDFS. Data ingestion into HDFS.	Apache	Java
Sqoop	Tool designed for efficiently transferring bulk structured data (RDBMS) into HDFS and vies versa.	Apache	Java
Kafka	Distributed publish-subscribe messaging system for data integration	LinkedIn	Scala
Ambari	Web based cluster management UI	Hortonworks	Java
Mahout	Library of machine learning algorithms	Apache	Java
Oozie	Define collection of jobs with their execution sequence and schedule time	Apache	Java
Sentry	Role based authorization of data stored on an Apache Hadoop cluster.	Cloudera	Java
Zookeeper	Coordination service between hadoop ecosystems.	Yahoo	Java

9. RESEARCH CHALLENGES

Big data can be stored, processed and analysed in many different ways. The data generated has many attributes which results in different dimensions of data to come in to play. This gives rise to challenges in processing big data and business issues associated with it. Volume of the data been generated worldwide doubles almost every year. Retail industries do millions of translations per day and also have established data warehouses to store data to take advantages of machine learning techniques to get the insight of data which would help in the business strategies. Public administration sector also uses information patterns from data generated from different age levels of population to increase the productivity. Also, many of the scientific fields have become data

driven and probe into the knowledge discovered from these data. Although cloud computing is been used for processing of big data applications there are several challenges in data storage, data transformation, data quality, privacy, governance [9].

Data Capture and Storage

Data gathered from various sensor devices, machine logs and networks keeps increasing every year. It has changed the way we store data and their access mechanism. Previously, hard disk drives (HDD) had poor I/O performance but solid-state drives (SSD) may alleviate I/O performance to some extent but not completely.

Data Transmission

Cloud data stores are used for data storage however, network bandwidth and security poses challenges.

Data Curation

It involves data archiving, management and retrieval process. Structured data is stored in data warehouse and data marts which requires pre-processing of data before loading data and also can be queried using Standard Query Languages. Unstructured data is stored in NoSQL data stores which are schema free, support replication, distributed storage and consistency. There are various NoSQL data stores such as key-value, columnar, document and graph data stores which are specific to type of data which gets stored in them.

Scalability

Scalability is mainly manual and is static. Most of the big data systems must be elastic to handle data changes. At the platform level there is vertical and horizontal scalability.

Elasticity

Elasticity accommodates data peaks using replication, migration and resizing techniques. Most of these are manual instead being automated.

Availability

Availability refers to systems been available to users. One of the key aspect of cloud providers is to allow users to access one or more data services in short time even during security breach.

Data integrity

Data needs to be modified only by the authorized user or parties. Since the users may not be able to physically access the data, the cloud should provide mechanisms to check for the integrity of data.

Security and Privacy

Based on the service level agreement the data can be encrypted. But querying encrypted data would result in time consumption. User privacy can be de- identified, it’s also been proved that de-identification can be reverse engineered.

Heterogeneity

Big data systems need to deal with different formats of data coming from various sources. Handling unstructured data during peak hours and processing them for analysis becomes a challenge.

Data Governance

Data governance specify the way data needs to be handled, data access policies have its life cycle. Defining the data cycle is not easy task and also its policies could lead to counter productiveness.

Data Uploading

Data is usually been uploaded through internet which is unsecure but results in time consumption if they are encrypted and transmitted.

Data Recovery

Specifies the procedures and locations from where the data can be recovered. Generally there is only one destination from where the data is securely recovered.

Data Visualization

Data Visualization is used to represent knowledge graphically for better intuition and understanding. It helps to analyse the data quickly.

10. BIG DATA BUSINESS CHALLENEGES

Utilities: Power consumption prediction

Utility companies use smart meter to measure gas and electricity consumption. These devices generate huge volumes of data. A big data solution needs to monitor and analyse power generation and consumption using smart meters.

Social Network: Sentiment analysis

Social networking companies such as Twitter needs to determine what users are saying and topics which are trending in order to perform sentiment analysis.

Telecommunication: Predictive analytics

Telecommunication provides need to build churn models which depends on the customer profile data attributes. Predictive analytics can predict churn by analysing the subscribers calling patterns.

Customer Service: Call monitor

Call center big data solutions use application logs to improve performance. The log files needs to be consolidated from different formats before they can be used for analysis.

Banking: Fraud Detection

Banking companies should be able to prevent fraud on a transaction or a user account. Big data solutions should analyse transactions in real time and provide recommendations for immediate action and stop fraud.

Retailers: Product recommendation

Retailers can monitor user browsing patterns and history of products purchased and provide a solution to recommend products based on it. Retailers need to make privacy disclosures to the users before implementing these applications [3].

11. GOOD PRINCIPLES

Below are some of the good design principles for big data applications

Good Architectural Design

Big data architecture should provide distributed and parallel processing through cloud services. NoSQL can be used for high performance and faster retrieval of data. Lambda and Kappa architectures can be used for processing in real-time and batch processing mode.

Different Analytical Methods

Big data applications need to take the advantage of data mining, machine learning, distributed programming, statistical analysis, in-memory analytics and visualization techniques offered through cloud.

Use appropriate technique

No one technique can be used to analyse data. We must use appropriate technology stack to analyse the data.

Use in-memory analytics

It is not advisable to move data around. In-memory database analytics can be used to execute analytics where data resides. In-memory analytics also provides real-time processing of data.

Distributed data storage for in-memory analytics

The data needs to be partitioned and stored in distributed data stores to take the advantage of in memory analytics. Cloud computing infrastructure offers this distributed data storage solutions which must be adopted.

Coordination between tasks and data is required

To achieve scalability and fault-tolerance coordination between data and its processing tasks is required. Specialized cluster management frameworks as a Zookeeper can be used [10].

12. CONCLUSION

In the big data era of innovation and competition driven by advancements in cloud computing has resulted in discovering hidden knowledge from the data. In this paper we have given an overview of big data applications in cloud computing and its challenges in storing, transformation, processing data and some good design principles which could lead to further research.

REFERENCES

[1] Konstantinou, I., Angelou, E., Boumpouka, C., Tsoumakos, D., & Koziris, N. (2011, October). On the elasticity of nosql databases over cloud management platforms. In Proceedings of the 20th ACM international conference on Information and knowledge management (pp. 2385-2388). ACM.

[2] Abadi, D. J. (2009). Data management in the cloud: Limitations and opportunities. IEEE Data Eng. Bull, 32(1), 3-12.

[3] Luhn, H. P. (1958). A business intelligence system. IBM Journal of Research and Development, 2(4), 314-319

[4] https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

[5] https://www.ripublication.com/ijaer17/ijaerv12n17_89.pdf

[6] Sakr, S. & Gaber, M.M., 2014. Large Scale and big data: Processing and Management Auerbach, ed.

[7] Han, J., Haihong, E., Le, G., & Du, J. (2011, October). Survey on nosql database. In Pervasive Computing and Applications (ICPCA), 2011 6th International Conference on (pp. 363-366). IEEE.

[8] Zhang, L. et al., 2013. Moving big datato the cloud. INFOCOM, 2013 Proceedings IEEE, pp.405–409

[9] http://acme.able.cs.cmu.edu/pubs/uploads/pdf/IoTBD_2016_10.pdf

[10] Labrinidis and Jagadish 2012, A. Labrinidis and H. Jagadish, Challenges and Opportunities with Big Data, In Proc. of the VLDB Endowment, 5(12):2032-2033, 2012

BLIND IMAGE QUALITY ASSESSMENT USING SINGULAR VALUE DECOMPOSITION BASED DOMINANT EIGENVECTORS FOR FEATURE SELECTION

Besma Sadou[1], Atidel Lahoulou[2*], Toufik Bouden[1], Anderson R. Avila[3], Tiago H. Falk[3], Zahid Akhtar[4]

[1]Non Destructive Testing Laboratory, University of Jijel, Algeria
[2]LAOTI laboratory, University of Jijel, Algeria
[3]Institut National de la Recherche Scientifique, University of Québec, Montreal, Canada [4]University of Memphis, USA

ABSTRACT

In this paper, a new no-reference image quality assessment (NR-IQA) metric for grey images is proposed using LIVE II image database. The features used are extracted from three well-known NR-IQA objective metrics based on natural scene statistical attributes from three different domains. These metrics may contain redundant, noisy or less informative features which affect the quality score prediction. In order to overcome this drawback, the first step of our work consists in selecting the most relevant image quality features by using Singular Value Decomposition (SVD) based dominant eigenvectors. The second step is performed by employing Relevance Vector Machine (RVM) to learn the mapping between the previously selected features and human opinion scores. Simulations demonstrate that the proposed metric performs very well in terms of correlation and monotonicity.

KEYWORDS

Natural Scene Statistics (NSS), Singular Value Decomposition (SVD), dominant eigenvectors, Relevance Vector Machine (RVM).

1. INTRODUCTION

In the present decade, no reference image quality assessment (NR-IQA) and enhancement has become an interesting topic in image processing as it handles the image without the need for its original version which may not exist in some applications (e.g., image restoration). Indeed, the most efficient NR-IQA metrics are based on Natural Scene Statistics (NSS) which assume that all original images are natural and that the distortions disrupt this naturalness and make images seem unnatural [1]. This fact may make users feel uncomfortable with visual data and may consequently affect their judgement concerning data's visual quality. Most of the commonly used NR-IQA metrics in the literature are based on NSS features which are extracted from different domains such as the Discrete Wavelet Transform (DWT) domain (e.g. BIQI [2] and DIIVINE [3]), the Discrete Cosine Transform (DCT) domain (e.g. BLIINDS [4] and BLIINDS-II [5]) and

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 233-242, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90919

the spatial domain (e.g. BRISQUE [6] and NIQE [7]). However, the latest generation of metrics exploit the multi-domain information which simulates well the hierarchical structure of the visual cortex perception [8-9] (e.g. WG-LAB [10] and metrics proposed in [11] and [12]).

In the present paper, the first step of the framework is to extract a descriptive vector containing natural scene statistics features from multiple domains, namely DWT, DCT and spatial domain. For the quality estimator to be accurate, the descriptive vector should hold as less as possible of generated features which can be relevant, irrelevant or redundant. Since the work by A. Lahoulou et al. [13], more and more researchers apply feature selection methods to image quality assessment in order to keep only informative features that describe better the visual quality attributes.

Feature selection models can be classified into three main categories [14] : (1) Filter models: where a relevance index is calculated for each feature independently of the predictor considering some measures such as information measure, (2) Wrappers: these methods use learning algorithms to identify relevant features. This is what makes it more accurate than filter methods but time consuming and computationally expensive, and (3) Embedded models: it is a combination of the two previous methods, the feature selection is embedded in the learning process e.g. decision trees.

In this paper, we develop a new and efficient NR-IQA metric for grey level images. First, a features vector is extracted using three well known NR-IQA metrics operating in three different domains (i.e. DCT domain, DWT domain and spatial domain) in order to better capture human vision properties.

After that, the variable selection process is launched to keep only the most pertinent attributes. This step is performed by using an embedded method namely the dominant eigenvectors after the singular value decomposition (SVD). Finally, the nonlinear regression algorithm of the relevance vector machine (RVM) is applied to generalize prediction of quality scores to out of sample images. The LIVE (release 2) image quality database [15] provides the ground truth data (i.e. the DMOS values) as well as the test images from which the features vector is computed.

2. FEATURES EXTRACTION AND SELECTION

2.1. Image Features Extraction

The features used in this paper come from three learning-based NR-IQA metrics namely BRISQUE, BIQI and BLIINDS-II summarized in table 1 below. The size of the vectors of features is 36, 18 and 24, respectively. The blind metrics where these features come from are described as follows:

2.1.1. BRISQUE [6]

This metric does not require any transformation of the image. It directly extracts NSS features in the spatial domain. For each image, a generalized Gaussian distribution (GGD) is used to estimate the distribution, and then generates the parameters as resulted features. 18 features are extracted using 2 scales, resulting in 36 features used to evaluate the perceptual quality of an image.

2.1.2. BIQI [2]

This algorithm is based on the extraction of NSS in the wavelet domain over three scales and three orientations. Three features are extracted (mean, variance and shape) and used to classify a distorted image into one of N distortions using support vector machine (SVM), then support vector regression (SVR) is used to predict quality score.

2.1.3. BLIINDS-II [5]

Presented by Saad et al., this model works in the DCT domain. A total of 24 features are extracted from the block DCT domain and are affected by changing the type and the level of distortion. These features are then input to the Bayesian inference model to get the perceived quality estimate.

Table 1. NR-IQA metrics considered to investigate the relevance of features for perceptual quality judgement..

NR-IQA algorithm	Domain	Features	
BRISQUE	Spatial domain	36	$f_{1,\ldots},f_{36}$
BIQI	DWT domain	18	$f_{37},\ldots,f_{54}$
BLIINDS-II	DCT domain	24	$f_{55},\ldots f_{78}$

As a first step, we build in a 78-D vector of original attributes by putting all the extracted features together.

2.2. Feature Selection Technique

All 78 descriptors previously discussed are extracted from LIVE image database release 2 (LIVE II) [15]. This database contains 29 high resolution colour reference images degraded by 5 distortion types (JPEG2000, JPEG, white noise, Gaussian blur, and transmission errors using a fast fading Rayleigh channel model). A set of 982 test images is subjectively evaluated by 29 observers and the Difference Mean Opinion Scores (DMOS) are calculated as recommended by the Video Quality Experts Group (VQEG) Phase I FR-TV [16]. DMOS corresponds to the difference of the Mean Opinion Scores between reference and distorted images.

In order to eliminate redundant and irrelevant features and select only useful ones, we used singular value decomposition (SVD), which is one among a large array of techniques used for dimension reduction.

SVD decomposes a M(m x n) matrix into three matrices as:

$$M = USV^T \text{ (Eq. 1)}$$

where U and V are two orthogonal matrices of (m x p) and (n x p) dimensions, respectively.
S is a (p x p) diagonal matrix.
p is called the rank of matrix M
The diagonal positive entries of matrix S are called singular values of M. These values are arranged in descending order of their magnitude.

For feature selection, we used the same algorithm as the column select problem [17]. This algorithm can be summarized in the following steps:

i. Input the matrix where rows are images and columns are features.
ii. Compute the centralized data.
iii. Apply SVD to get the main components.
iv. Get the dimensions having most of the variation (select the dominant eigenvectors, e.g. representing the 95% of the data).
v. Compute leverage scores using the dominant eigenvectors of the principal components (.i.e. the norm of the eigenvector's coefficients).
vi. Sort the leverage scores in descending order.
vii. Get the indices of the vectors with the largest leverage scores.

In this paper, we select the features which have a leverage score greater than or equal to 0.4. Figure 1 shows the resulting selected features with their leverage scores. We can note that the most significant features come from BLIINDS-II no-reference quality metric.

3. PREDICTION MODEL

In this work, Relevance Vector Machine (RVM) [18] is employed as prediction model instead of support vector machine (SVM) [19, 20] which is the most common. This choice is made based on the benefits the RVMs offer over the SVMs, mainly probabilistic predictions and automatic estimation of the hyper-parameters.

For a given set of samples $\{x_i, t_i\}_{i=1}^{N}$ where x_i is the input variable vector, t_i is the target value, N is the length of training data. The RVM regression expression is:

$$t(x) = \sum_{i=1}^{N} w_i K(x, x_i) + w_0 + \varepsilon_n \qquad \text{(Eq. 2)}$$

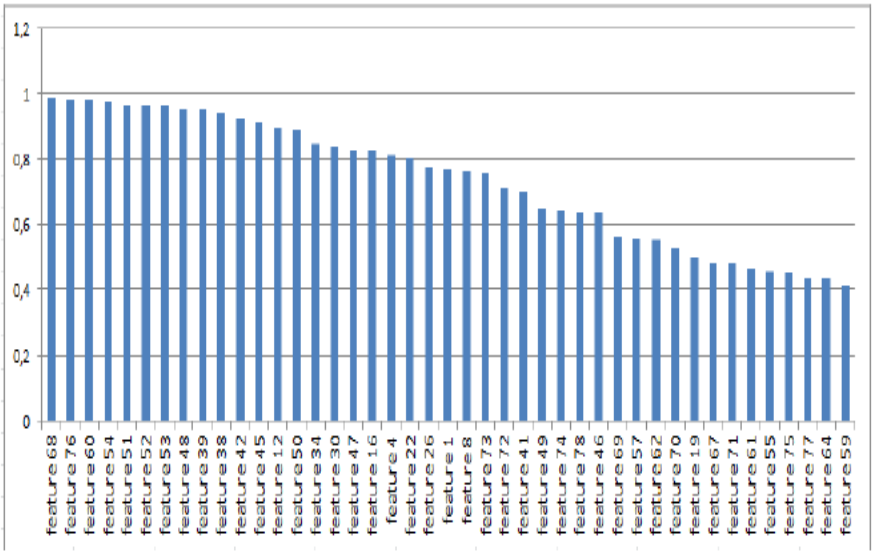


Figure 1. The most significant features with their leverage scores

Where N is the number of data points, $w = [w_1,.., w_n]$ is weights vector, w_0 is the bias, $K(x,x_i)$ is the kernel function and $\varepsilon_n = N(0,\sigma^2)$ is the error term with zero Gaussian mean and variance σ^2 . Usually, the Gaussian Kernel is preferred and its formula is:

$$K(x, x_i) = exp\left[\frac{-(x-x_i)^T(x-x_i)}{2S^2}\right] \quad \text{(Eq. 3)}$$

Where S^2 is the Gaussian kernel width.
Assuming that the samples $\{x_i,t_i\}_{i=1}^N$ are independently generated, the likelihood of all data set can be written as follows:

$$P(t|w,\sigma^2) = (2\pi\sigma^2)^{-\frac{N}{2}} exp\left\{-\frac{1}{2\sigma^2}\|t-\varphi_w\|^2\right\} \quad \text{(Eq. 4)}$$

Where φ is a design matrix having the size $N * (N+1)$ with:

$$\varphi(x_i) = [1, K(x_i,x_1), K(x_i,x_2),.., K(x_i,x_N)]^T \quad \text{(Eq. 5)}$$

The highest probability estimation of w and σ^2 of equation (4) may suffer from serious over-fitting. To solve this, Tipping [18] imposed an explicit zero-mean Gaussian prior probability distribution for the weights, w, with diagonal covariance of α as follows:

$$P(w|\alpha) = \prod_{i=0}^{N} N\left(w_i|0,\alpha_i^{-1}\right) \quad \text{(Eq. 6)}$$

Where α is a vector of $(N + 1)$ named hyper parameters.
In this way, using Baye's rule, the posterior over all unknown parameters could be calculated given the defined non informative prior distribution:

$$P(w,\alpha,\sigma^2|t) = \frac{P\left(t|w,\alpha,\sigma^2\right).P(w,\alpha,\sigma)}{\int P\left(t|w,\alpha,\sigma^2\right)P(w,\alpha,\sigma^2)\,dw\,d\alpha\,d\sigma^2} \quad \text{(Eq. 7)}$$

Full analytical solution of the integral of (Eq. 7) is obdurate. Thus, decomposition of the posterior distribution according to equation 8 below is called upon to ease the solution [18].

$$P(w,\alpha,\sigma^2|t) = P(w|t,\alpha,\sigma^2)P(\alpha,\sigma^2|t) \quad \text{(Eq. 8)}$$

The posterior distribution over the weights is calculated using Bayes rule and is given by:

$$P(w|t,\alpha,\sigma^2) = \frac{P\left(t|w,\sigma^2\right)P(w|\alpha)}{P\left(t|\alpha,\sigma^2\right)} \quad \text{(Eq. 9)}$$

The resulting posterior distribution over the weights is the multivariate Gaussian distribution:

$$P(w|t,\alpha,\sigma^2) = N(\mu,\epsilon) \quad \text{(Eq. 10)}$$

Where the mean and the covariance are respectively expressed by:

$$\mu = \sigma^{-2}\epsilon\varphi^T t \quad \text{(Eq. 11)}$$

$$\epsilon = (\sigma^{-2}\varphi^T\varphi + A)^{-1} \quad \text{(Eq. 12)}$$

With diagonal matrix $A=diag(\alpha_0,.., \alpha_N)$
For uniform hyper priors over α and σ^2, one requires only to maximize the term $(t|\alpha,\sigma^2)$ as follows:

$$P(t|\alpha,\sigma^2) = \int P(t|w,\sigma^2)P(w,\alpha)\,dw \quad \text{(Eq. 13)}$$

$$P(t|\alpha,\sigma^2) = \left[(2\pi)^{\frac{-N}{2}}/\sqrt{|\sigma^2 + \varphi A^{-1}\varphi^T|}\right] * exp\left\{-\frac{1}{2}t^T(\sigma^2 + \varphi A^{-1}\varphi^T)^{-1}t\right\} \quad \text{(Eq. 14)}$$

By simply forcing the derivatives of Equation (14) to zero, we can get the re-estimation formulas on for α and σ^2 respectively as follow:

$$\alpha_i^{new} = \frac{1-\alpha_i\epsilon_i}{\mu_i^2} \quad \text{(Eq. 15)}$$

$$(\sigma^2)^{new} = \frac{\|t-\varphi_\mu\|^2}{N-\sum_i(1-\alpha_i\epsilon_i)} \quad \text{(Eq. 16)}$$

4. EXPERIMENTS AND RESULTS

The performance of our metric is evaluated using two criteria: Pearson Correlation Coefficient (PCC) and Spearman Rank Order Correlation Coefficient (SROCC) between subjective and objective scores. The first criterion gives estimation about the prediction linear correlation while the second measures the prediction monotonicity.

Before computing PCC, a nonlinear mapping between true DMOS and algorithm scores is carried out using the logistic function with five parameters [21]. The expression of the quality score which is the predicted MOS is given by:

$$DMOS_p = \beta_1 logistic(\beta_2, D - \beta_3) + \beta_4 D + \beta_5 \quad \text{(Eq. 17)}$$

Where D and $DMOS_p$ are the predicted scores before and after regression, respectively.
β_1 to β_5 are the regression parameters estimated using fmin search function in Matlab's optimization Toolbox. The logistic function is given by:

$$logistic(\tau, D) = \frac{1}{2} - \frac{1}{1+exp(\tau D)} \quad \text{(Eq. 18)}$$

We randomly split the images of LIVE II database into two non-overlapping sets, 80% for training and the remaining 20% for test phase. This random splitting is repeated 100 times in order to ensure the robustness of our metric. At the end, we calculate the average of the obtained performance criteria.

Tables 2 and 3 give SROCC and PCC mean values between subjective and objective scores on each of the five distortion subsets and the entire database (noted by ALL). These values are compared to six state-of-the-art general-purpose NR-IQA metrics (BIQI, BLIINDS, DIIVINE, BLIINDS-II, BRISQUE and NIQE).

Table 2. SROCC of different methods on LIVE II database.

	JP2K	JPEG	WN	Gblur	FF	ALL
BIQI	0.736	0.591	0.958	0.778	0.700	0.726
BLIINDS	0.805	0.552	0.890	0.834	0.678	0.663
DIIVINE	0.913	0.910	**0.984**	0.921	0.863	0.916
BLIINDS -II	0.951	0.942	0.978	0.944	**0.927**	0.920
BRISQUE	0.914	**0.965**	0.979	**0.951**	0.877	0.940
NIQE	0.917	0.938	0.966	0.934	0.859	0.914
Proposed	**0.949**	0.924	0.982	0.946	0.884	**0.955**

Table 3. PCC of different methods on LIVE II database.

	JP2K	JPEG	WN	Blur	FF	ALL
BIQI	0.750	0.630	0.968	0.800	0.722	0.740
BLIINDS	0.807	0.597	0.914	0.870	0.743	0.680
DIIVINE	0.922	0.921	**0.988**	0.923	0.888	0.917
BLIINDS-II	**0.963**	**0.979**	0.985	0.948	**0.944**	0.923
BRISQUE	0.923	0.974	0.985	0.951	0.903	0.942
NIQE	0.937	0.956	0.977	0.953	0.913	0.915
Proposed	0.962	0.945	0.981	**0.957**	0.911	**0.953**

Numerical results show that the proposed no-reference image quality assessment metric achieves good performances in terms of monotonicity (table 2) and correlation (table 3). The first position best results are mentioned in bold whereas the second positions best results are the underlined values. We can notice that the proposed metric gives the first or the second best performance for all the subsets except that of the encoded images via JPEG algorithm.

Furthermore, the scatter plot of our method for test set with median SROCC is provided in figure 2; where the horizontal axis corresponds to the objective scores and the vertical axis corresponds to subjective scores. Every dot in the plot represents an image in the database. It can be seen that most of the dots are clustered around the red line that represent ideal linear correlation line "Proposed=DMOS", this means that the proposed metric achieves good correlation with human scores.

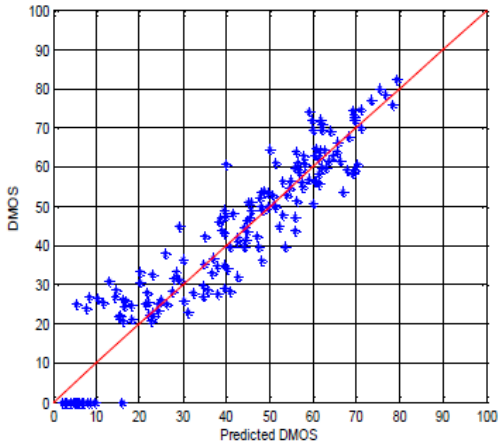


Figure 2. The scatter plots of the predicted perceived quality vs. the DMOS

5. CONCLUSION

The two main ideas of this work is that the most successful NR-IQA metrics are based on NSS features and that the multi-domain information simulate well the hierarchical structure of the visual cortex perception. For these reasons, the features used to build the present NR-IQA metric are collected from three NR-IQA methods based on NSS features operating in three different domains (spatial, DWT and DCT). Only pertinent features are input to the relevance vector machine algorithm to predict the objectives score. The step of feature selection is achieved using Singular Value Decomposition (SVD) based dominant eigenvectors. Numerical experiments show that the proposed metric is competitive with DIVINE, BLIINDS II and BRISQUE methods. It also outperforms BLIINDS, BIQI and NIQE algorithms.

REFERENCES

[1] D. Zhang, Y. Ding , N. Zheng, "Nature scene statistics approach based on ICA for no- reference image quality assessment", Proceedings of International Workshop on Information and Electronics Engineering (IWIEE), 29 (2012), 3589- 3593.

[2] A. K. Moorthy, A. C. Bovik, A two-step framework for constructing blind image quality indices[J], IEEE Signal Process. Lett., 17 (2010), 513-516.

[3] L. Zhang, L. Zhang, A.C. Bovik, A Feature-Enriched Completely Blind Image Quality Evaluator, IEEE Transactions on Image Processing, 24(8) (2015), 2579- 2591.

[4] M.A. Saad, A.C. Bovik, C. Charrier, A DCT statistics-based blind image quality index, Signal Process. Lett. 17 (2010) 583–586.

[5] M. A. Saad, A. C. Bovik, C. Charrier, Blind image quality assessment: A natural scene statistics approach in the DCT domain, IEEE Trans. Image Process., 21 (2012), 3339-3352.

[6] A. Mittal, A.K. Moorthy, A.C. Bovik, No-reference image quality assessment in the spatial domain, IEEE Trans. Image Process. 21 (2012), 4695 - 4708.

[7] A. Mittal, R. Soundararajan, A. C. Bovik, Making a completely blind image quality analyzer, IEEE Signal Process. Lett., 20 (2013), 209-212.

[8] N. Kruger, P. Janssen, S. Kalkan, M. Lappe, A. Leonardis, J. Piater, A. Rodriguez-Sanchez, L. Wiskott, "Deep hierarchies in the primate visual cortex: What can we learn for computer vision?", IEEE Trans. Pattern Anal. Mach. Intell., 35 (2013), 1847–1871.

[9] D. J. Felleman, D. C. Van Essen, "Distributed hierarchical processing in the primate cerebral cortex," Cerebral cortex, 1 (1991), 1–47.
[10] B. Sadou, A. Lahoulou, T. Bouden, A New No-reference Color Image Quality Assessment Metric in Wavelet and Gradient Domains, 6th International Conference on Control Engineering and Information Technologies, Istanbul, Turkey, 25-27 October (2018), 954-959.
[11] Q. Wu, H. Li, F. Meng, K. N. Ngan, S. Zhu, No reference image quality assessment metric via multi-domain structural information and piecewise regression. J. Vis. Commun. Image R., 32(2015), 205–216.
[12] X. Shang, X. Zhao, Y. Ding, Image quality assessment based on joint quality-aware representation construction in multiple domains, Journal of Engineering 2018 (2018), 12p.
[13] A. Lahoulou, E. Viennet, A. Beghdadi, ''Selecting low-level features for image quality assessment by statistical methods,'' J. Comput. Inf. Technol. CIT 18 (2010), 83–195.
[14] H. Liu, H. Motoda, R. Setiono, and Z. Zhao, "Feature Selection: An Ever Evolving Frontier in Data Mining", Journal of Machine Learning Research, Proceedings Track, pp. 4-13, 2010.
[15] H. R. Sheikh, Z. Wang, L. Cormack, A. C. Bovik, LIVE Image Quality Assessment Database Release 2, http://live.ece.utexas.edu/research/quality
[16] Final VQEG report on the validation of objective quality metrics for video quality assessment:http://www.its.bldrdoc.gov/vqeg/projects/frtv_phaseI/
[17] M. W. Mahoney, P. Drineas, "CUR matrix decompositions for improved data analysis," in Proc. the National Academy of Sciences, February 2009.
[18] M.E. Tipping. The relevance vector machines. In Advances in Neural Information Processing Systems 12, Solla SA, Leen TK, Muller K-R (eds). MIT Press: Cambridge, MA (2000), 652-658.
[19] D. Basak, S. Pal, D.C. Patranabis, Support vector regression, Neural Information Processing – Letters and Reviews, 11 (2007).
[20] B. SchÖlkopf, A.J. Smola, Learning with Kernels. MIT press, Cambridge, (2002).
[21] H. R. Sheikh, M. F. Sabir, A. C. Bovik, A statistical evaluation of recent full reference image quality assessment algorithms, IEEE Trans. Image Process., 15 (2006), 3440–3451.

AUTHORS

Besma Sadou is currently a PhD student in the department of Electronics at university of Jijel (Algeria). She also works as full-time teacher of mathematics at the middle school. Her research interests are focused on reduced and no-reference image quality assessment.

Atidel Lahoulou is Doctor in Signals and Images from Sorbonne Paris Cité (France) since 2012. She earned her Habilitation Universitaire in 2017 and is currently associate professor in the department of computer science at university of Jijel (Algeria). Her research interests include visual data quality evaluation and enhancement, biometrics, machine learning and cybersecurity.

Toufik Bouden received the engineer diploma (1992), MSc (1995) and PhD (2007) degrees in automatics and signal processing from Electronics Institute of Annaba University (Algeria). Since 2015, he is full professor in the department of Automatics. His areas of research are signal and image processing, non-destructive testing and materials characterization, biometrics, transmission security and watermarking, chaos, fractional system analysis, synthesis and control.

Anderson R. Avila received his B.Sc. in Computer Science from Federal University of Sao Carlos, Brazil, in 2004 and his M.Sc in Information Engineering from Federal University of ABC in 2014. In October 2013, Anderson worked as a short-term visiting researcher at INRS, where he now pursues his Ph.D degree on the topic of speaker and emotion recognition. His research interests include pattern recognition and multimodal signal processing applied to biometrics.

Tiago H. Falk is an Associate Professor at INRS-EMT, University of Quebec and Director of the Multimedia Signal Analysis and Enhancement (MuSAE) Lab. His research interests are in multimedia quality measurement and enhancement, with a particular focus on human-inspired technologies.

Zahid Akhtar is a research assistant professor at the University of Memphis (USA). Prior to joining the University of Memphis, he was a postdoctoral fellow at INRS-EMT-University of Quebec (Canada), University of Udine (Italy), Bahcesehir University (Turkey), and University of Cagliari (Italy), respectively. Dr. Akhtar received a PhD in electronic and computer engineering from the University of Cagliari (Italy). His research interests are biometrics, affect recognition, multimedia quality assessment, and cybersecurity.

MOTION COMPENSATED RESTORATION OF COLONOSCOPY IMAGES

Nidhal Azawi and John Gauch

Department of Computer Science and Computer Engineering,
University of Arkansas, Fayetteville, Arkansas

ABSTRACT

Colonoscopy examinations are widely used for detecting colon cancer and many other colon abnormalities. Unfortunately, the resulting colon videos often have artifacts caused by camera motion and specular highlights caused by light reflections from the wet colon surface. To address these problems, we have developed a method for motion compensated colonoscopy image restoration. Our approach utilizes RANSAC-based image registration to align sequences of N consecutive images in the colonoscopy video and restores each frame of the video using information from these aligned images. We compare image alignment quality when N adjacent images are registered to each other versus registering images with larger step sizes between them. Three types of image pre processing were evaluated in our work. We found that the removal of non-informative images prior to image registration produced better alignment results and reduced processing time. We also evaluated the effects of image smoothing and resizing as a pre processing step for image registration.

KEYWORDS

RANSAC, Image alignment, Informative images, Non informative images, motion compensation, Colonoscopy.

1. INTRODUCTION

Image registration/alignment has been used in a wide range of image processing, computer vision and pattern recognition applications, including panorama creation, motion estimation, object recognition, and multi-sensor data fusion. For this reason, a lot of work has been done to develop fast and efficient image alignment methods.

The process of overlying two or more images by matching common features identified in the images using some methods is called image registration [1]. These images can be taken at different times may be taken in different angles or different camera/devices. Image registration-based feature matching involves feature detection and extraction, feature matching, transformation and fitting function, and image resampling and transformation.

Another image registration definition is illustrated by [2] who stated that image registration/aligning is the procedure to align two or more images after determining the optimal transformation that can fit or give the best transformation for a particular input image. Image registration also called image fusion, warping or matching. Registering two or more images helps

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 243-256, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90920

to combine information from multiple images. Image registration helps to integrate information for more than one image which are taken from different viewpoints, different angles, different times or different sensors. Therefore, it is very important step in image or video analysis

Image alignment methods can be classified into two broad categories based on how images are aligned with each other. The first category is area-based matching. Here, patches from one image are compared to patches in another image at different offsets to determine the (dx,dy) motion of the patch from frame to frame. A large number of methods have been devised for comparing patches, and for searching for (dx,dy) displacements with different accuracy/speed trade-offs. Recent examples of area-based approaches are described by [3], [4], [5] and [6].

The second category of image alignment methods is based on feature matching. Here, each image is examined to find feature points based on some search criteria, and the neighbourhood around each feature point is used to create a feature vector that can be matched against feature vectors from another image. Feature points are typically found by calculating geometric properties in an image, and detecting visually interesting points like corners, centres of bright/dark objects. Feature descriptors are chosen so they describe the local neighbourhood of feature points in a way that is robust to changes in position, orientation, scale, and illumination.

The scale invariant feature transform (SIFT) is one of the most widely used feature-based image alignment techniques [7]. Other recent examples of this approach include [8] and [9]. A hybrid approach using both area and feature matching was developed in [10].

Another proposed scheme for alignment of differently exposed images is by [11]. The proposed method consists of two stages. First, directional mapping to normalize images and to mitigate the effect of saturation has been implemented. Second, intensity invariant features have been represented using LBP (a non-parametric local binary pattern). The experimental results showed that their method achieved better accuracy than the state-of-the-art methods.

An efficient and robust method has been done in image alignment based on matching of relative gradient map. The match of the relative gradient feature from the training dataset has been used to find some candidate poses of the pattern from image. An iterative energy minimization approach is used to verify the candidate images. The authors show this approach is robust against non-uniform illumination [12].

Another approach is use viewpoint invariant patches (VIP) in the alignment of scenes and images especially if there are images that are seen or captured from different viewpoints [13]. VIP consists of features that are uniquely finds the matching transformation between 3D sciences. Features vector of VIP contains some invariant features such as 3D position, local gradient orientation in the patch plane, SIFT descriptors, and surface normal and the patch scale. The authors claim that their method able to distinguish between square and rectangle while affine invariant approaches could not recognize them. The proposed method rectified the image texture with respect to the geometry locality of the science. Ortho-texture (viewpoint independent of 3D science) can be seen using rectification.

Image registration in medical image analysis include applications of image registration to integrate information from computed tomography (CT), magnetic resonance imaging (MRI), single photon emission computed tomography (SPECT). Application areas include computer aided diagnosis, surgery simulation, intervention and treatment planning, radiation therapy,

anatomy segmentation, computational model building and image subtraction for contrast enhanced based approach, correction of scatter attenuation, partial volume corrections based on CT images, and assisted/guided surgery. Medical image registration has been applied on a wide range of body images such as brain [14], [15], [16], heart [17], breast, bones, wrist, entire body, liver, kidney, spine, knee, analysis of heart motion detection and many others [2].

In this paper, we address the problem of colonoscopy image registration. The proposed approach relies on three pre-processing steps, namely the removal of non-informative images, image resizing, median and mean filtering with or without image resizing. To the best of our knowledge we are the first researcher who tested these three pre-processing steps in image registration for colonoscopy images. By creating an image panorama from registered images, we are able to restore and enhance image details in colonoscopy images. The experimental set up shows that the removal of non-informative images allows enhancing the alignment results.

2. OUR APPROACH

Image alignment is an important component of our research. This is a very challenging task because we are dealing with colonoscopy images taken with a moving camera with significant changes in illumination and a number of images artefacts. It should be possible to align sequences of colonoscopy images with gradual changes in viewpoint, but it may not be possible to align very long sequences of images or sequences with rapid motion to each other. Our work will try to overcome these difficulties by preprocessing the colonoscopy video to identify and remove non-informative images from the input prior to registration (see figure1). The method we use to find and remove bad images is based on feature-based image classification described in our earlier paper [18].

To register sequences of N colonoscopy images to each other we used RANSAC (random sample consensus) to solve for the projective transformation that produces the best image alignment. RANSAC is a widely used for fitting models to some data in the presence of outliers. As the name suggest, this approach uses trial and error approach to find model parameters that best fit the data. The RASAC algorithm works as follows [19].

Let X represent the set of experimental data points we wish to model, we choose S1 points from X at random and build the parametric model through these points. To evaluate this model, we check the error tolerance for other points in X to find the subset that are less than distance D from the model. We call this the consensus set S*. The goal of RASAC is to find the parameters with the largest size consensus set S*, so we repeat this process until we find S* with more than V members or until a pre-determined number of random trials T has been performed. The speed and accuracy of RANSAC is controlled by three parameters, the distance threshold D, the target consensus set size V, and the maximum number of trials T.

They key to effective image registration is finding corresponding points in adjacent images. We do this by extracting a collection of feature points from each image and match their corresponding feature vectors to identify potential point correspondences. We performed RANSAC based image registration with four different types of image features (SURF, BRISK, FAST, and HARRIS) and our experiments show that SURF provides the best registration accuracy for our colonoscopy images [18].

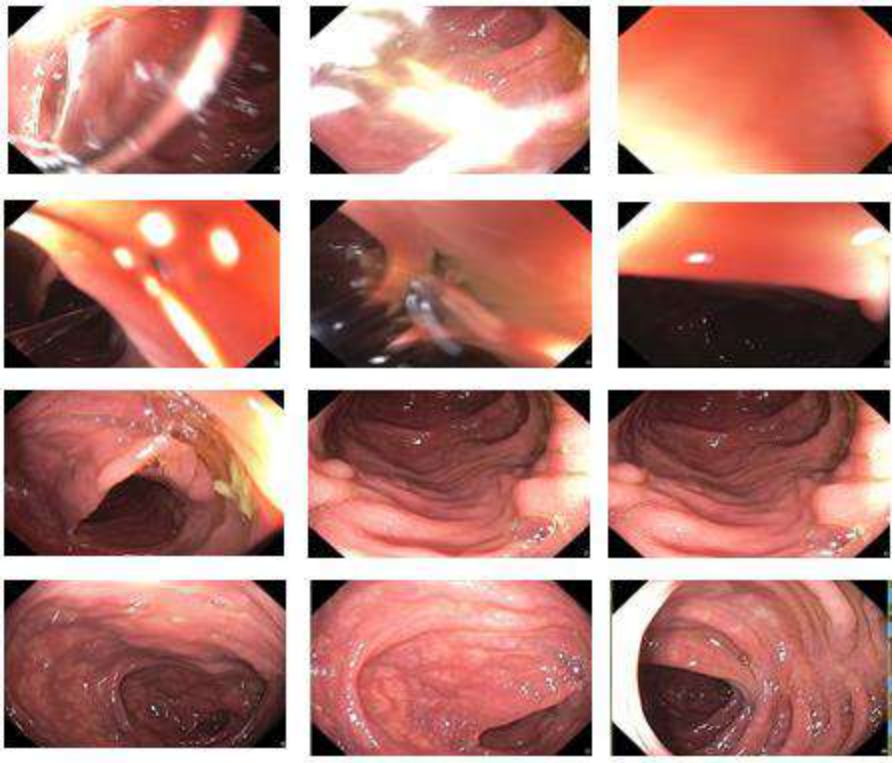


Figure 1. An illustration typical colonoscopy images. The top six images are non-informative because they are very blurred or have large specular highlights. The bottom six images are informative views of the colon, with small specular highlights and little blurring.

We evaluated RANSAC based image registration with affine and projective transformations. Affine transformations capture translation, rotation, scaling and sheer between consecutive images, while projective transformations also capture changes due to changes in viewpoint. Affine transformations preserve parallelism while projective transformations do not. Affine transformation can be defined in terms of the motion of vertices of a triangle while projective transformation is defined by the transformation of quadrangle vertices. The affine transform equation is $A \cdot H_A = C$ where

$$A = \begin{pmatrix} x1 & y1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & x1 & y1 & 1 \\ x2 & y2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & x2 & y2 & 1 \\ x3 & y3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & x3 & y3 & 1 \end{pmatrix} \quad H_A = \begin{pmatrix} hf1 \\ hf2 \\ hf3 \\ hf4 \\ hf5 \\ hf6 \end{pmatrix} \quad C = \begin{pmatrix} X1 \\ Y1 \\ X2 \\ Y2 \\ X3 \\ Y3 \end{pmatrix}$$

The affine homography matrix is represented as a vector called H_A that contains six degrees of freedom (DOFs). Hence, the minimum number of points needed to solve for homography is three

matching points (x1,y1), (x2,y2) and (x3,y3). These three matching points are combined into matrix A

The projective transform is given by $A \cdot H_P = C$ where

$$A = \begin{pmatrix} x1 & y1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & x1 & y1 & 1 \\ x2 & y2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & x2 & y2 & 1 \\ x3 & y3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & x3 & y3 & 1 \\ x4 & y4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & x4 & y4 & 1 \end{pmatrix} \quad H_P = \begin{pmatrix} hp1 \\ hp2 \\ hp3 \\ hp4 \\ hp5 \\ hp6 \\ hp7 \\ hp8 \end{pmatrix} \quad C = \begin{pmatrix} X1 \\ Y2 \\ X3 \\ Y4 \\ X5 \\ Y6 \\ X7 \\ Y8 \end{pmatrix}$$

The projective homography matrix is represented as a vector is called HP which has eight DOF and for that reason the minimum number of points required to solve for homography is four points. These four matching points (x1,y1), (x2,y2), (x3,y3) and (x4,y4) are gathered into tow dimensional matrix A. The coordinate points (Xi,Yi) for affine or projective transformation can be calculated by multiplying the matching points A by the corresponding homography matrix [20] [21].

Using RANSAC to align colonoscopy images with affine transformations yields a large number of non singular transformation matrices, which means there is no viable affine transformation that can successfully align these two images. Hence affine transformations are not a good choice for image registration. Since the camera capturing colonoscopy video is changing position during the procedure, we will use RANSAC to calculate the best projective transformation that aligns all pairs of images within a moving 10 frame window of the colonoscopy image. The algorithm we use to register, and process colonoscopy images has the following steps:

- Loop over all sets of 10 consecutive images in the colonoscopy video.
- Detect and extract features points for all 10 images in the sequence.
- Find the matching feature points for all pairs of images im1 and im2.
- Determine the best projective transformation using RANSAC algorithm.
- Exclude all transforms that fail any condition below:
  - o The number of inlier points less than 5 points.
  - o The determinant of the transform less than 0.5.
  - o The image difference after alignment is less than before alignment.
- Save aligned images in an output directory and create image panorama.

3. EXPERIMENTAL RESULTS

To evaluate the effectiveness of this image registration algorithm on colonoscopy images, we performed a number of experiments using a collection of 1000 typical colonoscopy images. These images have been automatically classified as being informative or non-informative using feature-based image classification [18].

3.1 Evaluation Metrics

- In each of our experiments, we considered the following four evaluation metrics. Three of these measures are objective, while one is subjective and depends on the viewer's requirements.
- The alignment error is calculated as the average RMSE between pairs of images after alignment for all images that are successfully aligned.

$$RMSE = \sqrt{\frac{\sum_{i=1}^{H}\sum_{j=1}^{W}[im1(i,j) - T(im2(i,j)]^2}{H \cdot W}}$$

  where T(im2(i,j)) is image im2(i,j) after it has been transformed by the optimal projective transformation T to align with image im1(x,y).
- The percentage aligned is the percentage of image pairs with valid projective transformations out of the total number of images in the sequence.
- The average computation time for aligning images in the colonoscopy video.
- The visual quality of the panorama image generated from the aligned images compared to the original images in the colonoscopy video. Panorama images that have specular highlights removed and/or have improved image detail would be considered high quality, and panoramas that are highly distorted would be considered low quality.

3.2 Parameter Selection

We performed RANSAC based image registration with four different types of image features (SURF, BRISK, FAST, and HARRIS) and our experiments show that SURF provides the best registration accuracy for our colonoscopy images [18]. This image registration algorithm has several parameters that control the accuracy and speed of colonoscopy image alignment.

The identification of SURF feature points is controlled by a metric threshold. As this threshold is decreased more SURF feature points are detected. We experimented with a range of metric thresholds between [0..1000] and had the best alignment results with a metric threshold of 100. The number random trials used by RANSAC to find the optimal transformation effects the speed and accuracy of the results. As the number of trials increases, the quality of the alignment improves, but the computational cost increases. We experimented with a range of values between [400..3000] and selected 2500 to align images in reasonable time.

After choosing the metric threshold and the number of trials, we conducted experiments to evaluate two pre processing operations, median filtering and image resizing.

To smooth these images to remove noise, we performed median filtering with a 10x10 mask. The root mean square image alignment error (RMSE) when median filtering was used was 3.52 for the 150 images we aligned. The percentage aligned after median filtering was 30% for this group of images. The RSME without median filtering was slightly lower at 3.44 and the alignment

percentage increased to 43%. Median filtering reduces the number of matching points which in turn reduces the number of frames that can be successfully aligned.
The images we extracted from our colonoscopy video were 1347x540 pixels. We experimented with image resizing prior to image alignment with a scale factor of 0.5 (673x270) and with a scale factor of 0.25 (336x135). Unfortunately, these resized images were too small for our algorithm to find enough matching points to successfully align any images. Median filtering before or after image resizing did not improve these results, so we will use our original images in our subsequent image alignment experiments.

3.3 Pairwise Image Alignment

Our first experiment performed pairwise image alignment with 1000 adjacent colonoscopy images. For each pair of images, we calculated the projective transformation using RANSAC that provided the best image alignment. Our experiments show that the average RMSE for the 1000 images was equal to 8.85. This alignment error was reduced to 7.8 when the non-informative images were removed from the input sequence prior to alignment. Similarly, the percentage successfully aligned for the full video sequence was 61.5%. This was increased substantially to 80.6% when non-informative images were omitted from the input sequence. These improvements in alignment error and percentage aligned are to be expected because the non-informative images are so highly distorted [18].

Once pairwise alignments have been calculated, it is possible to partition the 1000 images into aligned sequences by connecting adjacent images that are successfully aligned to each other. In our case, this resulted in 22 sequences of images that varied in length from [2..385] images. Once we have calculated this partition of the colonoscopy video into separate sequences, we can focus our image restoration and display efforts on these sequences. For example, we can recreate 22 video clips that contain only the informative images, or in some cases we can create a panorama image using these images (see figure 2).

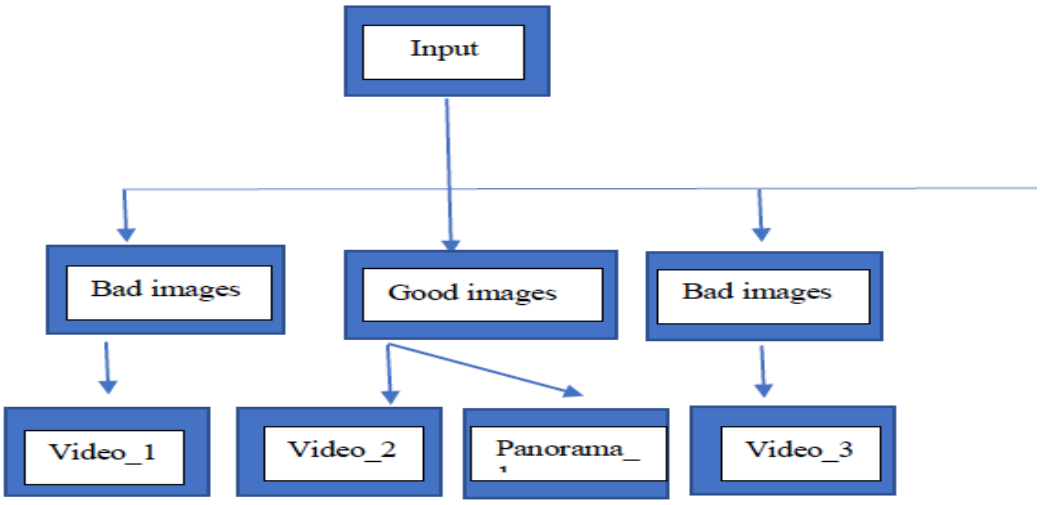


Figure 2. Visualization structure for pair image alignment. Once the input video has been classified into informative (good) images and non-informative (bad) images, we have the option of creating video clips or panoramas from the good images for each aligned sequence of images.

3.4 **Sequence Image Alignment**

Our second experiment, we performed image sequence alignment as a pre processing step to image panorama creation. For each frame in the colonoscopy video, we calculated the best alignment with the 10 subsequent images. Figure 3 shows that in some cases only a subset of the 10 subsequent images were able to be successfully aligned with the starting image.

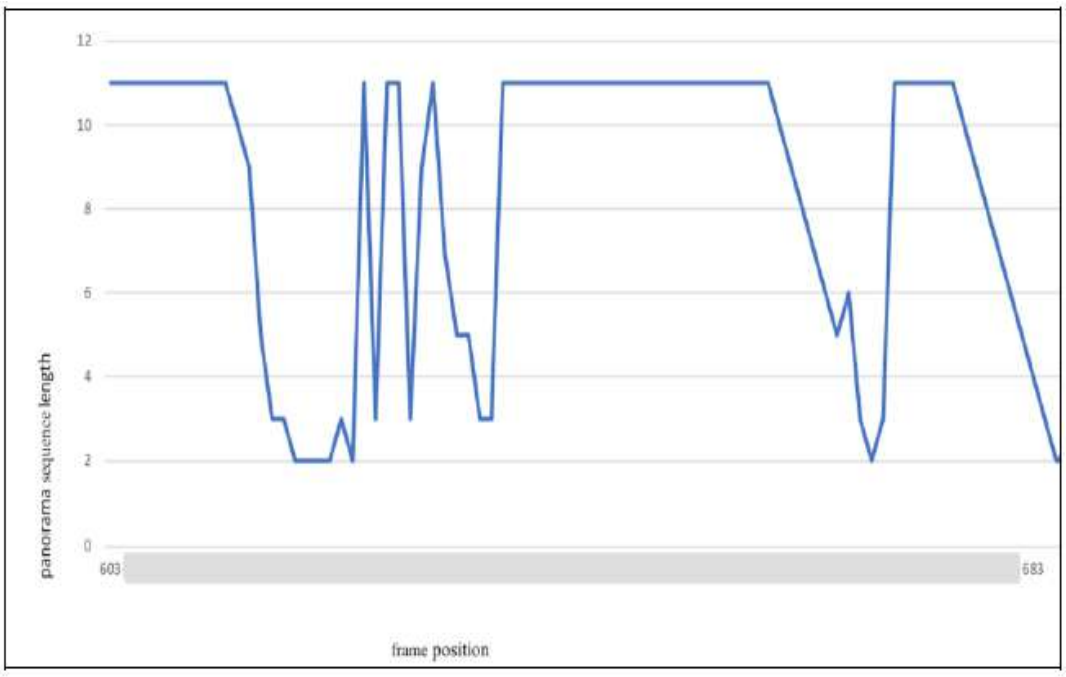


Figure 3. Plot of panorama sequence length for colonoscopy frames 603 to 683. Notice that the sequence length ranges from 11 frames down to only 2 frames. This is because some portions of the colonoscopy video have high motion or contain non-informative images.

When we evaluated our image alignment results for the entire 1000 frame sequence, we had a RMSE of 4.16 and a percentage aligned of 37%. When we ran the experiment again, excluding the non-informative images, the RMSE increased slightly to 4.38 and the percentage aligned increased significantly to 48%.

When we compare our image sequence alignment results to our pairwise image alignment results we can see that the percentage aligned is much lower for sequence alignment. This is because we are attempting to align images that are more than one frame apart from each other in time, so there has been more motion, and it becomes more difficult to find and match image features. Consequently, it is harder to successfully align images as the sequence length increases.

The average CPU time for image alignment and panorama creation was also significantly reduced from 15.7 seconds for the original video down to 5.1 seconds when non-informative images were excluded. This large change in CPU time can be explained by looking at the RANSAC image alignment process. When two images can be successfully aligned, the algorithm converges before the maximum number of iterations is reached. When two images can not be aligned, RANSAC

will attempt the maximum number of iterations before failing. Therefore, attempting to align non-informative images to other images wastes a lot of CPU time.

The results from our image sequence alignment and panorama creation are illustrated in the figures below. In figure 4 and figure 5, we show how some subsequences produce very good panoramas. In figure 6 and figure 7, we show how non-informative subsequences produce very poor panoramas that has no useful information.

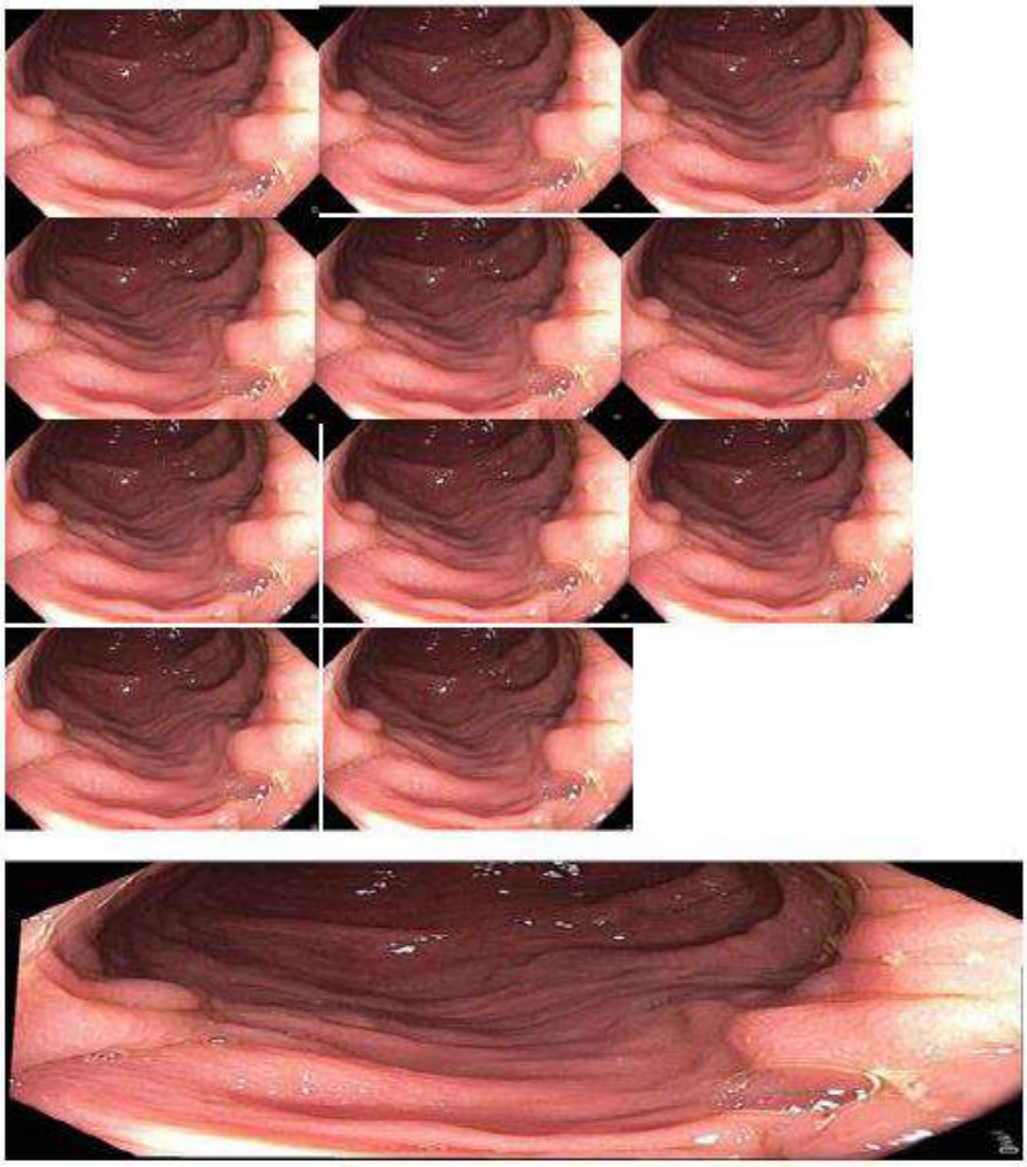


Figure 4. An illustration of image sequence alignment showing eleven consecutive input images and the resulting image panorama. Notice that the panorama includes additional information on the left and right sides of the first image in the sequence.

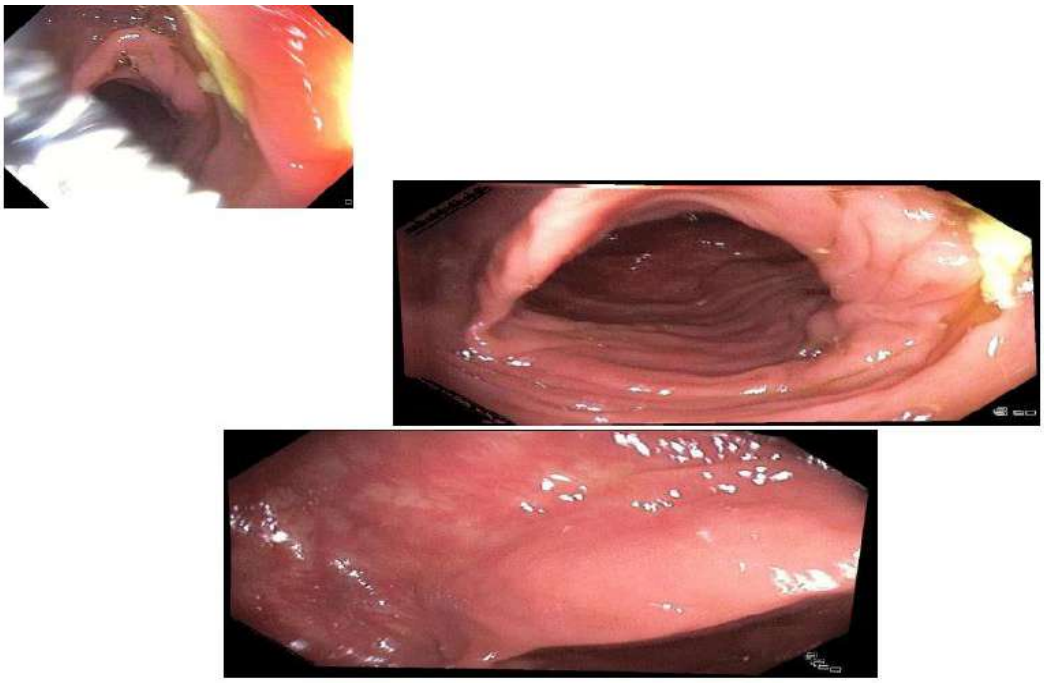


Figure 5. An illustration of two additional image panoramas. In both cases, the width of the panorama is larger than the first frame in the image sequence and include more information about adjacent colon features.

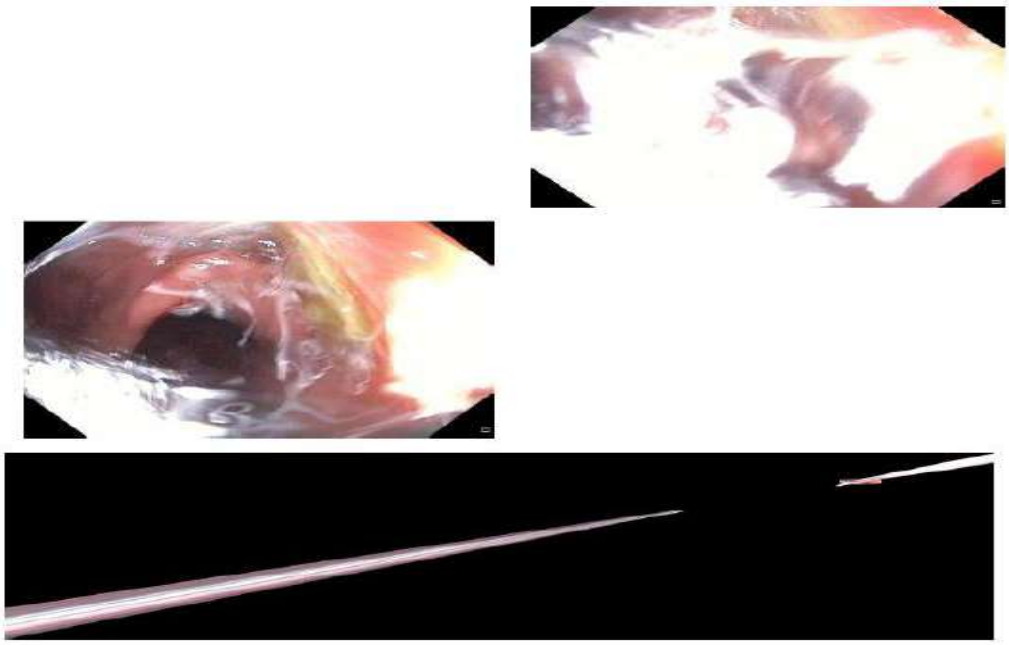


Figure 6. An illustration of unsuccessful panorama creation with non-informative images. The three colonoscopy images above were incorrectly aligned to each other by our RANSAC method. This produces singular transformations, and a highly distorted image panorama.

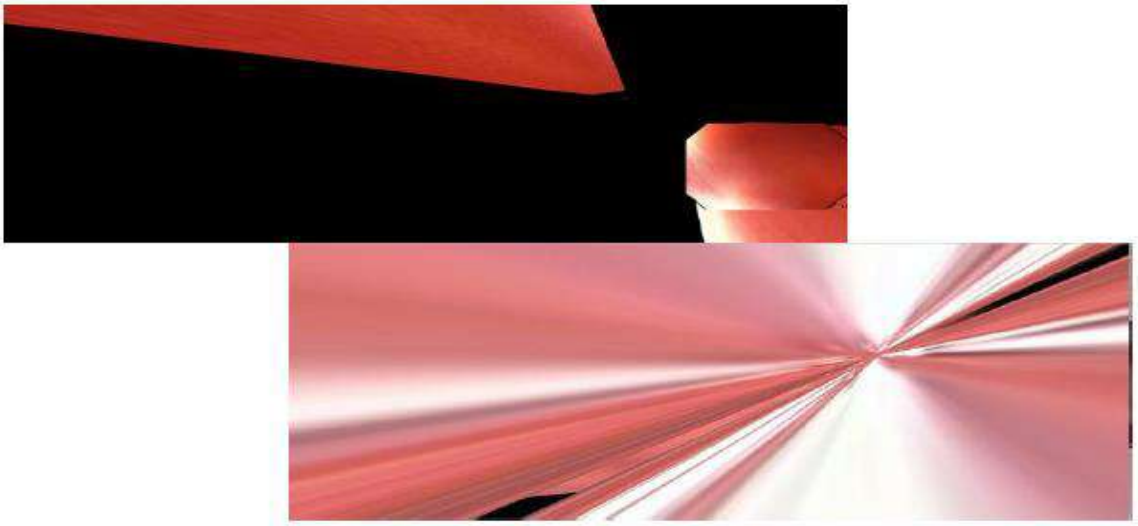


Figure 7. More examples of unsuccessful panorama creation. The two panoramas above were produced by aligning sequences that contained one or more non-informative images, which yielded singular transformations, and highly distorted image panoramas.

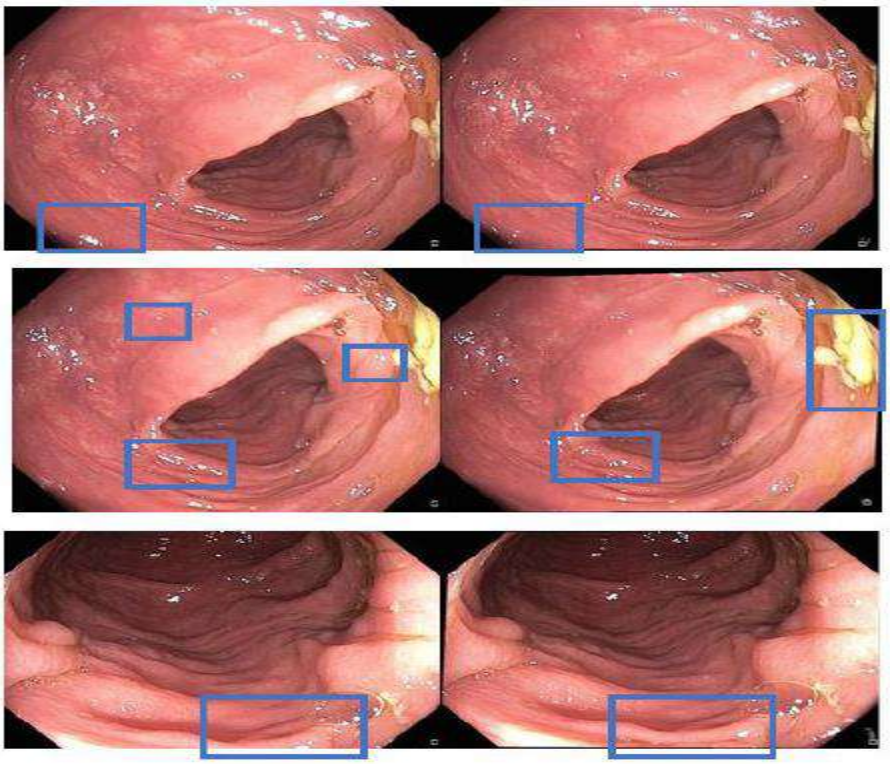


Figure 8. Three examples of panoramas that were created with image sequences that had zooming out motions. The images on the left are the original colonoscopy images, and the images on the right are the corresponding panoramas. Blue boxes indicate areas of where specular highlights have been removed and where more image detail is visible.

One benefit of our image sequence alignment is that it restores some important details in our colonoscopy images. This can be seen in figure 8 which shows some original images and enhanced versions that have been generated using our approach. Notice that some specular noise has been removed, also some image details have been added that are indicated using blue rectangles.

4. CONCLUSIONS AND FUTURE WORK

In this paper we described our method for motion compensated colonoscopy image restoration. As a first step we perform RANSAC-based image registration to align sequences of N consecutive images in the colonoscopy video. We then use this sequence to construct panorama images that improve image quality. We have demonstrated that this approach successfully removes unwanted specular highlights from colonoscopy images, and in many cases adds details that are not present in the original image.

Our experiments verify that the removal of non-informative images prior to image registration reduces the CPU time necessary for image alignment. This is because the RANSAC algorithm executes the maximum number of iterations without finding a good alignment transform for non-informative images. We also experimented with different sequence lengths and found that sequences of 11 consecutive images provided a good trade-off between CPU time and panorama quality.

For future work, we will focus on improving the quality of image alignment using different image registration techniques. In addition, we will explore methods to reduce the CPU time needed to perform this image restoration. By combining image alignment transformations from frame, A to B and from frame B to C, we should be able to get better estimates of the transformation from A to C. Since we are performing many independent image alignment operations, CPU time can also be reduced using parallel programming on a cluster or using GPUs.

REFERENCES

[1] L. Dung, C. Huang, and Y. Wu, “Implementation of RANSAC Algorithm for Feature-Based Image Registration,” Journal of Computer and Communications, pp. 46–50, 2013.

[2] F.P.M. Oliveira, J.M.R.S. Tavares. Medical Image Registration: a Review. Computer Methods in Biomechanics and Biomedical Engineering 17(2):73-93, 2014.

[3] S. B. Kang, M. Uyttendaele, S. Winder, and R. Szeliski, “High dynamic range video,” ACM Trans. Graph., vol. 23, no. 3, pp. 319–325, 2003.

[4] F. M. Candocia, “On the Featureless Registration of Differently Exposed Images,” in Proc. Int. Conf. Imaging Science, Systems & Technology, Las Vegas, NV, USA, Jun. 2003, vol. I, pp. 163–169.

[5] Hossain and B. K. Gunturk, “High Dynamic Range Imaging of Non-Static Scenes,” in Proc. SPIE Digital Photography VII, 2011, vol. vol. 7876.

[6] H. Q. Luong, B. Goossens, A. Pizurica, and W. Philips, “Joint photometric and geometric image registration in the total least square sense,” Pattern. Recognition. Lett., vol. 32, no. 15, pp. 2061–2067, 2011.

[7] D. G. Lowe, "Object recognition from local scale-invariant features," Proc. of the Int. Conf. on Computer Vision, pp. 1150–1157, 1999.

[8] B. Zitova and J. Flusser, “Image registration methods: A survey,” Image Vis. Comput., vol. 21, pp. 977–1000, 2003.

[9] S. Oldridge, G. Miller, and S. Fels, “Mapping the problem space of image registration,” in Proc. Can. Conf. Computer and Robot Vision, St. John’s, NF, Canada, May 2011, pp. 309–315.

[10] M. Tico and K. Pulli, “Robust image registration for multi-frame mobile applications,” in Proc. Asilomar Conf. Signals, Systems & Computers, Pacific Grove, CA, USA, 2010, pp. 860–864.

[11] S. Wu, Z. Li, J. Zheng, and Z. Zhu, “Exposure-robust alignment of differently exposed images,” IEEE Signal Process. Lett., vol. 21, no. 7, pp. 885–889, 2014.

[12] S. Wei and S. Lai, “Robust and efficient image alignment based on relative gradient matching,” IEEE Trans. image Process., vol. 15, no. 10, pp. 2936–43, 2006.

[13] C. Wu, B. Clipp, X. Li, J. M. Frahm, and M. Pollefeys, “3D model matching with viewpoint-invariant patches (VIP),” 26th IEEE Conf. Comput. Vis. Pattern Recognition, CVPR, pp. 1–8, 2008.

[14] P. A. Freeborough and N. C. Fox, “Modelling Brain Deformations in Alzheimer Disease by Fluid Registration of Serial 3D MR Images”, vol. 22. 1998.

[15] D. Leow, A. D. Klunder, C. R. Jack, A. W. Toga, A. M. Dale, M. A. Bernstein, P. J. Britson, J. L. Gunter, C. P. Ward, J. L. Whitwell, B. J. Borowski, A. S. Fleisher, N. C. Fox, D. Harvey, J. Kornak, N. Schuff, C. Studholme, G. E. Alexander, M. W. Weiner, and P. M. Thompson, “Longitudinal stability of MRI for mapping brain change using tensor-based morphometry,” Neuroimage, vol. 31, no. 2, pp. 627–640, 2006.

[16] K. A. Ganser, H. Dickhaus, R. Metzner, and C. R. Wirtz, “A deformable digital brain atlas system according to Talaicrach and Tournoux,” Med. Image Anal., vol. 8, no. 1, pp. 3–22, 2004.

[17] X. Huang, J. Ren, G. Guiraudon, D. Boughner and T. M. Peters, "Rapid Dynamic Image Registration of the Beating Heart for Diagnosis and Surgical Navigation," in IEEE Transactions on Medical Imaging, vol. 28, no. 11, pp. 1802-1814, Nov. 2009. doi: 10.1109/TMI.2009.2024684.

[18] N. Azawi, J. Gauch, “Automatic Method for Classification of Informative and Noninformative Images in Colonoscopy Video”, Int. Conf. on Medical Image Processing and Analysis (ICMIPA), Vancouver, Canada, August 2018.

[19] M. A. Fischler and R. C. Bolles, “Paradigm for Model,” vol. 24, no. 6, 1981.

[20] D. Wierzbicki, “Multi-Camera Imaging System for UAV Photogrammetry,” Sensors (Basel, Switzerland) vol. 18,8 2433. 26 Jul. 2018, doi:10.3390/s18082433.

[21] R. Redzuwan, N. A. M. Radzi, N. M. Din, and I. S. Mustafa, “Affine versus projective transformation for SIFT and RANSAC image matching methods,” 2015 IEEE Int. Conf. Signal Image Process. Appl., pp. 447–451, 2015.

AUTHORS

Nidhal K. Azawi finished her bachelor and master's degree in computer science / image processing at the University of Technology / department of computer science in Baghdad. She was an assistant teacher in the computer science and Engineering in the University of Al_Mustansiriya in Baghdad. She is now a PhD student researcher in computer science and engineering department in the University of Arkansas. Her research is in medical image processing. Her research interest seeks to combine machine learning with image processing and computer vision for advancements in the medical field pertaining to image enhancement, reconstruction, motion analysis, and visualization.

John M. Gauch joined the computer science and computer engineering department at the University of Arkansas as a professor in 2008. He held previous faculty positions at the University of Kansas and Northeastern University. His research interests include real-time digital video processing, content-based image and video retrieval, biomedical image enhancement, image segmentation, and motion tracking applications. This research has resulted in over sixty publications in these areas including one book and one patent.

SEA SURFACE ELECTROMAGNETIC SCATTERING CHARACTERISTICS OF JONSWAP SPECTRUM INFLUENCED BY ITS PARAMETERS

Xiaolin Mi, Xiaobing Wang, Xinyi He, Fei Dai

Science and Technology on Electromagnetic Scattering Laboratory, Shanghai, China

ABSTRACT

The JONSWAP spectrum sea surface is mainly determined by parameters such as the wind speed, the fetch length and the peak enhancement factor. In view of the study of electromagnetic scattering from JONSWAP spectrum sea surface, we need to determine the above parameters. In this paper, we use the double summation model to generate the multi-directional irregular rough JONSWAP sea surface and analyze the distribution concentration parameter and the peak enhancement factor's influence on the rough sea surface model, then using physical optics method to analysis the JONSWAP spectrum sea surface's average backward scattering coefficient change with the different distribution concentration parameters and the peak enhancement factors, the simulation results show that the peak enhancement factor influence on the ocean surface of the average backward scattering coefficient is less than 1 dB, but the distribution concentration parameter influence on the JONSWAP surface of the average backward scattering coefficient is more than 5 dB. Therefore, when we study the electromagnetic scattering of the JONSWAP spectral sea surface, the peak enhancement factor can be taken as the mean value but the distribution concentration parameter have to be determined by the wave growth state.

KEYWORDS

JONSWAP spectrum, multidirectional wave, wave pool, the peak enhancement factor, electromagnetic scattering

1. INTRODUCTION

With the in-depth study of sea clutter, the physical quantity of sea spectrum is used to describe the sea surface[1-3]. The sea spectrum is the power density spectrum of the sea surface. It is one of the most basic methods for describing the sea surface. It reflects the statistical distribution of wave energy in the wavelength and propagation direction. It is also the Fourier transform of the sea surface height fluctuation correlation function. The sea-spectrum model can be derived from the equilibrium equation of ocean wave energy, or the autocorrelation function of the sea surface height can be calculated by using fixed-point observation sea surface or laboratory wave-making pool data, and then obtained by Fourier transform. The various forms of sea- spectrum density provided in the existing literature are mostly semi-empirical, semi-theoretical results. Since the

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 257-265, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90921

1950s, many oceanographers have done a lot of observations and research on random waves, analyzed various statistical values of ocean waves from the large amount of data obtained, and then selected a function as an approximate expression of the wave spectral density. Common wave spectrums include PM (Pierson-Moscowitz) spectrum, JP (JONSWAP) spectrum, and Wen's spectrum. However, due to the different emphasis of various sea level models, the sea surface generated by different sea level simulations is very different. JONSWAP spectrum is a deep-water wind wave spectrum, which was developed by some institutes of England, Netherland, America and Germany after analyzing and fitting data collected during the "Joint North Sea Wave Observation Project" and is used extensively in the ocean wave research and engineering practice. The JONSWAP spectrum is commonly used for modeling sea surface geometry.

The JONSWAP spectrum's function is mainly determined by parameters such as wind speed, water depth, and peak enhancement factor. In this paper, we focuses on the effects of different peak enhancement factors and direction concentration parameters on the sea surface electromagnetic scattering. According to the research needs, the multi-directional JONSWAP spectral ocean model is generated by the double stacking method, and the physical optical optics (PO) is used to simulate the sea surface backscattering coefficient under different peak enhancement factors or different direction concentration parameters. Finally, the conclusions of the selection of relevant sea spectrum parameters in the study of JONSWAP sea surface electromagnetic scattering are given.

2. JON SWAP SPECTRUM

2.1. Power Spectrum

The JONSWAP spectrum function is:

$$S(\omega)=\frac{\alpha g^2}{\omega^5}\exp\left(-\frac{5}{4}\times\left(\frac{\omega_p}{\omega}\right)^4\right)\gamma^{\exp\left[-\frac{(\omega-\omega_p)^2}{2\sigma^2\omega_p^2}\right]} \quad (1)$$

Where, g is acceleration of gravity, γ is the peak enhancement factor, which is used to represent wind-wave growth state, its values are in the range of 1.5~6, typical value is 3.3, ω is the wave frequency, σ is peak shape parameter, its values are defined by:

$$\sigma=\begin{cases}0.07, & \omega\le\omega_p\\ 0.09, & \omega>\omega_p\end{cases} \quad (2)$$

α is the intensity of the spectrum that relates to the wind speed and fetch length and has the following experience formula:

$$\alpha=0.076\left(\frac{gF}{U_{10}^{\ 2}}\right)^{-0.22} \quad (3)$$

Among them, F is the wind zone, it is the distance (km) at which the wind blows at a constant Speed. $U10$ is the wind speed (m/s) at 10 m above sea level. ω_p is the peak wave-frequency,

which is the maximum value appeared in the frequency spectrum. The peak of the JONSWAP spectrum is empirically defined by:

$$\omega_p = 22(\frac{U_{10}F}{g^2})^{-0.33} \quad (4)$$

From the above analysis, the relationship between the power spectral density and the frequency of the JONSWAP spectrum at a wind speed of 5 m/s and a wind region of 40 km at different peak enhancement factors is shown in Fig. 1.

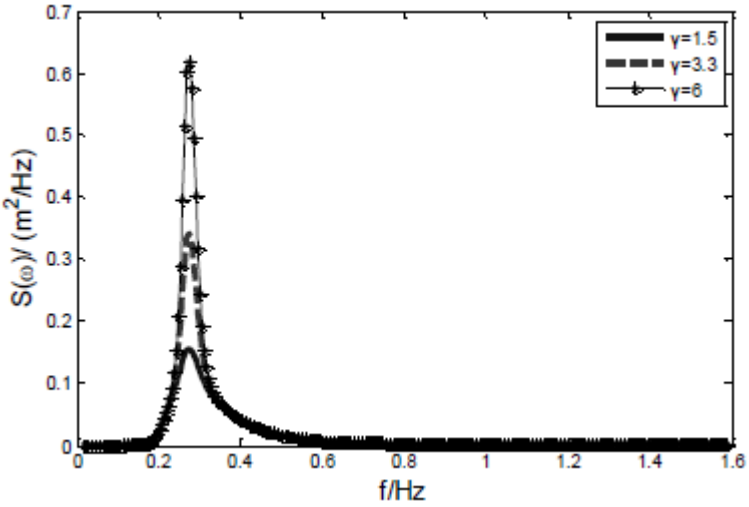


Fig.1 JONSWAP spectrum energy distribution curves with different peak enhancement factors

From Fig. 1 we can see that JONSWAP spectrum is narrow band spectrum, and its energy is mainly focused on some frequency band. The peak enhancement factor in the spectrum is used to correct the shape of the main peak, making the main peak thinner or higher. It can realistically simulate small changes in the wave model.

2.2. Direction Function

The actual sea surface waves are multi-directional irregular waves, so it is necessary to introduce a direction distribution function [4-9] to describe the energy distribution of the ocean waves with respect to the wind direction. A variety of directional distribution functions have been proposed so far, and the commonly used directional distribution function is an optically easy distribution function.

The directional spectrum is the product of the power spectrum and the direction distribution function, which can be expressed as:

$$S(f,\theta) = S(f)G(f,\theta) \quad (5)$$

Where, $S(f)$ is the frequency spectrum, $G(f,\theta)$ is called direction spreading function, the commonly used direction spreading functions are:

$$G(f,\theta) = G_0(s)\left|\cos\frac{\theta-\theta_0}{2}\right|^{2s} \tag{6}$$

Where θ_0 is the main direction of wave propagation, s is the direction distribution concentration parameter, and the coefficient G_0 is determined by equation (7):

$$G_0(s) = \frac{1}{\pi}2^{2s-1}\frac{\Gamma^2(s+1)}{\Gamma(2s+1)} \tag{7}$$

In the formula, Γ is the gamma function. When the direction concentration parameter is independent, we can give out the direction function distribution curves with different direction concentration as in Fig. 2.

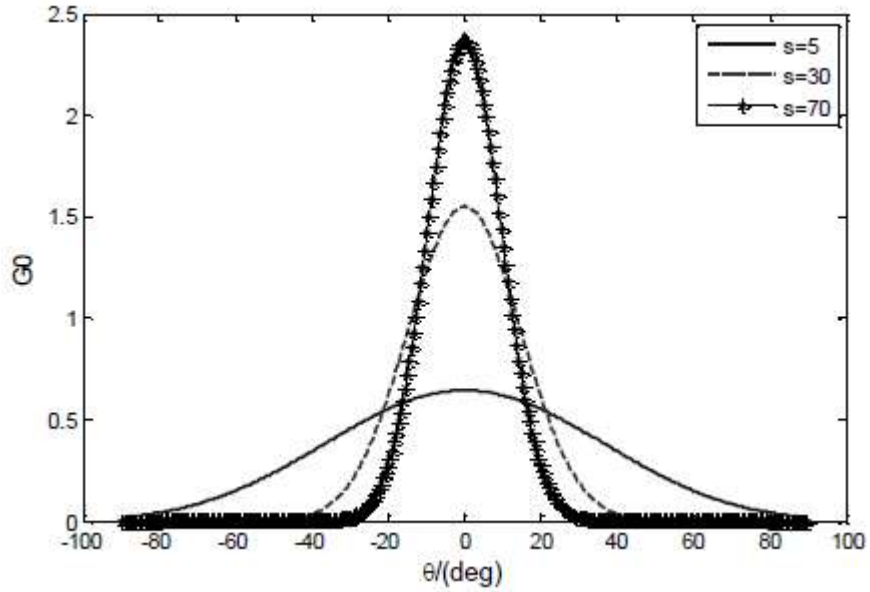


Fig2. The direction function distribution curves with different direction concentration

Figure 2 shows the distribution of the directional function with the direction distribution concentration parameters when the main propagation direction is 0°. It can be seen from the figure that the larger the direction distribution concentration parameter, the more concentrated the wave energy of the multi-directional irregular wave is in the main direction range, that is, the wave energy in the main direction is large, and the wave energy on both sides in the main direction is rapidly reduced. Generally, the wind wave's s is set to about 10, the swell with a short attenuation distance which s is set at about 25, and the swell with a long attenuation distance s is about 75 [5].

3. REALIZATION OF SIMULATING 3D OCEAN WAVES

Sea waves are of stochastic nature in the stable sea conditions and, mathematically, are represented as Gaussian stationary and ergodic processes. So sea waves can be viewed as wave superposition of infinite simple Cosine waves spreading in the direction of θ angle relatively with x axis in (x,y) plane[9], and those Cosine waves are with different amplitudes, different

frequencies and different initial phases. The sea surface elevation $\eta(x, y,t)$ can be represented by the Double Summation Model:

$$\eta(x,y,t)=\sum_{i=1}^{M}\sum_{j=1}^{N}\zeta_{ij}\cos[k_i\left(x\cos\theta_{\mathrm{dj}}+y\sin\theta_{\mathrm{dj}}\right)-\omega_{\mathrm{di}}t+\beta_{ij}] \qquad (8)$$

Where k_i is the wave number ($k_i=\omega_{\mathrm{di}}^2/g$), θ_{dj} is spreading directional angle of a single wave ($0<\theta_{\mathrm{dj}}\le 2\pi$) , ω_{di} is representative frequency in the range of frequency division, β_{ij} is initial phase angle distributed at random($0\le\theta_{\mathrm{dj}}<2\pi$). ξ_{ij} is the wave amplitude of frequency i and directional angle j, which can be represented by:

$$\zeta_{ij}=\sqrt{2S\left(\omega_i,\theta_j\right)\mathrm{d}\omega\mathrm{d}\theta}. \qquad (9)$$

Equation (8) is the generation principle of multi-directional irregular ocean waves. According to the sea spectrum to be described, the corresponding parameters in the equation are discretized, and the wave height distribution data of the multi-directional irregular sea surface can be obtained through computer simulation.

According to the above analysis, a multi-directional irregular sea surface of a peak enhancement factor is 3.3, a wind speed is 5 m/s at 10 meters above the sea surface, a direction concentration parameter is 75 and a fetch length is 10 km is established. The result is shown in Fig. 3.

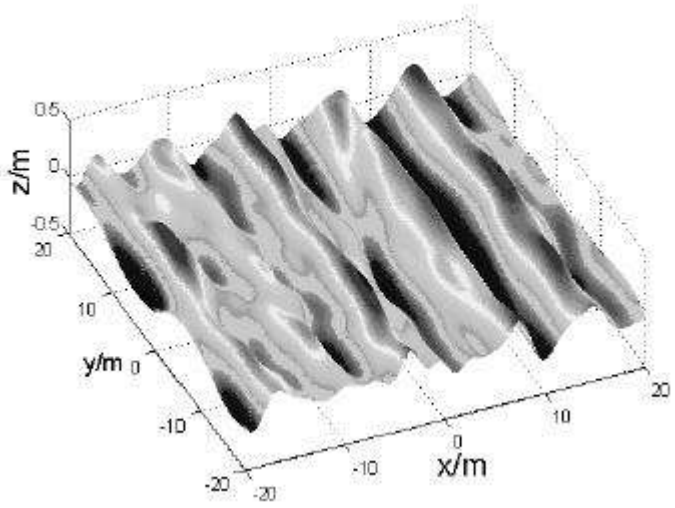


Fig3. The three-dimensional JONSWAP sea surface simulation model

4. PHYSICAL OPTICS

The PO method is an approximation method for solving the Helmholtz integral equation. It is widely used in solving electromagnetic scattering problems [10-14]. The basic idea is that when

the wavelength of the incident wave and the radius of curvature of the rough surface are satisfied, the rough surface can be regarded as many small triangular facets are spliced together, and the electromagnetic waves are diffracted at the edges and sharp points of the rough surface, and the multiple scattering between the bins can be neglected. The area where the incident wave cannot be directly irradiated is a dark area, and the area where the incident wave can directly illuminate is a bright area, and each bright area scattering field is calculated, and the total scattered field is obtained after superposition. Rough surface element electromagnetic flow is:

$$\begin{cases} \mathbf{J} = \mathbf{n} \times \mathbf{H}^{\mathrm{i}} = \dfrac{1}{\eta_0}\{-(\hat{\mathbf{e}}_{\mathrm{i}} \bullet \mathbf{h})(\mathbf{n} \bullet \mathbf{k}_{\mathrm{i}})(1 - R_{\mathrm{H}})\mathbf{h} + (\hat{\mathbf{e}}_{\mathrm{i}} \bullet \mathbf{v})(\mathbf{n} \bullet \mathbf{h})(1 + R_{\mathrm{V}})\} E_0 p(x,y) e^{-\mathrm{j}k\mathbf{k}_{\mathrm{i}} \bullet \mathbf{r}}, \\ \mathbf{M} = \mathbf{E}^{\mathrm{i}} \times \mathbf{n} = -\{(\hat{\mathbf{e}}_{\mathrm{i}} \bullet \mathbf{h})(\mathbf{n} \bullet \mathbf{h})(1 + R_{\mathrm{H}})\mathbf{h} + (\hat{\mathbf{e}}_{\mathrm{i}} \bullet \mathbf{v})(\mathbf{n} \bullet \mathbf{k}_i)(1 - R_{\mathrm{V}})\} E_0 p(x,y) e^{-\mathrm{j}k\mathbf{k}_{\mathrm{i}} \bullet \mathbf{r}} \end{cases} \tag{10}$$

Where, R_H , R_V is the local polarization reflection coefficient, respectively:

$$\begin{cases} R_{\mathrm{H}} = \dfrac{\sin\phi - \sqrt{\varepsilon_c - \cos^2\phi}}{\sin\phi + \sqrt{\varepsilon_c - \cos^2\phi}} \\ R_{\mathrm{V}} = \dfrac{\varepsilon_c \sin\phi - \sqrt{\varepsilon_c - \cos^2\phi}}{\varepsilon_c \sin\phi + \sqrt{\varepsilon_c - \cos^2\phi}} \end{cases} \tag{11}$$

Where ϕ is the incident angle, which is the complex permittivity, and its calculation formula is ：

$$\varepsilon_c = \varepsilon_r - \mathrm{j}60\lambda\sigma_e \tag{12}$$

Where ε_r is the relative dielectric constant; σ_e is the conductivity of the surface material, the unit is Siemens meters (S / m).

This gives the scattering field:

$$\begin{cases} \mathbf{E}^s(\mathbf{r}) = -\mathrm{j}\dfrac{\omega\mu_0}{4\pi r} e^{-\mathrm{j}kr} \bullet \displaystyle\int_S \left\{\mathbf{J}(\mathbf{r}') - \left[\mathbf{J}(\mathbf{r}') \bullet \mathbf{k}_s\right]\mathbf{k}_s + \sqrt{\frac{\varepsilon_0}{\mu_0}}[\mathbf{M}(\mathbf{r}') \times \mathbf{k}_s]\right\} e^{\mathrm{j}k\mathbf{r}' \bullet \mathbf{k}_s} ds', \\ \mathbf{H}^s(\mathbf{r}) = -\mathrm{j}\dfrac{\omega\mu_0}{4\pi r} e^{-\mathrm{j}kr} \bullet \displaystyle\int_S \left\{\mathbf{M}(\mathbf{r}') - \left[\mathbf{M}(\mathbf{r}') \bullet \mathbf{k}_s\right]\mathbf{k}_s + \sqrt{\frac{\varepsilon_0}{\mu_0}}[\mathbf{J}(\mathbf{r}') \times \mathbf{k}_s]\right\} e^{\mathrm{j}k\mathbf{r}' \bullet \mathbf{k}_s} ds' \end{cases} \tag{13}$$

5. RESULTS AND COMPARISON

According to the mathematical model analysis of the first part of JONSWAP spectrum, When the wind speed and wind fetch length are determined, the JONSWAP sea surface is affected by the peak enhancement factor and the direction concentration parameter. The peak enhancement factor mainly represents the power spectrum of the spectral function at the peak frequency, on the

geometric model, it shows the sharpness of the waves at the peaks and troughs. The direction concentration parameter mainly represents the concentration of the multi-directional irregular sea surface in the main propagation direction, and the selection of the direction concentration parameter is related to the growth state of the wave. Therefore, in this section, the scattering characteristics of multi-directional irregular ocean waves under different peak enhancement factor and directional concentration parameters are calculated, and their effects on scattering characteristics are analyzed. Thus a method for determining the selection of relevant ocean wave parameters in the simulation or wave-making test of JONSWAP spectrum sea surface when study the electromagnetic scattering is given. During simulation, the dielectric constant of seawater is given according to the double Debye model [14].

5.1 Influence of Peak Enhancement Factors on Electromagnetic Scattering Characteristics

When the wind fetch length is 10 km and the wind speed is 5 m/s, the JONSWAP spectral dynamic sea surface with peak enhancement factors of 1.5 and 6 is generated respectively. The incident electromagnetic wave frequency is 1 GHz, upwind observation, and the sea surface size is 16m ∗ 16m, and the triangle facet size is smaller than 0.01m. Under the above conditions, We calculated the backscattering coefficient of the sea surface at the incident angle between 0°~70° by PO. The dynamic sea surface is sampled 40 times at each angle, and the sampling time is 1s, and the results are the forty average results. When the direction concentration s is 70, the curve of the backscattering coefficient under different spectral peak enhancement factors with the incident angle is shown in Fig. 4.

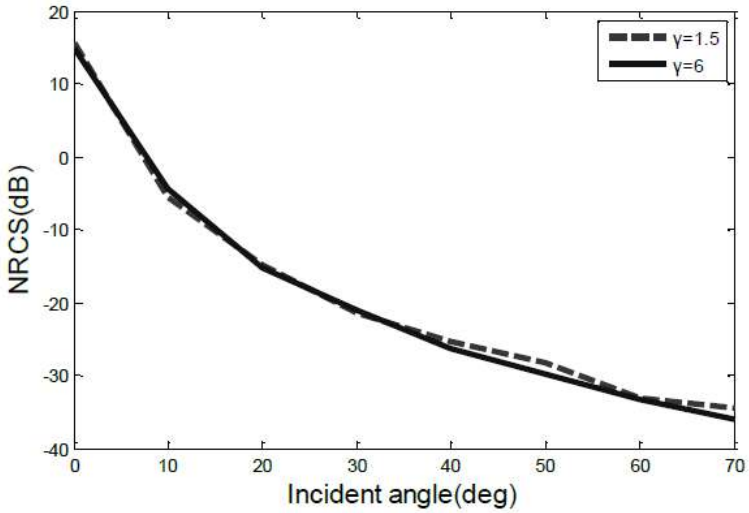


Fig4. The simulation results of normalization radar cross section (NRCS) under different spectral peak enhancement factor

It can be seen from the figure that the maximum difference of the backscattering coefficient of the multi-directional irregular JONSWAP wave at different incident angles is less than 1 dB under different spectral peak enhancement factors. Therefore, the peak enhancement factor has little effect on the average scattering coefficient of the ocean wave.

5.2 Influence of Direction Concentration Parameters on Electromagnetic Scattering Characteristics

When the peak enhancement factor is the average value of 3.3, the other parameters are the same as those described in Section A. The relationship between the backscattering coefficient and the incident angle under different concentration parameters is simulated as shown in Fig. 5.

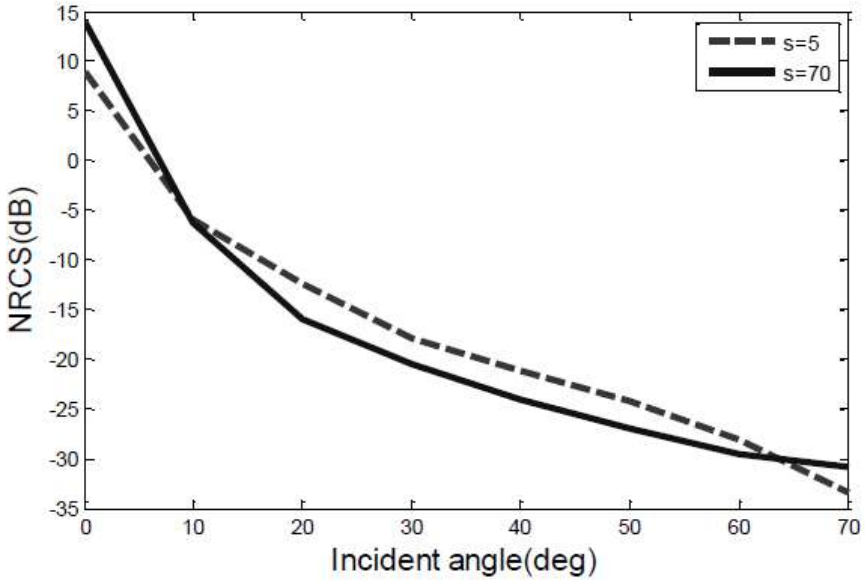


Fig5. The simulation results of normalization radar cross section (NRCS) under different direction concentration

According to the figure, the maximum difference of the scattering coefficients under different s parameters exceeds 5dB. From the geometric model of the sea surface, the larger s is, the more concentrated the wave is in the main propagation direction. Therefore, the backscattering coefficient of the sea surface is concentrated at the low incident angle to the wind, therefore the result is larger. But as the angle of incidence increases, the back scattering coefficient is smaller than the sea scattering coefficient of the lower s parameter of the coarser distribution.

6. CONCLUSIONS

In this paper, a Double Summation Model is used to combine the power spectrum and the direction distribution function of JONSWAP spectrum to establish a multi-directional irregular rough sea surface, and the physical optics method is used to simulate the sea surface electromagnetic scattering coefficient. And then give out the conclusions that when the JONSWAP spectrum sea surface is simulated or simulated in the wave pool, the peak enhancement factor parameters have little effect on the electromagnetic scattering characteristics, which can be taken as the average value, but the direction concentration parameter has a great influence on the sea surface electromagnetic scattering, thus its value needs to be determined according to the growth state of the sea surface.

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China (Grant No.61471242). The authors would like to thank the reviewers for their constructive suggestions.

REFERENCES

[1] Hasselmann K,Barnett T P, Bouws E,et al. Measurements of wind-wave growth and swell decay during the Joint North Sea Wave Projects (JONSWAP) [J]. Ergnzungsheft zur Deutschen Hydrographischen Zeitschrift Reihe A8(Suppl.),1973,12:95.

[2] Estimation of JONSWAP Spectral Parameters by Using Measured Wave Data[J].China Ocean Engineering,1995(03):275-282.

[3] Annalisa Calini,Constance M. Schober. Characterizing JONSWAP rogue waves and their statistics via inverse spectral data[J]. Wave Motion,2016.

[4] YU Yu-xiu, LIU Shu-xue.Random Wave and Its Applications to Engineering[M],Dalian:Dalian University of Technology Press,2016.

[5] ZHAO Ke, LI Mao-hua, ZHENG JIAN-li, TIAN Guan-nan. 3-D simulation of random ocean wave based on spectrum of ocean wave[J]. Ship Science and Technology,2014,36(02):37-39.

[6] Mitsuyasu H, et al. Observation of the directional wave spectra of ocean waves using a cloverleaf buoy.[J].Physical Oceanography,1975,5:750-760.

[7] Si Liu,Shu-xue Liu,Jin-xuan Li,Zhong-bin Sun. Physical simulation of multidirectional irregular wave groups[J]. China Ocean Engineering,2012,26(3)

[8] Hong Sik Lee,Sung Duk Kim. A three-dimensional numerical modeling of multidirectional random wave diffraction by rectangular submarine pits[J]. KSCE Journal of Civil Engineering,2004,8(4).

[9] MI Xiao-lin, WANG Xiao-bing, HE Xin-yi, XUE Zheng-guo. Simulation and Measurement Technology of 3-D Sea surface in Laboratory Based on Double Summation Model[J].GUIDANCE&FUZE,2016,37(02):19-23.

[10] WEI Ying-yi, WU Zhen-sen, LU Yue. Electromagnetic scattering simulation of Kelvin wake in rough sea surface[J],CHINESE JOURNAL OF RADIO SCIENCE.,2016,(3)：438-442.

[11] Biglary, H.,Dehmollaian, M.. RCS of a target above a random rough surface with impedance boundaries using GO and PO methods[P]. Antennas and Propagation Society International Symposium (APSURSI), 2012 IEEE,2012.

[12] Joon--Tae Hwang. Radar Cross Section Analysis Using Physical Optics and Its Applications to Marine Targets[A]. Scientific Research Publishing.Proceedings of 2015 Workshop 2[C].Scientific Research Publishing,2015:6.

[13] YANG Peng-ju, WU Rui, ZHAO Ye, REN Xin-cheng. Doppler spectrum of low-flying small target above time-varying sea surface[J]. Journal of Terahertz Science and Electronic Information Technology,2018,16(04):614-618.

[14] MEISSNER T. WENTZ F J. The complex dielectric constant of pure and sea water from microwave satellite observations[J]. IEEE Transactions on Geoscience and Remote Sensing, 2004,42(9)：1836-1849.

AUTHORS

Xiaolin Mi (1993-), male, Chinese, engineer, mainly engaged in radar signal processing research.

INTENTIONAL BLANK

THREE-DIMENSIONAL RECONSTRUCTION USING THE DEPTH MAP

[1]A.El abderrahmani , [2]R.Lasri and [3]K.Satori

[1,2]Advance Technology Lab, Department of Computer Sciences, Larache Poly Disciplinary School, Abdelmalek EssaâdiUniversity
[3]LIIAN, Department of Mathematic & Computer Sciences Dhar-Mahraz Sciences School, FEZ, MOROCCO

ABSTRACT

This paper presents an approach to reconstructing 3D objects based on the generation of dense depth map. From a two 2D images (a pair of images) of the same 3D object, taken from different points of view, a new grayscale image is estimated. It is an intermediate image between a purely 2D image and a 3D image where each pixel of this image represents a z-height according to its gray level value. Our objective therefore is to play on the precision of this map in order to prove the interest and effectiveness of this map on the quality of the reconstruction.

KEYWORDS

Dense reconstruction; depth map; disparity map; camera parameters.

1. INTRODUCTION

Obtaining 3D models of very high quality and more accurate is the main concern of researchers of 3D reconstruction domain. This is why several methods are proposed in the literature [1, 2, 3]. Most of these methods rely on a classical reconstruction process that provides us with only a scattered set of 3D points. This does not give us enough information about the scene. Hence, the interest of enriching this 3D structure by other information contained in the depth map what is the subject of this paper where we present the different steps to estimate a dense depth map. However, the quality of the depth map and the performance of the process of creating this map are our main objective in this paper.

Our work is structured around four sections. In the second section, we present a synthesis of existing approaches in the literature concerned with the estimation of the depth map. Then, we describe in the third section the different steps to build the depth map. The experiments and interpretation are the subject of the fourth section. Finally, the fifth section provides a conclusion to this work.

2. RELATED WORK

The depth information is a key and essential element in several fields of research such as video processing [4], visual communication [5, 6], computer vision [7, 8], and many others areas. Its importance encouraged researchers to work on the accuracy of this information by presenting the latter in the form of a map, called depth map, where the value of each pixel of this map corresponds to its depth.

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 267-274, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90922

In all these researches interested in the depth map, we find in the literature two categories of the researchers, the first category is interested in the exploitation of the depth map [9, 10, 11] and the second is interested only to the improvement of the quality of this map [12, 13, 15, 16],so that other researchers use it in their research.

Among the researches that used the depth map are the one based on image-based rendering (IBR) techniques [9]: in this work, Kim et al. found that they needed accurate depth information in order to generate reliable and accurate multiview intermediate images for use in a multiview 3D display system. It is for this reason that they decided to exploit the depth map. In their article, they carried out an experiment to estimate the depth map quantization for multiview intermediate image generation using depth image-based rendering (DIBR). This DIBR synthesizes several virtual views of a 3D scene from a 2D image and its associated depth map.

Using the vanishing point, Kim et al. [10] proposed a new 3D panorama system based on the generation of the depth map to restore a 3D space structure from the 2D images. The points of intersection of the vanishing lines detected indicate the vanishing points.

In order to describe the human actions Li et al. [11] also exploited the depth map, they presented a real- time human action recognition system that uses the depth map sequence as input. The proposed algorithm uses only depth information for applications where environmental illumination is weak or changing. This algorithm is based on depth continuity, which is the most essential attribute of objects in depth maps.

For the second category, several efforts have been made in recent years to estimate the depth map whose main objective is to improve the quality of this map. As an example, Pascal Fua [12] proposed a correlation algorithm that reliably produces much denser depth maps with little false correspondence and in the presence of depth discontinuities and occlusions. This algorithm aims to match each point of the image and uses a consistency criterion to reject invalid matches. This criterion is designed so that when the correlation fails, instead of producing an incorrect response, the algorithm does not return a response. Subsequently, in order to calculate dense depth maps, the author proceeds to combine the depth map produced by correlation and the gray level information present in the image itself to introduce depth discontinuities and to adjust a surface, which is smooth in pieces.

With the same objective, Zhang et al. [13] have developed a new system for the estimation of high quality and high resolution depth maps by the common fusion of stereo data and Kinect depth sensor [14]. The fusion problem is formulated as a maximum a posteriori probability (MAP) estimation problem and the MAP problem is solved using a multi scale belief propagation (BP) algorithm.

Similarly, Malik and Choi [15] presented a new focus measure for the estimation of the depth map using image focus. This depth map can then be used in techniques and algorithms leading to the recovery of a 3D structure of the object. This new measurement aims to determine the best number of frames for each pixel, that is to say the frame where the pixel is best focused. In other words, only the frame corresponding to the best focusing value is selected for each pixel, and all the other frames in which the pixel is less focused are ignored.

For a successful 2D-3D conversion, depth information is required. Then, for this reason Yang et al. [16] proposed an interactive method of depth map generation from a single image for 2D-3D conversion using a local depth hypothesis. The use of a depth variation hypothesis can reduce human effort to generate a depth map. The only thing required from a user is to mark some salient

areas to be distinguished with respect to depth variation. The proposed algorithm assumes hypothesis of each salient area and generates a depth map of an input image.

3. STEPS FOR DEPTH MAP ESTIMATION

In order to generate the depth map, the disparity map is first calculated. Given a pair of stereoscopic images, it is possible to calculate a dense disparity map, which encodes the correspondences per pixel between two views of the same scene. Given the calibration parameters of a pair of cameras, it is possible to transform a disparity map into a depth map.
The steps for estimating the depth map is as in Fig. 1.

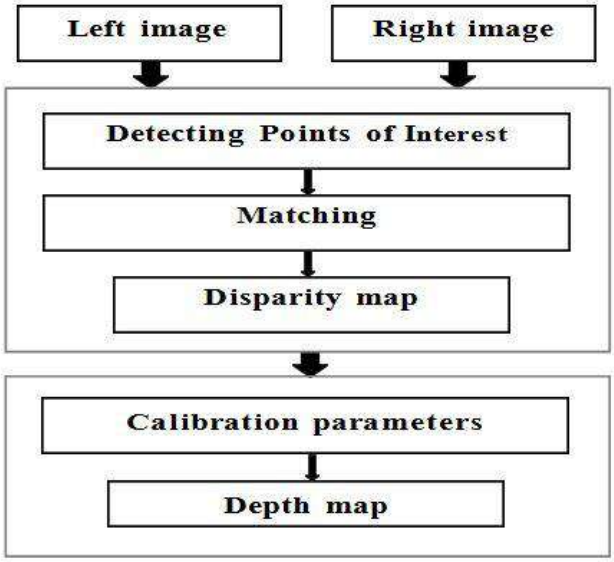


Fig. 1 Steps for estimating the depth map

3.1 Calculation of the Disparity Map

A disparity map is a collection of distances of correspondence between the homologous visual indices of two images studied. We call visual index any object extracted from the image and containing in a compact way the information relevant to its analysis [17]. These indices may be points of interest, regions or contours. The points are mainly present, specific and numerous which give them more advantages over the contours and regions. In this work, we will use the primitive point.

To generate this map several steps to follow:

3.1.1 Detecting Points Of Interest

This step involves extracting points of interest: Points of interest are defined as points that have characteristics that distinguish them from other points in the image. To detect these points, a point of interest detector is used. This detector consists of calculating a response value, representing the interest for each pixel of the image and then selecting the best ones. In this work, we will use the Harris detector [18], which has given better results according to this comparative study of the detectors of points of interest [19].

Fig. 2 The points of interest of the left image

Fig. 3 The points of interest of the right image

3.1.2 MATCHING

This phase consists in finding, on two images of the same scene taken from different positions, the two points corresponding to the projection of the same element of the scene. In recent years, many matching methods have been proposed [20, 21, 22, 23].

In this work we will compute the pairings of each image (left / right) using a mapping method based on the correlation measure. In this case, it is assumed that the points neighboring two homologous points have gray levels that are similar. This resemblance can be quantified by a correlation measure. Thus, only the neighborhood of a point is used to find its correspondent.

The correlation between stereoscopic images consists, from a window placed in one of the images, in calculating the degree of correlation with another window moving along the corresponding epipolar line in the other image. A sequence of correlation values along the epipolar line is thus obtained. The point corresponding to the best score will be chosen as being to match the point of the center of the fixed window in the other image.

Several families of correlation measures can be distinguished in the literature [21]. In our work, the correlation measure between the points of the images is carried out by the centered and normalized correlation function ZNC (Zero mean Normalized Cross Correlation), it is a centered version of the NCC family, which obtained the best percentages d 'Matching according to the evaluation carried out in [21].

The function ZNCC for each point (u, v) is written:

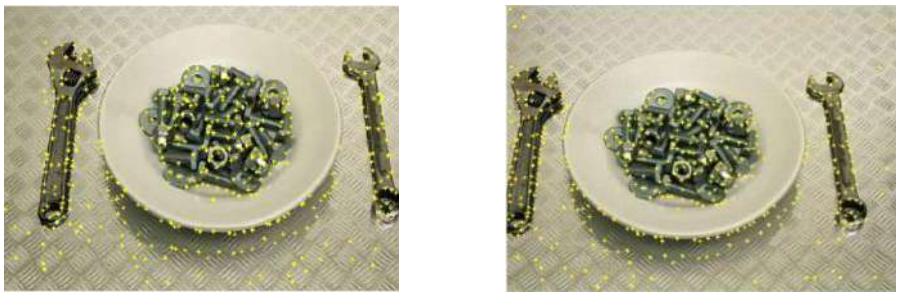
$$ZNCC\ (u,v)\ \frac{\sum_{x,y}(I1(x,y)-\overline{I1u,v})(I2(x-u,y-v)-\overline{I2})}{\sqrt{\sum_{x,y}(I1(x,y)-\overline{I1u,v})^2\ \sum_{x,y}(I2(x-u,y-v)-\overline{I2})^2}} \quad (1)$$

With

$$I1u,v=\blacksquare 1\ MxMy\ \Sigma\ \Sigma\ I1(x,\ y)\ v+My-1\ y=v\ u+Mx-1\ x=u \quad (2)$$

And

$$I2\bar{}1\ NxNy\ \Sigma\ I2(x,\ y)\ Ny-1\ y=0$$



(a) (b)

Fig. 4: Corresponding points between the couple of images (a) and (b)

3.2 DISPARITY MAP

After the matching step, it is possible to calculate the disparity map. For each point of the left image (right resp). The position difference is calculated with the corresponding point of the right image (left resp) on the same line. These differences are then transformed for each point into a gray level image.

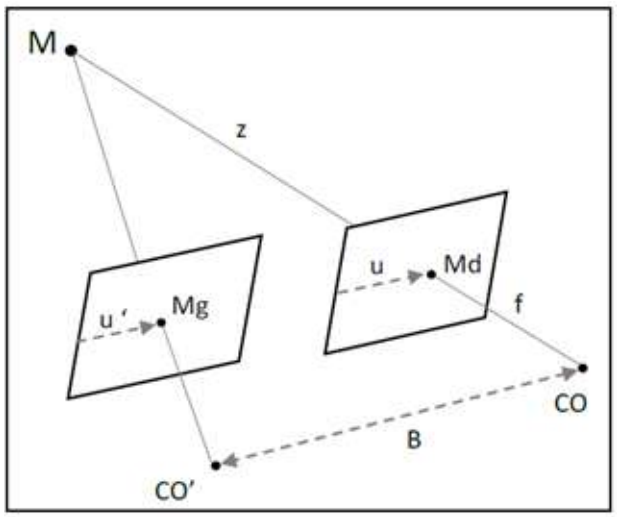


Fig. 5 Pinhole model for the projection of the point M

In this figure the measured disparity, defined as:

$$d = u - u'$$

With u and u' the horizontal position of the two image points Mg and Md corresponding to the projection of the point 3D in the two images.

The disparity map is closely related with the depth map. We can create a depth map from a disparity map if we knows the camera focal length and the distance between the cameras.

The distance Z from the 3D point to the camera is inversely proportional to the disparity measured on the image as in Fig. 5:

$$Z = {}^{(fB)}/_{d} \quad (4)$$

With:
B: distance between the cameras
f: focal length
d:disparity.
To find these unknown, once the parameters of the camera are estimated then it is easy to deduce the value Z of depth.

4. EXPERIMENTATIONS

To estimate the depth map, an object-oriented programming language (Java) implemented the steps of estimating this map

In the first interface as in Fig. 6, our process allows loading the left and right image and then displaying the points of interest for each image, thereafter displaying the matching points. In addition, it can generates a file of the matching points. Then the process provide the possibility of calculate disparity map and depth map as in Fig. 7.

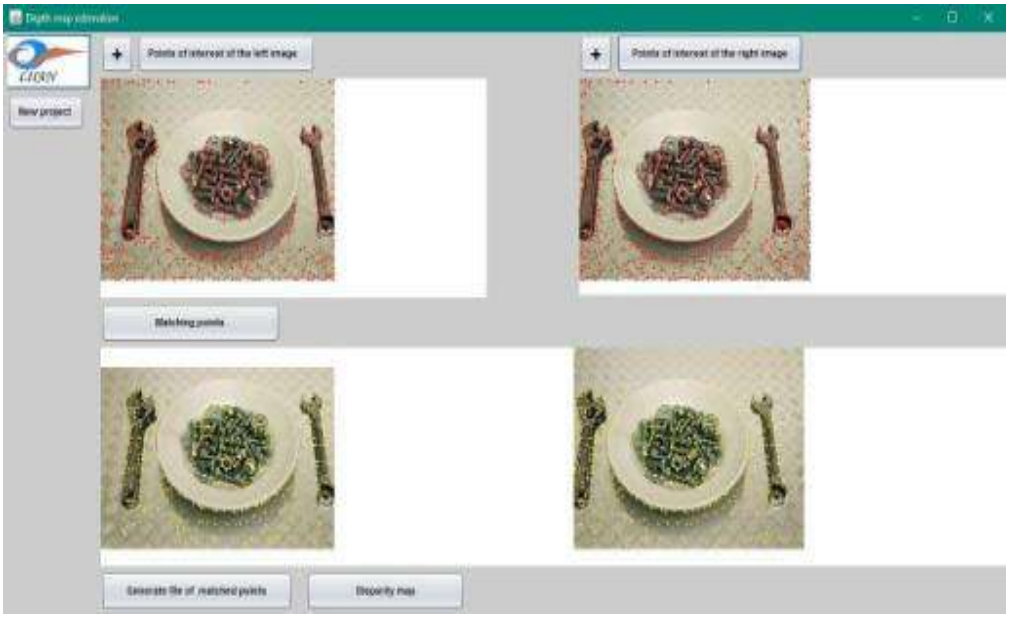
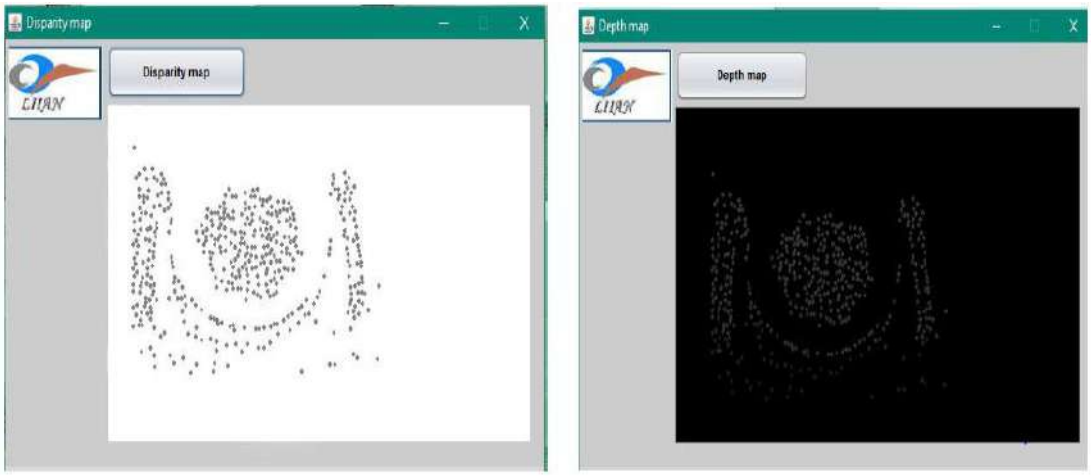


Fig. 6 The first interface of a program for estimating depth map



(a) (b)

Fig. 7 Disparity map (a) and Depth map (b)

Our program is being improved, in order to generate a more precise depth map to use it later in the 3D reconstruction.

5. INTERPRETATION

The results obtained in Figures 6 and 7, shows the satisfaction of our depth map estimation method. In addition this result would be used later to improve the 3D reconstruction

6. CONCLUSION

In this article, we have presented the different steps to estimate a dense depth map for the reason that the generation of this map is a very important step in improving the quality of 3D reconstruction. Our goal later is to get other information more than depth from this map before proceeding to the reconstruction step.

REFERENCES

[1] El Hazzat, S., Saaidi, A., & Satori, K. Euclidean 3d reconstruction of unknown objects from multiple images. Journal of Emerging Technologies in Web Intelligence, 6(1), 59–63, 2014.
[2] M.A.Ameller, A.Bartoli et L.Quan. Reconstruction métrique minimale à partir de trois caméras affines In 13ème Congrès Francophone AFRIF-AFIA de Reconnaissance des Formes et Intelligence Artificielle, Volume 2, p : 471-477, January 2002.
[3] M.HanetT.Kanade. Multiple motion scene reconstruction from uncalibrated views.In Proc of the 8th International Conference on computer Vision, Vancouver, Canada, July 2001.
[4] A. Fernando, S.T. Worrall, et al., 3DTV: Processing and Transmission of 3D Video Signals, John Wiley & Sons, 2013.
[5] R. Ji, Y.Gao, R.Hong, Q.Liu, D.Tao, X.Li, Spectral-spatial constraint hyperspectral image classification, IEEE Trans.Geosci. Remote Sens. 52(3) (2013) 1811–1824.
[6] Y.Liu, S.Ci, H.Tang, Y.Ye, Application adapted mobile 3d video coding and streaming a-survey, 3DR Rev. 3 (1) (2012) 1–6.
[7] S. Chaudhuri, V. Koltun, Data-driven suggestions for creativity support in 3d modeling, in: ACM Transactions on Graphics (TOG), vol. 29, ACM, 2010, p. 183.
[8] Y.Gao, Q.Dai, N.Y.Zhang, 3d model comparison using spatial structure circular descriptor, Pattern Recognit. 43 (3) (2010) 1142–1151.

[9] Jong Chan kim et Oh Hoon Cho. Effects of Depth Map Quantization for Computer-Generated Multiview Images using Depth Image-Based Rendering. KSII Transactions on Internet and Information Systems vol. 5, no. 11, November 2011.
[10] Jong Chan kim et Oh Hoon Cho. A study on 3D Panorama System using depth map Generation techniques. International Journal of Multimedia and Ubiquitous Engineering. Vol 11, pp 117-128, 2016.
[11] Y. L. Li, G. J. Wang, X. G. Lin, G. Cheng, L. He, "Real-Time Human Action Recognition System Using Depth Map Sequences", Advanced Materials Research, Vols. 760-762, pp. 1647-1651, 2013.
[12] Pascal Fua. A parallel stereo algorithm that produces dense depth maps and preserves image features. Machine Vision and Applications. 1993
[13] S. Zhang, C. Wang, S. C. Chan. A New High Resolution Depth Map Estimation System Using Stereo Vision and Kinect Depth Sensing, 2013.
[14] Smisek, J., Jancosek, M., Pajdla, 3D with kinect. IEEE Workshop Consum. Depth Cameras Comput. Vision pp. 1154–1160. 2011
[15] Aamir Saeed Malik, Tae-Sun Choi. A novel algorithm for estimation of depth map using image focus for 3D shape recovery in the presence of noise. Pattern Recognition 41(7) : 2200-2225 · July 2008.
[16] Na-Eun Yang, Ji Won Lee, and Rae-Hong Park. Depth map generation using local depth hypothesis for 2D-to-3D conversion. International Journal of Computer Graphics & Animation (IJCGA) Vol.3, No.1, January 2013
[17] A. Lux. Algorithme et contrôle en vision par ordinateur. These de doctoral, INPG Grenoble, 1985.
[18] C.Harris et M.Stephens. A combined Corner et Edge Detector. 4th Alvey vision Conference. pp. 147-151, 1988.
[19] N.Elakkad, A.Baataoui, A.El abderrahmani, A.Saaidi et K.Satori. « Etude Comparative des détecteurs des points d'intérêt »WCCCS 11, 2011.
[20] Daniel Scharstein et Richard Szeliski. A taxonomy and evaluation of dense two-frame stereo correspondence algorithms. Int. J. Comput. Vision, 47 :7–42,April 2002.
[21] S.Chambon and A. Crouzil. Similarity measures for image matching despite occlusions in stereo vision. Pattern Recognition. Vol. 44, No. 9, pp. 2063-2075, 2011.
[22] S. T. Barnard. Stochastic Stereo Matching over Scale. International Journal of Computer Vision. Vol. 3, No. 1, pp. 17-32, 1989.
[23] J. Shao. Generation of Temporally Consistent Multiple Virtual Camera Views from Stereoscopic Image Sequences. International Journal of Computer Vision. Vol. 47, No. 2, pp. 171-180, 2002.

DATA AUGMENTATION BASED ON PIXEL-LEVEL IMAGE BLEND AND DOMAIN ADAPTATION

Di LIU[1],Xiao-Chun HOU[2],Yan-Bo LIU[3] , Lei Liu[4] , Yan-Cheng Wang[5]

[12345]School of Information and Software Engineering, University of Electronic Science and Technology of China, ChengDu,China

ABSTRACT

Object detection typically requires a large amount of data to ensure detection accuracy. However, it is often impossible to ensure sufficient data in practice. This paper presents a new data augmentation method based on pixel-level image blend and domain adaptation. This method consists of two steps: 1.Image blend using a labeled dataset as object instances and an unlabeled dataset as background images.2. Domain adaptation based on Cycle Generative Adversarial Networks (Cycle GAN).A neural network will be trained to transform samples from step 1 to approximate the original dataset. Statistical consistency between new dataset generated by different data augmentation methods and original dataset will be measured by metrics such as generator loss and hellinger distance. Furthermore, a detection/segmentation network for diabetic retinopathy based on Mask R-CNN will be built and trained by the generated dataset. The effect of data augmentation method on the detection accuracy will be presented.

KEYWORDS

Data Augmentation, Object Detection, Image Blend, Domain Adaptation, Diabetic Retinopathy

1. INTRODUCTION

In the task of object detection, data augmentation of training samples is of great significance, which can reduce over-fitting and improve the generalization performance of the detection models. Traditional data augmentation methods, such as cropping, flipping, and colour jittering, are able to obtain a certain degree of detection accuracy. However, object detection needs to not only recognize different kinds of instances but also distinguish the same instance in different contexts. Therefore, using image blend to expand context information is an effective data augmentation method [1].Image blend is to cut and paste object instances into other background images to obtain new samples which contains object instances. Nevertheless, if object instances are blended randomly with background images, it's possible to generate unreasonable image contexts, which can even degrading the detection accuracy [2], [3]. Related work presents a method of training a deep learning network to predict whether the background image is suitable for image blend with the object instances [4].But when it comes to the object detection of medical images, which has less information, it only needs to judge whether the scale and location of an instances are correct or not.

Samples generated by image blend often have different styles from original object instances. Domain adaptation is a effective method to transform blended image to be close to the original

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 275-285, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90923

object instances, so as to improve the quality of generated samples. Generative Adversarial Networks (GAN) is a common domain adaptation method recently [5], 6]. On the basis of GAN, a cyclic network called Cycle GAN which is composed of two mirror GAN was presented [8].Cycle GAN is able to transform and reconstruct samples cyclically between source domain and target domain, thus improving the consistency between the real samples and generated samples [9].This paper presents a new data augmentation method combined pixel-level image blend and domain adaptation. And a object detection model of diabetic retinopathy will be established to verify the validity and applicability of this method.

2. PARTIAL ALGORITHM PRINCIPLE

2.1 Object Detection Algorithm

Object detection is an important branch of computer vision field. Which is mainly used to locate and recognize object instances with specific features in the image. Traditional methods, such as SIFT [10], SURF [11], DPM [12], mainly devoted to extract local features and match these features to retrieve instances. Few instance samples are needed when using traditional methods. But at the same time, local features extracted by these methods are not 'rich' enough to obtain better detection accuracy. The recent object detection algorithm are based on convolutional neural network (CNN)[13] andregion proposal algorithm to obtain better detection accuracy [14], [15], [16].Mask R-CNN is a representative of such algorithms. It presents a new structure based on feature pyramid network (FPN) [17] and micro Fully Convolutional Networks (FCN) [18]for each region of interest (RoI). Mask R-CNN [19] has excellent detection accuracy and can segment the object instances at the pixel level at the same time. But these algorithms based on CNN require a large amount of labeled dataset to train the detection model. Otherwise, Problems such as over-fitting, low detection accuracy will comes to these algorithms. In conclusion, it is necessary to search a suitable data augmentation method to expand dataset in practice.

2.2 Data Augmentation Algorithm

Data augmentation is to expand datasets by generate new samples with a certain methods. There are some traditional data augmentation methods below:

1. PCA Jittering: Applinga transformation to each pixel $I_{xy} = [I_{xy}^R, I_{xy}^G, I_{xy}^B]^T$of the image. The transformation is defined as :

$$[p_1, p_2, p_3][\alpha_1\lambda_1, \alpha_2\lambda_2, \alpha_3\lambda_3]^T.$$

p_i,λ_i are the eigenvectors and eigenvalues of the covariance matrix of I_{xy}, α_i is a random variable.

2. Noise: such as filter image with Gaussian Blur.
3. Random Scale, Random Crop, Horizontal/Vertical Flip, Shift and Rotation/Reflection, and Color Jittering etc.

Traditional data augmentation method will cause distortion and distortion to the original image. Due to the translation invariance in Mask R-CNN, methods such as shift have no significant effect on the detection accuracy. In contrast, pixel-level image blendis an effective method to generate new image samples.

2.3 Pixel-level Image Blend

According to recent research I, a single instance which is placed in different views, scales, directions, or lighting conditions extracts different features in object detection algorithm based on

CNN. Therefore, image blend is an effective methodto improve the coverage of various context conditions in a dataset [1]. It is necessary to ensure the global and local consistency of the image when generating new image samples. Therefore, it is reasonable to blend background image with pixel-level segmentation mask of the instance object instead of RoI about it. Pixel-level image blend includes the following steps:

1. Collecting object instances: labeled dataset is necessary for object detection. In order to extract object instances in images, pixel-level mask of each image is necessary. These foreground masks can be used to cut and paste object instances to the background image.
2. Collect background images: Background images must not contain the object instances and be similar to the original background of the instances. Otherwise, the differences between instances and background images may lead to useless context information [4].
3. Cut and paste the object instances: Different blending methods can be chosen to paste the object instances into the background images which is randomly selected. By this way, it is possible to ensure that the blending images covers different context information.

However, due to the difference between the object instances and the background images, artifacts may appeared at the edge of the object instances, which cause to a decrease in the global consistency of the blending image.

2.4 Cycle GAN Domain Adaptation

GAN is a generation model based on deep networks that distinguishes the distribution of input data and generates new data samples [7]. GAN usually consists of two sub-networks: one called generator, denoted by $G(z)$, another one called discriminator, denoted by $D(x)$. The generator takes noise data as input and provides the generated data to the discriminator. The discriminator takes real data or generated data as input, then predicts whetherthe input data is real or not. Training this networks corresponds to a minimax two-player game. The generator generates samples closer to real data in the process. The process can be denoted as:

$$\min_G \max_D V(G,D) \tag{1}$$

$$V(G,D) = \mathbb{E}_{x\sim p_{data}(x)}[log\, D(x)] + \mathbb{E}_{z\sim p_z(z)}\left[log\left(1 - D(G(z))\right)\right] \tag{2}$$

$V(G,D)$ denotes the loss function of the generator and the discriminator. p_{data} is the distribution of the original samples, p_z is the random noise distribution.

Based on GAN, Cycle GAN is used for establishing a mapping from the source domain to the target domain without additional information [8]. Cycle GAN contains two GANs, denoted by (G_{AB}, D_B) and (G_{BA}, D_A), which denotes a cyclic mapping between source domain A to target domain B. Mapping follows the following rules:

$$a \approx G_{BA}(G_{AB}(a)), b \approx G_{AB}(G_{BA}(b)) \tag{3}$$

The losses of two GANs can be expressed as:

$$L^B_{GAN}(G_{AB}, D_B) = \mathbb{E}_{b\sim p_d(b)}[log\, D_B(b)] + \mathbb{E}_{a\sim p_d(a)}\left[log\left(1 - D_B(G_{AB}(a))\right)\right] \tag{4}$$

$$L^A_{GAN}(G_{BA}, D_A) = \mathbb{E}_{a\sim p_d(a)}[log\, D_A(a)] + \mathbb{E}_{b\sim p_d(b)}\left[log\left(1 - D_A(G_{BA}(b))\right)\right] \tag{5}$$

In order to achieve cyclic consistency and prevent the GAN from mapping the source domain to a single picture in the target domain, cyclic consistent loss is defined as:

$$L_{CYC}(G_{AB}, G_{BA}) = \mathbb{E}_{a\sim p_d(a)}\left\|G_{BA}(G_{AB}(a)) - a\right\|_1 + \mathbb{E}_{b\sim p_d(b)}\left\|G_{AB}(G_{BA}(b)) - b\right\|_1 \tag{6}$$

In summary, the total loss of the Cycle GAN can be expressed as:

$$L = L^B_{GAN}(G_{AB}, D_B) + L^A_{GAN}(G_{BA}, D_A) + L_{CYC}(G_{AB}, G_{BA}) \tag{7}$$

3. EXPERIMENT AND RESULTS ANALYSIS

The paper's approach to treating diabetic retinopathy images uses the method described above and consists of three steps: 1. Data pre-processing, using existing data sets to fuse new data. 2. Data domain conversion, using Cycle GAN transformation to generate data to the target domain of the sample data. 3. Data validity test, using the generated data to train the Mask R-CNN detection network, and test the detection accuracy on the original data set, then analyze the detection metrics. On the basis of the experiment, this paper will compare the similarities and differences between the data generated by this program and the traditional data augmentation method, and analyze the validity and applicability of the method through statistical metrics such as the Intersection over Union (IoU), precision and recall.

3.1 Data

Diabetic retinopathy (DR) is a complication of diabetes that threatens vision and even leading to blindness. DR can be clinically divided into non-proliferative diabetic retinopathy and proliferative diabetic retinopathy. Due to the differences in medical equipment, datasets of DR often have different style. Therefore, it is difficult to obtain a large amount of available data.

All the object instances data in this paper is collected from West China hospital, Sichuan University. The dataset have 547 cases in total. DR manifests as retina hemorrhage, which has irregular texture, boundary and scale. Therefore, this paper mainly focus on instances larger than 20x20 pixels to extract more representative features. The background image data in this paper is from the Diabetic Retinopathy Detection dataset of kaggle 2018. Random combination of object instances and background images is adopted to ensure the diversity of generated data.

3.2 Cut and Paste Blend

It is mentioned above that pixel-level mask is necessary to blend the object instances and background images. But there are different methods to use the masks, such as Cut and Paste or Poisson Blend [7].

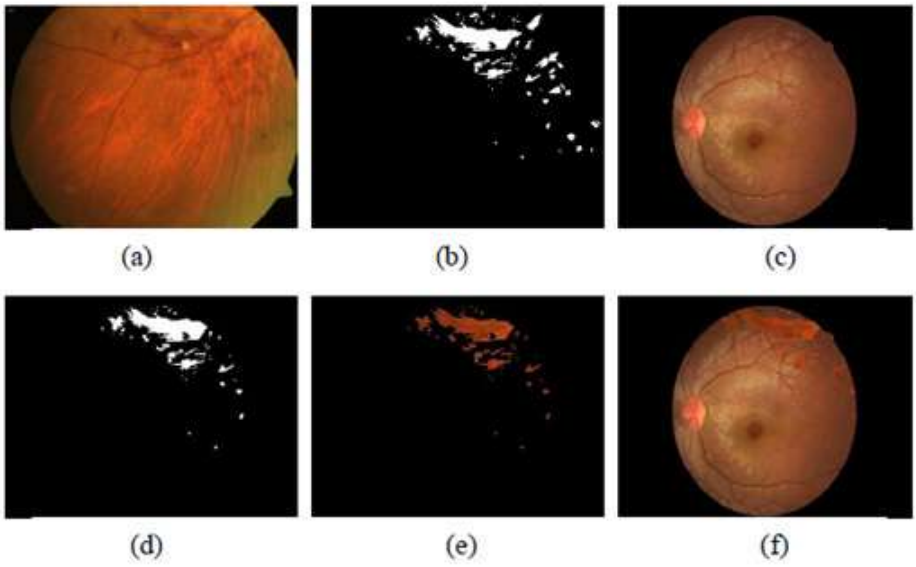


Figure 1. (a) original image (b) mask image (c) background image (d)mask after removing useless region (e) object instance after removing useless region(f) result of Cut and Paste Blend

Cut and Paste method means directly extracting the object instances area and replaces the corresponding pixel in the background images. The experiment is as follows:

Figure 1 (a) is a sample of 547 cases of object instances. Figure 1 (b) is a corresponding mask image, and Figure 1 (c) is a sample of the background image for blending. In order to prevent the object instance from appearing in an unrelated region, the first step is to find out the contour of the eyeball region of Figure 1 (c), and remove the mask where is beyond the eyeball region in Figure 1 (b). The mask after modify is shown in Figure 1 (d). And then, the corresponding object instance pixels in Figure 1 (a) are extracted as Figure. 1 (e) according to Figure 1 (d). Finally, Figure 1 (e) is used to replace the pixels of the corresponding region in Figure 1 (c), so that the blending image Figure 1 (f) is obtained.

3.3 Poisson Blend and Gaussian Blur

Poisson Blend is an image blend method based on the Poisson equation. Laplacian convolution kernel is used to obtain the divergence of each pixel in the image. Poisson Blend establishes a Poisson equation according to the divergence, and calculates the pixel value of the blend image.Poisson Blend can make the difference between the object instances and the background images smoothly diffused into the blend image and finally obtain seamless blend image [20].

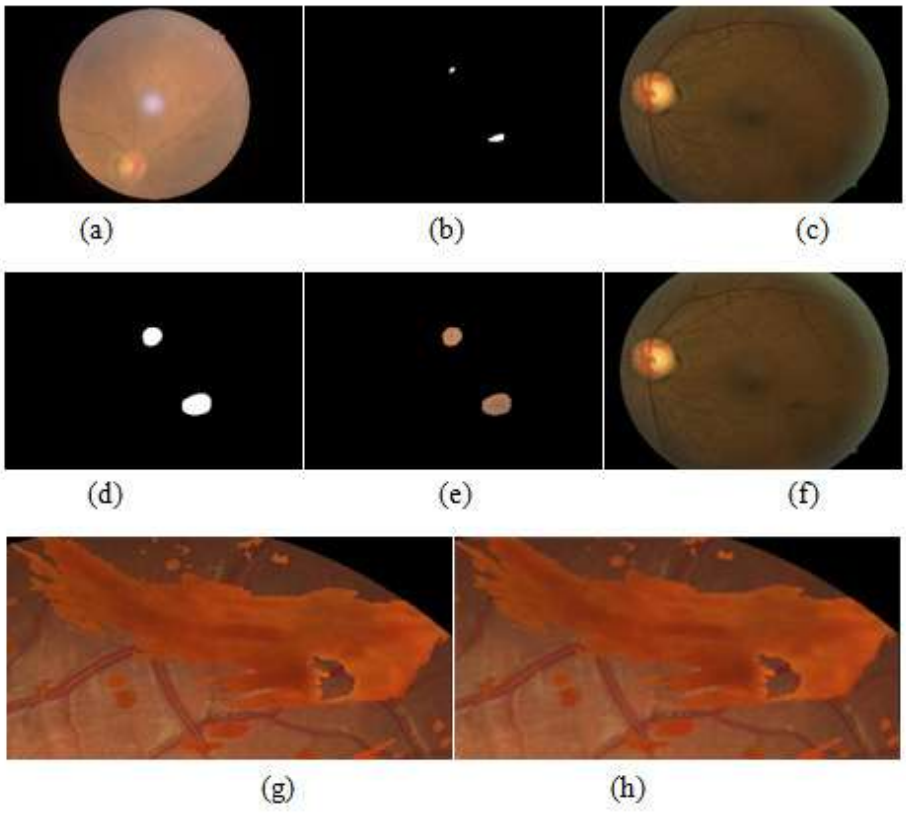


Figure 2. (a) original image (b) mask image (c) background image (d)mask after morphological dilation (e) object instance after morphological dilation (f) result of Poisson Blend (g) instance detail of Cut and Paste Blend (h) instance detail of Gaussian Blur

Poisson Blend need to cut pixels other than object instances edges. Therefore, mask image Figure 2 (b) should be processed with morphological dilation first. And then extracting the object instance pixels according to the mask Figure 2 (d). Figure 2 (e) is the extracted object instance.

Finally, the Poisson reconstruction equation of Figure 2 (c) and Figure 2 (e) is established and solved, so that a blend image obtained. The blending image is shown in Figure 2 (f).

Analyzing the results of the two blend method, it is obvious that Cut and Paste Blend retains the features of the object instance, but there are artifacts at the edge of the object instance, which decrease the global consistency of the blend image. Poisson fusion can achieve seamless blend, but the object instance is hard to recognize in the blend image. In order to maintain the features of the object instance, this paper chooses to use the Cut and Paste Blend and add a Gaussian Blur filter on the edge of the object instance to smooth the image. The result is shown in Figure 2 (h).

3.4 Domain Adaptation

Through the image blend processing above, a new instance sample containing object instance and background image has been obtained. However, due to the difference in distribution between the object instance and the background image, the blending image is still inconsistent with the original image, which may results in inaccurate feature extraction of the detection model. Domain adaptation is used to solve this problem. In this section, the blend images are defined as source domain and the original images are defined as target domain. And a Cycle GAN is trained learn the mapping between source domain and target domain. After training Cycle GAN, the generator G_{AB} can be used to transform blending images to new samples close to the original images.

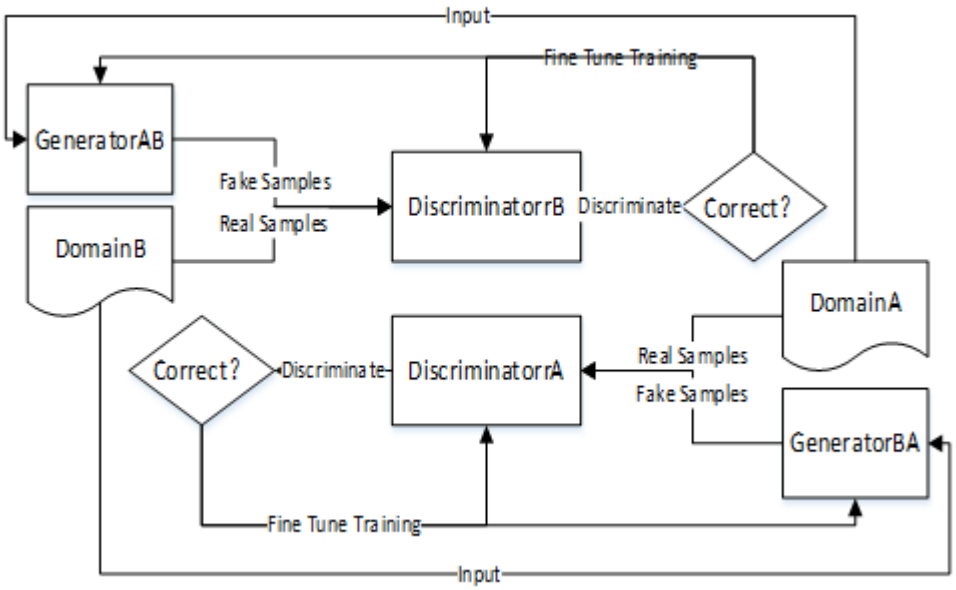


Figure 3 Structure of Cycle GAN Model. Cycle GAN works by training two transformations G_{AB} and G_{BA} between source domain A and target domain B in parallel.

Figure 3 shows the basic structure of the Cycle GAN. Cycle GAN uses the symmetric GANs to perform the same training on the source domain and target domain. But this paper focuses on the transformation of the source domain to the target domain. Therefore, G_{BA} is changed to takes the sample generated by G_{AB} as input instead of samples from domain B, so that two generators can be trained together. In addition, since the generated samples are used for object detection, hellinger distance is combined into cyclic consistent loss to improve the statistical consistency of the generated samples with the original images. The new loss function is defined as:

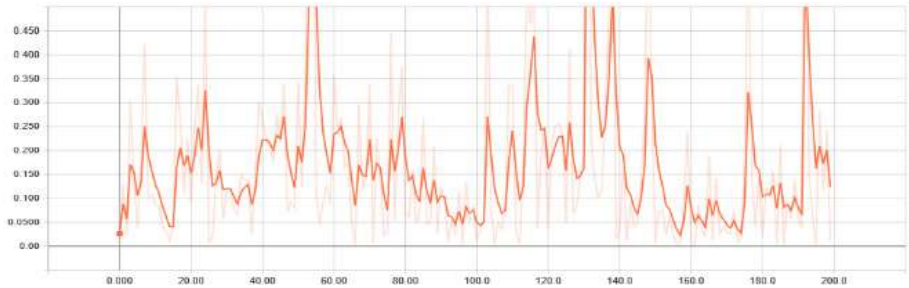
$$L = L_D + L_G + L_C \tag{8}$$

It consists of discriminator loss, generator loss and cyclic loop consistent loss:

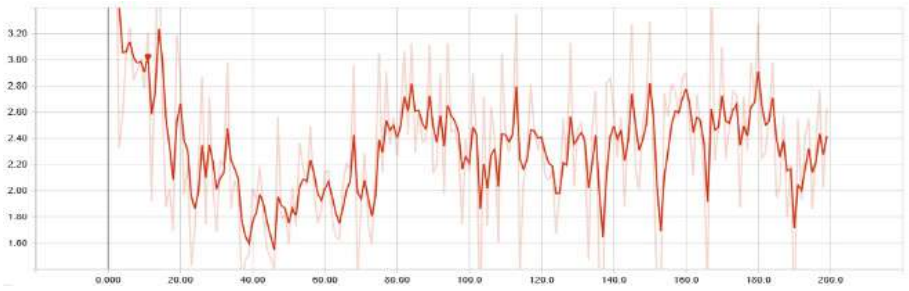
$$L_D = \mathbb{E}_{b\sim p_d(b)}[\log D_B(b)] + \mathbb{E}_{a\sim p_d(a)}[\log D_A(a)] \tag{9}$$

$$L_G = \mathbb{E}_{a\sim p_d(a)}\left[log\left(1 - D_B(G_{AB}(a))\right)\right] + \mathbb{E}_{a\sim p_d(a)}\left[log\left(1 - D_A\left(G_{BA}(G_{AB}(a))\right)\right)\right] \tag{10}$$

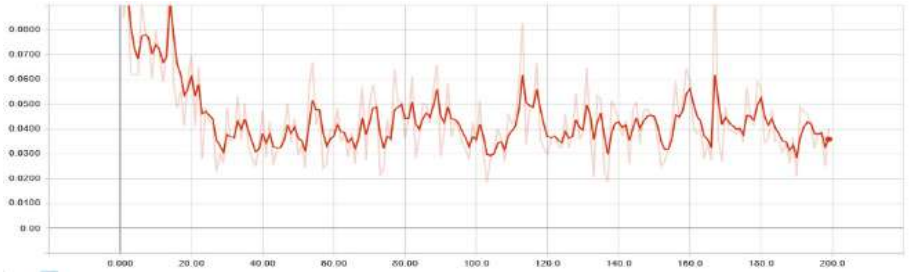
$$L_C = \mathbb{E}_{a\sim p_d(a)}\|G_{BA}(G_{AB}(a)) - a\|_1 + \mathbb{E}_{a\sim p_d(a)}\frac{1}{\sqrt{2}}\left\|\sqrt{G_{BA}(G_{AB}(a))} - \sqrt{a}\right\|_2 \tag{11}$$



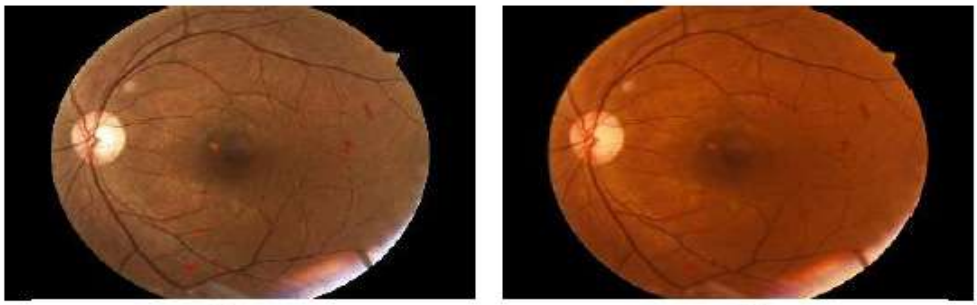
(a)



(b)



(c)



(d) (e)

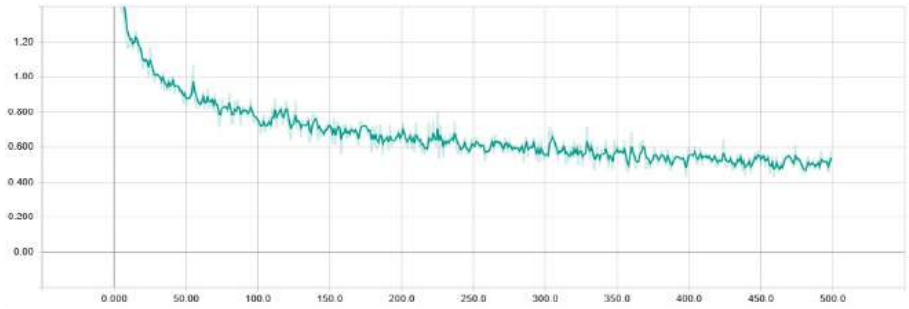
Figure 4. (a) discriminator loss (b) generator loss (c) cyclic consistency loss (d)blending image sample from source domain (e) generated image sample from target domain

Result of training this domain adaptation model is shown in Figure 4 (a) to Figure 4 (c). According to the loss, model in 50th iteration has better performance. Transform the blend image with the trained model, new samples shown in Figure. 4 (e) is obtained.

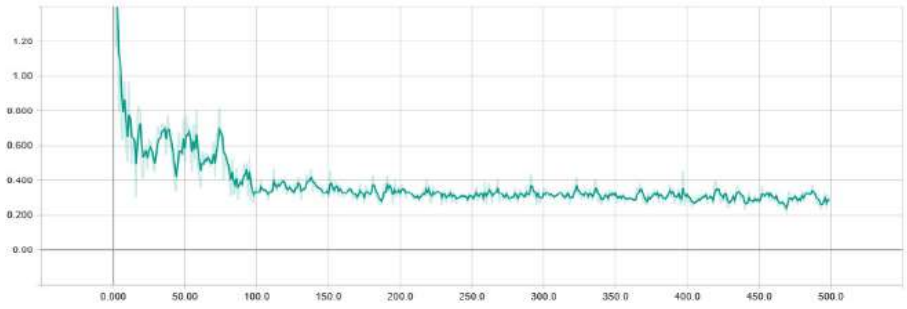
3.5 Object Detection

To examine the detection accuracy of the generated images. This paper trains the Mask R-CNN detection model with 2000 images generated by Cycle GAN. The original 547 cases of images are used as the test dataset to verify the accuracy of the trained model. For object detection, it is generally considered that the RoI is positive when the IoU is greater than 0.5. This paper use IoU over 0.5 and IoU over 0.75 to calculate the metrics include average precision and average recall. The average precision is denoted by $AP_{0.5}$and $AP_{0.75}$, and the average recall is denoted by $AR_{0.5}$ and $AR_{0.75}$.

The training loss and verification loss of the detection model are shown in Figure 5 (a) and Figure 5 (b). The annotated images and detection results of the test dataset are shown in Figure 5 (c) to Figure 5 (f). After calculation, The IoUs of instances between original image Figures 5 (c) and detection result Figures 5 (d) are 0.81 and 0.79, which results in precision 1.0 and recall 1.0.The IoUs of instances between original image Figures 5 (e) and detection result Figures 5 (f) are 0.77, 0 and 0.75, which results in precision 1.0 and recall 0.67. In order to compare and analyse the quality of the data augmentation methods above, 400 cases of original dataset and 2000 images generated by the traditional data augmentation method are also used to train Mask R-CNN As an experimental comparison. Similar to Figure 5, the metrics of the detection models obtained by the three datasets are calculated, and the results are shown in Table 1.



(a)



(b)

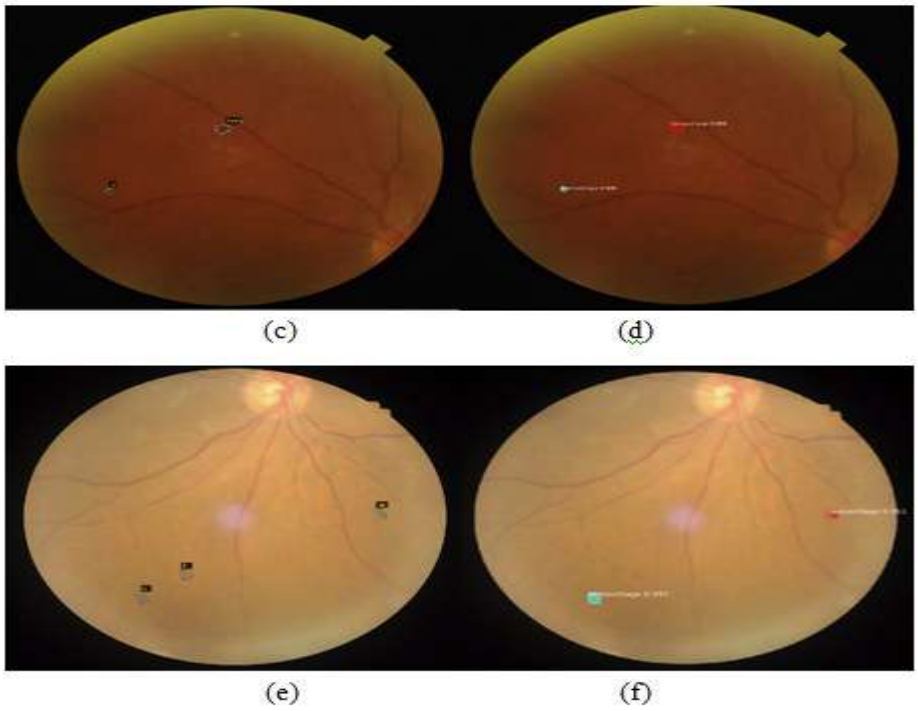


Figure 5. (a) train loss (b) val loss (c) labeled image from dataset (d) detected instance of Figure 5 (c) (e) labeled image from dataset (f) detected instance of Figure 5 (e)

Table 1. Detection results

Data Augmentation Method	$AP_{0.5}$	$AP_{0.75}$	$AR_{0.5}$	$AR_{0.75}$
No data augmentation	0.61	0.46	0.67	0.52
Traditional method	0.72	0.58	0.75	0.59
Image blend & Domain adaptation	0.74	0.61	0.84	0.79

4. CONCLUSION

In this paper, a data augmentation method combining pixel-level image blend and domain adaptation is proposed. By using the augmented data for the detection model training, the effectiveness of different data augmentation is compared.

Analysis of the results of Table 1 shows that the use of data augmentation can effectively reduce over-fitting of the detection model, improve the precision and recall. All data augmentation methods improve the $AP_{0.5}$ and $AR_{0.5}$ of the detection model to more than 0.7 when the training dataset was expanded from 400 cases to 2000 cases. Compared to the detection model without data augmentation. The precision was improved by more than 0.1. And the data augmentation method u combining pixel-level image blend and domain adaptation has a greater improvement on the recall rather than traditional method. The $AR_{0.5}$ reached 0.84 and $AR_{0.75}$ reached 0.79. The improvement of the precision is relatively lower than recall, the $AP_{0.5}$ reached 0.74 and $AP_{0.75}$ reached 0.61.

These results means that the additional context information generated by this method is more effective than the traditional method, so that the model can extract more features of the same object instance, which is beneficial to recognizing the object instance, thereby improving the recall. On the other hand, the fact that the features of the dataset are not obvious enough resulted in some false detection such as Figures 5(e). As a result, the precision is relatively low.

In summary, data augmentation can effectively expand the dataset of the object detection, and solve the over-fitting problem of the object detection model trained by small dataset. The data augmentation method based on pixel-level image blend and domain adaptation has better performance than the traditional method. At the same time, the validation of this method is accomplished in the dataset of medical images which has less contextual information. The validity and applicability of the method still need to be tested and optimized on other datasets. The subsequent work will also continue to optimize and improve the algorithm on the basis of this method.

ACKNOWLEDGEMENTS

The research work was supported by the Fundamental Research Funds for the Central Universities under Grant No. ZYGX2016J092, the Sichuan Science and Technology Project under Grant No. 2017GZ0318, and the Fundamental Research Funds for the Central Universities under Grant No. ZYGX2015J068.

REFERENCES

[1] Dwibedi, D., Misra, I., & Hebert, M. (2017, October). Cut, paste and learn: Surprisingly easy synthesis for instance detection. In The IEEE international conference on computer vision (ICCV).

[2] Karsch, K., Hedau, V., Forsyth, D., &Hoiem, D. (2011). Rendering synthetic objects into legacy photographs. ACM Transactions on Graphics (TOG), 30(6), 157.

[3] Ros, G., Sellart, L., Materzynska, J., Vazquez, D., & Lopez, A. M. (2016). The synthia dataset: A large collection of synthetic images for semantic segmentation of urban scenes. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 3234-3243).

[4] Dvornik, N., Mairal, J., &Schmid, C. (2018). Modeling visual context is key to augmenting object detection datasets. arXiv preprint arXiv:1807.07428.

[5] Chen, Y., Li, W., Sakaridis, C., Dai, D., & Van Gool, L. (2018, March). Domain adaptive faster r-cnn for object detection in the wild. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 3339-3348).

[6] Volpi, R., Morerio, P., Savarese, S., &Murino, V. (2018, June). Adversarial feature augmentation for unsupervised domain adaptation. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 5495-5504).

[7] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ...&Bengio, Y. (2014). Generative adversarial nets. In Advances in neural information processing systems (pp. 2672-2680).

[8] Chu, C., Zhmoginov, A., & Sandler, M. (2017). CycleGAN: a Master of Steganography. arXiv preprint arXiv:1712.02950.

[9] Almahairi, A., Rajeswar, S., Sordoni, A., Bachman, P., &Courville, A. (2018). Augmented CycleGAN: Learning Many-to-Many Mappings from Unpaired Data. arXiv preprint arXiv:1802.10151.

[10] Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. International journal of computer vision, 60(2), 91-110.

[11] Bay, H., Tuytelaars, T., & Van Gool, L. (2006, May). Surf: Speeded up robust features. In European conference on computer vision (pp. 404-417). Springer, Berlin, Heidelberg.

[12] Felzenszwalb, P., McAllester, D., &Ramanan, D. (2008, June). A discriminatively trained, multiscale, deformable part model. In Computer Vision and Pattern Recognition, 2008. CVPR 2008. IEEE Conference on (pp. 1-8). IEEE.

[13] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. In Advances in neural information processing systems (pp. 1097-1105).

[14] Girshick, R., Donahue, J., Darrell, T., & Malik, J. (2014). Rich feature hierarchies for accurate object detection and semantic segmentation. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 580-587).

[15] Girshick, R. (2015). Fast r-cnn. In Proceedings of the IEEE international conference on computer vision (pp. 1440-1448).

[16] Ren, S., He, K., Girshick, R., & Sun, J. (2015). Faster r-cnn: Towards real-time object detection with region proposal networks. In Advances in neural information processing systems (pp. 91-99).

[17] Lin, T. Y., Dollár, P., Girshick, R. B., He, K., Hariharan, B., &Belongie, S. J. (2017, July). Feature Pyramid Networks for Object Detection. In CVPR (Vol. 1, No. 2, p. 4).

[18] Long, J., Shelhamer, E., & Darrell, T. (2015). Fully convolutional networks for semantic segmentation. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 3431-3440).

[19] He, K., Gkioxari, G., Dollár, P., &Girshick, R. (2017, October). Mask r-cnn. In Computer Vision (ICCV), 2017 IEEE International Conference on (pp. 2980-2988). IEEE.

[20] Pérez, P., Gangnet, M., & Blake, A. (2003). Poisson image editing. ACM Transactions on graphics (TOG), 22(3), 313-318.

INTENTIONAL BLANK

EFFECTIVE SERVICE COMPOSITION APPROACH BASED ON PRUNING PERFORMANCE BOTTLENECKS

Navinderjit Kaur Kahlon and Kuljit Kaur Chahal

Department of Computer Science
Guru Nanak Dev University, Amritsar India

ABSTRACT

In recent years, several online services have proliferated to provide similar services with same functionality by different service providers with varying Quality of Service (QoS) properties. So, service composition should provide effective adaptation especially in a dynamically changing composition environment. Meanwhile, a large number of component services pose scalability issues. As a result, monitoring and resolving performance problems in web services based systems is challenging task as these systems depend on component web services that are distributed in nature. In this paper, a distributed approach is used to identify performance related problems in component web services. The service composition adaptation provides timely replacement of the performance bottleneck source that can prohibit performance degradation for the forthcoming requests. Experimentation results demonstrate the efficiency of the proposed approach, and also the quality of solution of a service composition is maintained.

KEYWORDS

Web service composition; Quality of Service; reconfiguration; self-adaptive; optimal.

1. INTRODUCTION

A web services based software system also referred as a Composite Web Service (CWS) makes use of third party web services which run on-the-fly. Adaptability is one of the key requirements of such systems keeping in view the dynamic environment in which they execute [1]. Despite having to be continuously available, they also need to strive to remain optimal in changing conditions. Thus, reconfiguration of a CWS is required to adjust or adapt as per the changed scenario [2].So an important infrastructure level concern is to add self-adaptation ability so that a web services based solution can adapt seamlessly as the execution environment changes.

A self-adaptive (self-healing or autonomic) system possesses capabilities to reconfigure in response to changing environment conditions [3]. In a self-adaptive system, monitoring occurs alongside its execution. The system may need to adapt depending upon the information extracted during monitoring. However, monitoring and adaptation [4] is not trivial in a web services based system which is distributed at different physical locations. The distributed ownership of the component web services add to the complexity of such systems.

Most of the existing approaches that focus on the challenges of building complex web services based systems; treat critical situations arising in a dynamic execution environment as exceptions [5] or failures that require repair [6]. However a web service based system executing in a static environment cannot be a real world application. In a real world web services based system;

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 287-296, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90924

change is not an exception but a rule. Changes are a natural phenomenon for such systems as they operate in a dynamic execution environment. Moreover, a web services based system has not only to be correct and reliable, but it should also ensure that it remains optimal as the component web services evolve independently. The need to reconfigure a web service composition in a timely manner when change events happen during its execution is an important issue and still an open question [7, 8].

In this paper, a distributed (a hybrid of client and server) monitoring approach that keeps track of QoS values of different component web services of a web services based system is presented. Whenever QoS of a component web service degrades, the composite web service is notified which then replaces the component web service with an alternative. We extend this framework further to identify component web services which make the composite web service sub-optimal. Such web services are pruned and replaced with better alternatives. Better alternatives may be available in distant/premium service repositories. It is assumed that all web services are substitutable and it is feasible to find direct substitutes either in local or in distant/premium repositories.

The main contributions of this paper are:

- The service clients are notified just-in-time using publish-subscribe mechanism when QoS of a component web service degrades. The service client then automatically (without any human intervention) shifts to a better alternative.
- To localize the source of performance bottlenecks by monitoring the present workflow and pruning such source by replacing it with a better alternative in the proposed framework.

This paper contains five sections. Section 2 presents related work about web service composition and self-adaptive web service composition at runtime. Section 3 gives an overview of the system design, and different modules to implement the proposed approach. Section 4 presents the results of the experiments. Finally, section 5 concludes the paper.

2. RELATED WORK

Existing web service composition approaches [9,10,11] strive to find an optimal solution at design phase, which is not efficient (as it is a NP-hard problem) and does not scale up for a large data set size. It also does not reflect a real world situation where a web service composition has to remain optimal in a dynamic execution environment. As consumers find it difficult to select a service composition that is near optimal solution satisfying functional and non-functional requirements, eagle strategy can be used [27].

Liu et al. [12] use prediction based on case based reasoning to solve web service composition problem efficiently and effectively. Moustafa and Zang [13] predict potential degradation scenarios, and apply a proactive approach whenever the system deviates from expected QoS. Such solutions are appropriate for a dynamic execution environment. But their major drawback is that many a time predictions fail, and the overhead incurred to handle failed prediction may be high. In case of the Internet based applications, QoS degradation of component web services may be transient when the system load is high at one point of time. The dynamic optimization of a service composition can be done by using multi-agent reinforcement learning [26]. A distributed Q-learning algorithm is used to accelerate the convergence rate.

Angarita et al. [14] propose to build fault tolerant CWS to ensure that either such a CWS completes successfully or leaves the execution in a safe state when component web services fail to perform as per expectations. Campos et al. [8] present an approach for building adaptive service compositions by detecting undesirable behaviors in their execution traces. They propose

to use formal methods to verify web service adaptation at execution time in a dynamic environment.

After detecting violations in QoS values, the adaptation mechanism gets triggered. Adaptation involves reconfiguring the execution plan without stopping the composite service execution. Adaptation may be implemented by following a reactive [8], a proactive approach [15], or a post-mortem of the previous execution traces to improve the system for future [16].

Zhu et al. [17] argue that effective runtime adaptation of service needs real changes in QoS of web services for timely and accurate decisions about -When to trigger adaptation action?, Which web service to replace in execution?, and Which candidate web service to select? Adaptable Web Services Framework (AWSF) [18] and Self ADaptIve for web service Compositon (SADICO)[19] are the two frameworks which take into consideration the service user's context (e.g. device features such as screen size, bandwidth, or user location) and adapt the web service behavior so that web service becomes more relevant and useful.

Although, many solutions have been proposed to adapt a web services based software solution to QoS changes of its component web services [20,21], but runtime monitoring of component web services, and then communication of the data, collected during monitoring, to the clients still needs to improve.

3. SYSTEM DESIGN AND IMPLEMENTATION

3.1 Assumptions

This work relies on a few key assumptions. First, it assumes that all component web services are substitutable and it is feasible to find direct substitutes either in local or in distant/premium repositories. Second, there exist two distinct periods of performance i.e. execution traces with distinct levels of performance. Third, the workload (i.e. request arrival rate) is uniform across different periods of analysis. Performance comparison of different execution traces under different workloads is not justified. Fourth, all the component web service are supposed to have same levels of performance. Though it seems unrealistic, but this assumption is motivated by the quality characteristics of web services. Fifth, the network connection between web services is error free, even though individual atomic services may be problematic. Lastly, service clients and providers are trustworthy entities, and there are no security risks when mobile agents execute on the provider side.

3.2 System Overview

This section presents the basic components of our proposed system by describing their own functions along with their interaction with other components in the system.
The proposed system is composed of five components as:

A. The Basic Process

A workflow manager receives a client request; gets the corresponding abstract composition; selects corresponding concrete web services; dispatches mobile agents to service providers to monitor the QoS behavior of the chosen web services for execution in composition; invokes the partner web services for preparing the results and responds back to the client.

B. Monitoring the logs for QoS degradation

Once the deployed web services are invoked upon client request in the composition workflow, continuous monitoring and analysis of component web services is done by examining their execution logs on the provider side. The execution logs consisting of QoS values of web services are maintained at the service provider side when each web service gets executed in the execution workflow. Each web service execution log is maintained for future prediction based analysis. Monitoring and adaptation of the component web services is based on four QoS parameters as execution time, throughput, reliability and availability. The values for QoS parameters are calculated using the formulae in Table 1.

Table1: QoS Parameters formulae

Execution Time	Response Time − Request Time
Throughput	$\frac{\text{No of completed requests}}{\text{unit time}}$
Reliability	$\frac{\text{Number of failures}}{\text{total requests per unit time}}$
Availability	$\frac{\text{MTBF}}{\text{MTBF + MTTR}}$

The throughput, reliability, and availability are the attributes with positive dimension i.e. higher the value, better it is, whereas, execution time is a negative dimension.

C. Log Monitoring to identify the source of performance bottleneck

This section presents an approach to improve QoS of a composite web service when some of its component web services are acting as a performance bottleneck in the service composition. Inter Quartile Range (IQR) is computed to measure variability in the data set by analyzing the previous execution logs. IQR is the difference between first quartile (Q1) and third quartile (Q3). The upper and lower threshold values in the dataset corresponding to every QoS attributes are calculated by using Tukey Fences [22] method which is a popular method of identifying extreme data values in a data set.

$$\text{Lower threshold} = Q1 - 1.5(IQR) \quad \text{----(1)}$$
$$\text{Upper threshold} = Q3 + 1.5(IQR) \quad \text{----(2)}$$

A component web service executing in the workflow that can act as performance bottleneck can be detected based on its QoS values. The comparison against the threshold values depend upon the type of dimension of the QoS attributes. A component web service with QoS attribute as a negative (positive) dimension will be compared with the upper (lower) threshold value. In case there are multiple component web services adding to the performance degradation of the workflow, then pruning of a web service is decided on the basis of the quantum of influence that a web service has on the workflow. A web service with maximum influence is pruned first and then the others in that order.

A workflow in a service composition may follow serial, cyclic, parallel, or a combination of the three execution patterns of partner web services [23]. Aggregate value of a QoS attribute for a CWS is calculated using different formulae for the different workflow patterns. Table 2 gives the formulae for a sequential workflow used in the service composition. In a sequential pattern, the

component web services execute in a serial order. The proposed service composition is a simple sequence of service executions.

Table 2: QoS aggregate formulae for a sequential workflow

QoS Constraint	Sequence
Execution Time	$\sum_{i=1}^{n}\sum_{j=1}^{l_i} q_{et}(c_{ij})$
Throughput	$Min\sum_{i=1}^{n}\sum_{j=1}^{l_i} q_{tp}$
Reliability	$\prod_{i}^{n} q_{rl}(ci)$
Availability	$\prod_{i}^{n} q_{al}(ci)$

D. Just-in-time Notification

In a web service based application, changes in QoS values of component web services take place on-the-fly. Therefore, the challenge lies in tracking up-to-date information regarding changes in status of component services and then implementing change reaction decisions as soon as possible.

Many researchers have proposed models and mechanisms for monitoring component web services for dynamic reconfiguration of a CWS [21], but to reconfigure a web service composition in a timely manner when change events happen during its execution is an important issue and still an open question [7,8].

A novel idea to handle web service failures in service oriented software systems uses a push mechanism to notify client application about the failure of a service. A multi agent system tracks a web service on the provider side, and informs the client application as soon as the service fails. This approach is expected to reduce delay in making the replacement decisions. It is also easy on resources as the solution is distributed, and therefore monitoring overhead is also divided between service consumer and provider.

An agent based approach for handling web service availability issues uses the concept of mobile agents, which run at service provider side and provide latest information regarding the web service to the service user. Therefore, service user can arrange alternatives of a failed service even before invoking it. In addition, it also proposes service replacement strategies for optimizing the process execution.

E. Adaption in case of QoS degradation and performance bottleneck

The proposed framework will trigger adaptation as soon as a web service executing in the service composition becomes unavailable or its aggregate QoS values degrade at a provider. This will replace the faulty web service with the next best service (of the same category) available in the local repository. If the last service of a particular category is used, an alert is raised to retrieve more services matching the criteria from the external repository. If the web services alternatives do not exist in the service registry, then the search space is expanded to distant or premium

service repositories. Therefore, a potential set of services are always ready for replacement. Lastly, if no matching candidate services are found, then the application may be terminated.

3.3 System Implementation

The prototype of proposed framework is implemented using Java EE. The experiment is conducted on an Intel Core i5 processor with 4 GB RAM running on Windows 7 using Tomcat server and JADE 7 [24, 25]. The web services used in the experiment are described and selected with quality parameters. In order to save time, an abstract service composition is available before execution of the workflow starts.

The process execution starts when a user hits the service client module on a (mobile) device as shown in Figure 1. The service client prompts the user to enter the type of problem (e.g. accident case or a sudden heart attack). The workflow of the service composition starts by finding the current location of user with help of the location locator service. Then an *emergency hospital finder* service finds the appropriate hospitals on the basis of the user location and the specialized services required in the case. The map and time services provide best route related information. If the user had opted for an ambulance service, then a transport management service provider is invoked. User's location and best route from the source to destination is passed as input to the transport service provider.

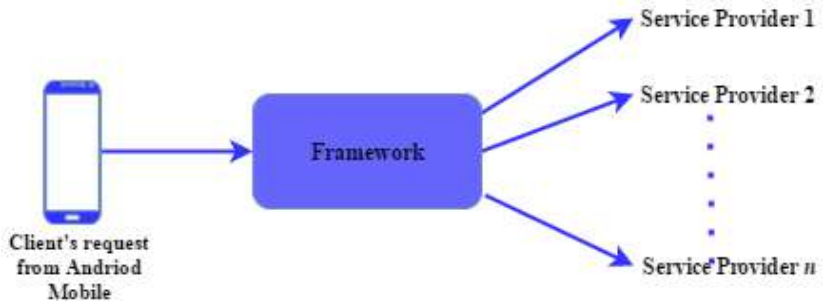


Figure 1. The service composition

4. RESULTS AND ANALYSIS

4.1 Performance Evaluation

A performance of a system can be evaluated on the basis of several criteria such as execution time, throughput, and scalability. The execution time is the time spent in servicing a request which also includes time the framework spends in handling the change events i.e. when the change event is detected, and the replacement of a web service is invoked. Throughput is the number of requests completed in unit time.

Figure 2 shows CWS execution time in three different situations 1) a best case that does not need to adapt, 2) a reactive solution to handle change events and, 3) proposed framework. The request was repeated 50 times, and average response time was calculated. In the first case, request is services in 0.28 sec as the system operates in a static environment, and no change event happens. However, such a case is suitable for comparison only to mark a benchmark case. In the real world, there cannot be a web services based solution that does not need to handle change events as the underlying environment is based on the Internet, and is continuously changing. In the second case, the execution time turns out to be 0.65 seconds. While in third case the execution time is around 0.45 seconds. It is remarkably less than the second case that follows a reactive approach to handle change events. The main reason for the time gap in these two cases is that our

proposed approach uses a preselected set of candidate services for replacement in case a component web service degrades or becomes a performance bottleneck.

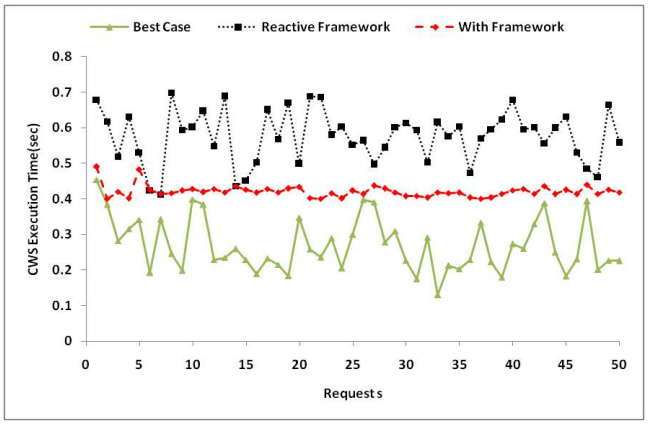


Figure 2. CWS Execution Time (seconds) (1) Best case, (2) Reactive Framework, (3) With Framework

4.2 Analyzing the Quality of Solution

The QoS attributes such as execution time, throughput, availability, and reliability of component web services play a vital role to determine the aggregate QoS of CWS. Figures 3 to 6 show the performance of QoS attributes of CWS performed for simultaneous 100 requests. Figure 3 demonstrate that the execution time of the CWS remains stable even if there is a QoS degradation of component web services or if any web service acts as a performance bottleneck. The average execution time of CWS is nearly 0.45 seconds; though there is a rise in execution time in first ten requests which is warmup time taken by the system to start the workflow. Figure 4 shows that throughput of the service composition improves over period of time. The throughput of proposed system increases as the number of requests is increased over time. After certain time interval the throughput of proposed system becomes stable even if the component web services are creating performance bottleneck for the service composition. Figure 5 and 6 depicts the reliability and availability of the service composition respectively. The results demonstrate that values of reliability and availability are consistently good on an average. The small variations in Figure 5 and 6 are depicted because of the time taken to substitute the component web service which is acting a performance bottleneck for the service composition execution.

Therefore, the proposed framework maintains a stable performance of various QoS attributes in a service composition execution even if the values of QoS attributes degrade over time. The variations in QoS values in a dynamic service execution environment is due to QoS degradation of component web services which should be replaced with better alternatives to improve the quality of solution of a workflow.

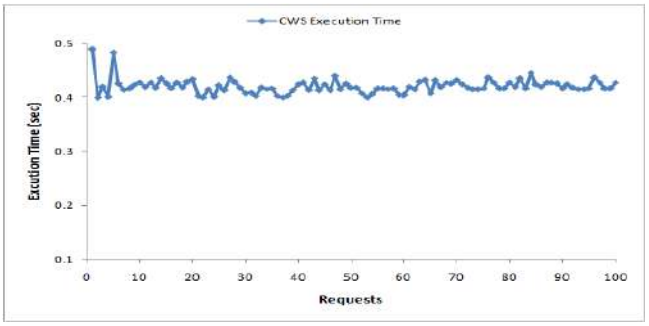


Figure 3. Execution time of the CWS

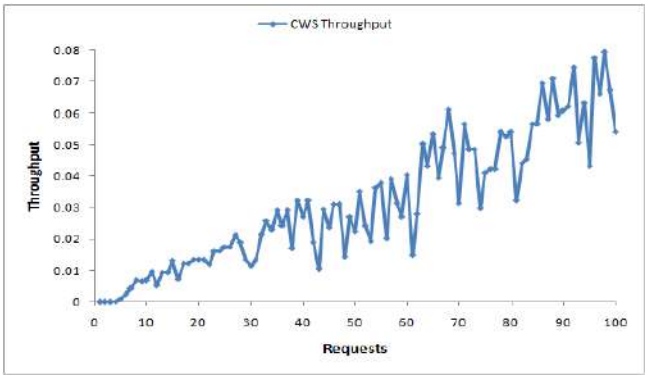


Figure 4. Throughput of the CWS

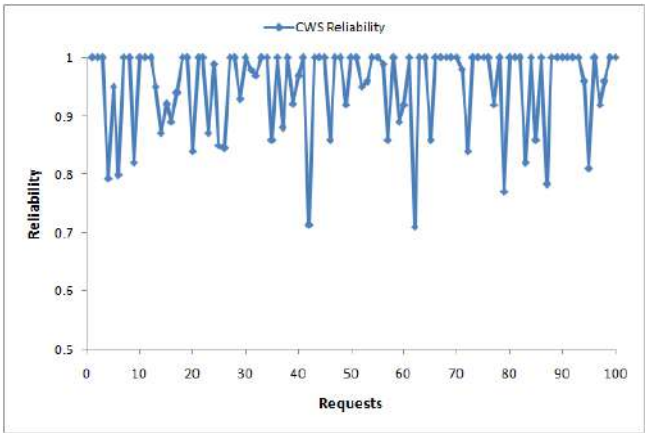


Figure 5. Reliability of the CWS

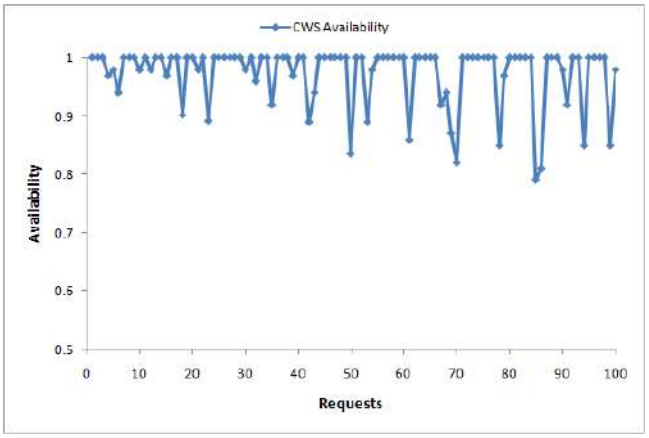


Figure 6. Availability of the CWS

5. CONCLUSIONS

The monitoring and adaptation of web service composition according to the changing scenario at runtime has drawn a lot of attention in the web services based solutions. This paper proposes a distributed monitoring and adaptation framework to keep track of the performance bottleneck of component web services. This paper follows a preventive approach in invocation of component web service with degraded QoS. Additionally, the applicability of the self-adaptive system on the various quality dimensions, such as reliability, availability and throughput is discussed. The

adaptation process is flexible enough as it takes into consideration different QoS requirements of different clients.

The experimental results demonstrate that the proposed approach performs better even if component web services are creating performance bottlenecks. The quality of solution is efficient for QoS parameters such as execution time, throughput, reliability and availability. In future, we plan to extend the framework for global optimization of web service composition using self-learning techniques.

REFERENCES

[1] Di Nitto, E., Ghezzi, C., Metzger, A., Papazoglou, M., & Pohl, K. (2008). A journey to highly dynamic, self-adaptive service-based applications. *Automated Software Engineering*, *15*(3), 313-341.

[2] Liang, Q., Lee, B., & Hung, P. (2014). A rule-based approach for availability of service by automated service substitution. *Softw.,Pract. Exper. 44(1)* , 47-76.

[3] Psaier, H., Juszczyk, L., Skopik, F., Schall, D., & Dustdar, S. (2010, September). Runtime behavior monitoring and self-adaptation in service-oriented systems. In *2010 Fourth IEEE International Conference on Self-Adaptive and Self-Organizing Systems* (pp. 164-173). Ieee.

[4] Guinea, S., Kecskemeti, G., Marconi, A., &Wetzstein, B. (2011, December). Multi-layered monitoring and adaptation. In *International Conference on Service-Oriented Computing* (pp. 359-373). Springer, Berlin, Heidelberg.

[5] Zeng, L., Lei, H., Jeng, J. J., Chung, J. Y., & Benatallah, B. (2005, July). Policy-driven exception-management for composite web services. In *Seventh IEEE International Conference on E-Commerce Technology (CEC'05)* (pp. 355-363). IEEE.

[6] Friedrich, G., Fugini, M. G., Mussi, E., Pernici, B., &Tagni, G. (2010). Exception handling for repair in service-based processes. *IEEE Transactions on Software Engineering*, *36*(2), 198-215

[7] He, Q., Xie, X., Wang, Y., Ye, D., Chen, F., Jin, H., & Yang, Y. (2017). Localizing Runtime Anomalies in Service-Oriented Systems. *IEEE Transactions on Services Computing*, *10*(1), 94-106.

[8] Campos, G. M., Souto Rosa, N., & Ferreira Pires, L. (2017, January). Adaptive service composition based on runtime verification of formal properties. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

[9] Cheng, S. P., Lu, X. M., & Zhou, X. Z. (2014). Globally optimal selection of web composite services based on univariate marginal distribution algorithm. Neural Computing and Applications, 24(1), 27-36. https://doi.org/10.1007/s00521-013-1440-9

[10] Chen, Y., Huang, J., Lin, C., & Hu, J. (2015). A partial selection methodology for efficient qos-aware service composition. IEEE Transactions on Services Computing, 8(3), 384-397.

[11] Cremene, M., Suciu, M., Pallez, D., & Dumitrescu, D. (2016). Comparative analysis of multi-objective evolutionary algorithms for QoS-aware web service composition. *Applied Soft Computing*, *39*, 124-139.

[12] Liu, X., Shi, W., Kale, A., Ding, C., & Yu, Q. (2017). Statistical Learning of Domain-Specific Quality-of-Service Features from User Reviews. *ACM Transactions on Internet Technology (TOIT)*, *17*(2), 22.

[13] Moustafa and ZangMoustafa, A., & Zhang, M. (2012, June). Towards Proactive Web Service Adaptation. In *CAiSE*(pp. 473-485).

[14] Angarita, R., Cardinale, Y., &Rukoz, M. (2014). Reliable composite web services execution: towards a dynamic recovery decision. Electronic Notes in Theoretical Computer Science, 302, 5-28.

[15] Xiong X., Wang P., Zhang Q., Pu C. L. (2014). Revisiting proactive service-oriented architecture: from design and implementation to validation and performance improvement, International Journal of Services ComputingVol. 2, No. 1, pp. 1-12.

[16] Chahal, K. K., Kahlon, N. K., &Narang, S. B. (2017). Improving the QoS of a Composite Web Service by Pruning its Weak Partners. In *Requirements Engineering for Service and Cloud Computing* (pp. 271-290). Springer International Publishing.

[17] Zhu, J., He, P., Zheng, Z., & Lyu, M. R. (2017). Online QoS prediction for runtime service adaptation via adaptive matrix factorization. *IEEE Transactions on Parallel and Distributed Systems*, *28*(10), 2911-2924.

[18] El Hog, C., Djemaa, R. B., & Amous, I. (2014). A User-Aware Approach to Provide Adaptive Web Services. *J. UCS*, *20*(7), 944-963.

[19] Nabli, H., Cherif, S., Djmeaa, R. B., & Amor, I. A. B. (2018, May). SADICO: Self-ADaptIve Approach to the Web Service COmposition. In *International Conference on Intelligent Interactive Multimedia Systems and Services* (pp. 254-267). Springer, Cham.

[20] Angarita, R. (2015, July). Responsible objects: Towards self-healing internet of things applications. In *2015 IEEE International Conference on Autonomic Computing* (pp. 307-312). IEEE.

[21] Angarita, R., Rukoz, M., &Cardinale, Y. (2016). Modeling dynamic recovery strategy for composite web services execution. World Wide Web, 19(1), 89-109.

[22] Yu, C. H. (1977). Exploratory data analysis. *Methods*, *2*, 131-160.

[23] Fakhfakh, N., Verjus, H., Pourraz, F., &Moreaux, P. (2013). QoS aggregation for service orchestrations based on workflow pattern rules and MCDM method: evaluation at design time and runtime. *Service Oriented Computing and Applications*, *7*(1), 15-31.

[24] Bellifemine, F., Caire, G., Poggi, A., &Rimassa, G. (2008). JADE: A software framework for developing multi-agent applications. Lessons learned. *Information and Software Technology*, *50*(1), 10-21.

[25] JADE mobile agent platform, http://jade.tilab.com

[26] Wang, H., Wang, X., Hu, X., Zhang, X., & Gu, M. (2016). A multi-agent reinforcement learning approach to dynamic service composition. *Information Sciences*, *363*, 96-119.

[27] Gavvala, S. K., Jatoth, C., Gangadharan, G. R., & Buyya, R. (2019). QoS-aware cloud service composition using eagle strategy. *Future Generation Computer Systems*, *90*, 273-290.

AUTHORS

Navinderjit Kaur Kahlon received Ph.D. degree and Master's degree in Computer Science and Engineering from Guru Nanak Dev University, India. She is currently working as an Assistant Professor in the Department of Computer Science, Guru Nanak Dev University, India. The research interests include Service Oriented Computing, Distributed Systems, Mobile Agents and Web Technologies.

Kuljit Kaur Chahal received the Ph.D. in Computer Science in 2011. She is working as an Associate Professor in the Department of Computer Science, Guru Nanak Dev University, India. Her research interests are Distributed Computing, Web Services Security, and Open Source Softwares.

DATA VIRTUALIZATION FOR ANALYTICS AND BUSINESS INTELLIGENCE IN BIG DATA

Manoj Muniswamaiah, Tilak Agerwala and Charles Tappert

Seidenberg School of CSIS, Pace University, White Plains, New York

ABSTRACT

Data analytics and Business Intelligence (BI) is essential for strategic and operational decision making in an organization. Data analytics emphasizes on algorithms to control the relationship between data offering insights. The major difference between BI and analytics is that analytics has predictive competence whereas Business Intelligence helps in informed decision-making built on the analysis of past data. Business Intelligence solutions are among the most valued data management tools available. Business Intelligence solutions gather and examine current, actionable data with the determination of providing insights into refining business operations. Data needs to be integrated from disparate sources in order to derive insights. Traditionally organizations employ data warehouses and ETL process to obtain integrated data. Recently Data virtualization has been used to speed up the data integration process. Data virtualization and ETL are often complementary technologies performing complex, multi-pass data transformation and cleansing operations, and bulk loading the data into a target data store. In this paper we provide an overview of Data virtualization technique used for Data analytics and BI.

KEYWORDS

Data Analytics, Business Intelligence, Big data, Data Virtualization, ETL and Data Integration.

1. INTRODUCTION

Success of an organization depends upon the decision making process. These decisions are based on the collection and analysis of data been gathered. During the early stages of business intelligence and analytical development in 1990s the data collected and processed was mostly structured, collected from legacy systems and stored in relational databases which also supported online analytical processing and reporting on the enterprise-specific data. In addition to reporting functionalities data mining techniques such as clustering, regression analysis, anomaly detection and classifications was also supported. In the early 2000s the raise of internet helped web search and e-commerce companies such as Google and Amazon to present their business online to the users and interact with them. Companies began collecting user specific data through logs and cookies in order to understand user behaviors and improve business. Web and text analytics was developed to determine user browsing and purchasing patterns. Web site design, personalization and recommendation engine can be built using web analytics. In recent times the use of IoT ("Internet of Things") such as mobile and sensor devices have increased in usage and provides an opportunity for analytics based on location-aware and person-centric operations [1].

Data needs to be collected from disparate data sources and processed as a part of data integration process. Analysis and correlation of data provides key insights into the business decisions and also helps in predictive analysis. Organization sales, human resources and marketing department gather and analyze data obtained from data integration process. They have multiple databases

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 297-302, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90925

which are in cloud and on-premise, extracting data from all these repositories and sources is a part of data integration process. Data from these repositories can be extracted in many different ways using either push or pull techniques. Also, same business entity could have different semantic value which needs to be reconciled and correlated. Extracted data also undergoes cleansing and transformation process before deriving key insights from it. Business Intelligence and analytical techniques also provide business-centric methodologies which can be applied to various applications such as e-commerce, healthcare and security. In this paper we are focused on Data analytics and Business Intelligence process using Data virtualization for data integration [2].

The traditional data integration approach of moving data from source to target database after cleaning, demoralization and transformation is called Extract-Transform-Load. The target data store is called data warehouse which runs on high end parallel computational hardware systems. Data virtualization is the new technique which does not move the data from the source data stores. Instead all the cleansing and transformation of data is done through virtual tables. It provides better agility and has shorter data integration life cycle. In this research we examine data virtualization technique impact for analytics and business intelligence and contrast it with traditional data warehouse process [3].

2. BACKGROUND

Organizations employ Data analytics and Business Intelligence for decision making process. Data discovery helps in integration of all the available data across the organization. It is common to have large databases and understanding the relations between tables and data is the first step of data integration. Data discovery is the process of collecting data from various databases in silos and consolidating it into a single source that can be easily and instantly evaluated. Having heterogeneous data stores results in different semantic definition of the same business entity which needs to be cleansed to remove discrepancies. Once data is cleansed it requires transformations to normalize tables and resolve any data type and unit differences in the data. Data can be correlated based on filtering, joins or aggregation. Business analysts can examine their hypothesis on the data available after data correlation stage. The analyzed data can be visualized using various tools for presentation.

Figure 1: Phases of Data Integration

ETL process involves moving the data from source data stores to staging area and later it undergoes cleansing and transformation before been loaded in to target data warehouse. Data warehouse off loads data analysis related work from source data stores, provides an integrated and consistent view of the integrated data. Data warehouse also supports materialized views of the tables, indexing on columns and creation of star and snowflake schemas which groups data into fact table containing business related information [4].

Data virtualization does data cleansing, transformation, association and correlation from source data stores evading any in-between physical data movement. Each of these stages are distinct using virtual tables, each step uses data from preceding one by using virtual tables. It uses connectors such as JDBC or ODBC to access the source data. The relationship of different tables, attributes and constraints metadata are stored in data source catalogs which is used by Data virtualization. Virtual tables are the result set of query which acts like a regular table, it is virtual since data is not physically stored and data is brought from underlying table when virtual table query is executed. Multiple views would be defined at various level of abstraction and when a

query is executed data moves through these views before producing the result [5].

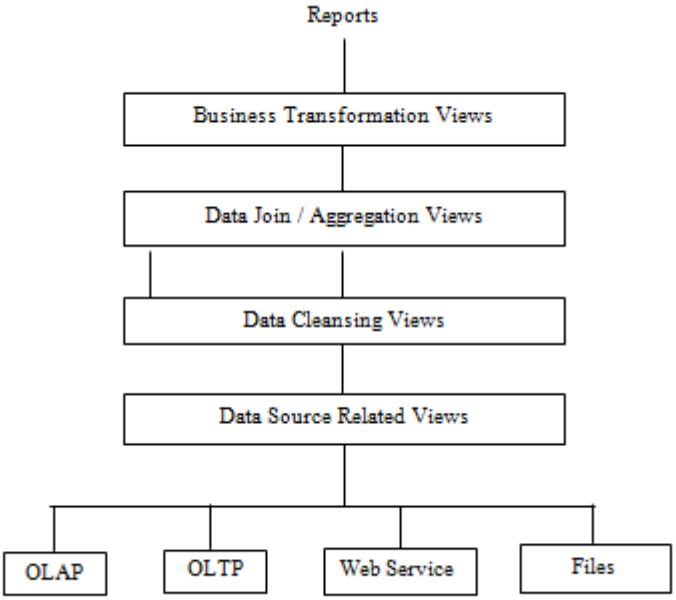


Figure 2: Data Virtualization

Since data is fetched from disparate data sources and views are defined for various data integration stages, the relevance of having a cost based query optimizer becomes important which reduces the query latency and improves performance. Figure 2 shows the various views of the Data virtualization process which extracts, cleans and transforms the data fetched from different sources.

3. DATA VIRTUALIZATION OVERVIEW

Data virtualization facilitates extraction of business insights by creating an abstraction layer and providing a unified view of data which are in traditional repositories or in cloud. The abstraction layer exposes only accessible data to the users without requiring them to know about the physical location of the data and it ensures that the users meet the data governance policies. Data virtualization enables easy data gathering and manipulation by reducing data duplication and compression across different databases. This also helps in infrastructure cost savings. It does not require to perform ETL process but instead virtually connects different databases to provide virtual views and publish them. This makes data readily available for analysis and reporting. This reduces silos across different data repositories with in an organization. Data virtualization is an integral part of data management which extracts greater value from data sources.

Data virtualization delivers data as a service to interested users. It also enables data transformation through user interface and eliminates the need for replication since data is not moved from the sources physically. Abstraction layer hides the storage structure and technology from the users allowing them to focus on the required tasks. It makes it easy for users to use the data according to their requirements. It brings agility to business decisions as data is readily available. The infrastructure cost is also reduced as the administrator are exempt from operational cost and data duplication. Data integration from cloud sources and on premise databases is also made easy when organizations adopt Data virtualization. It helps in improving services of existing or new products providing speed-to-market value.

Data virtualization enables logical data warehouse functionalities which federates queries across data warehouses and provides data access using different protocols. Business requires real-time and historical data to make decisions leading organizations to adopt different technologies which are designed for special requirements. Having abstraction layer enables collective benefit of their functionalities. Traditional ETL process needs to handle bulk and outdated data from previous operation which is streamlined using Data virtualization [6].

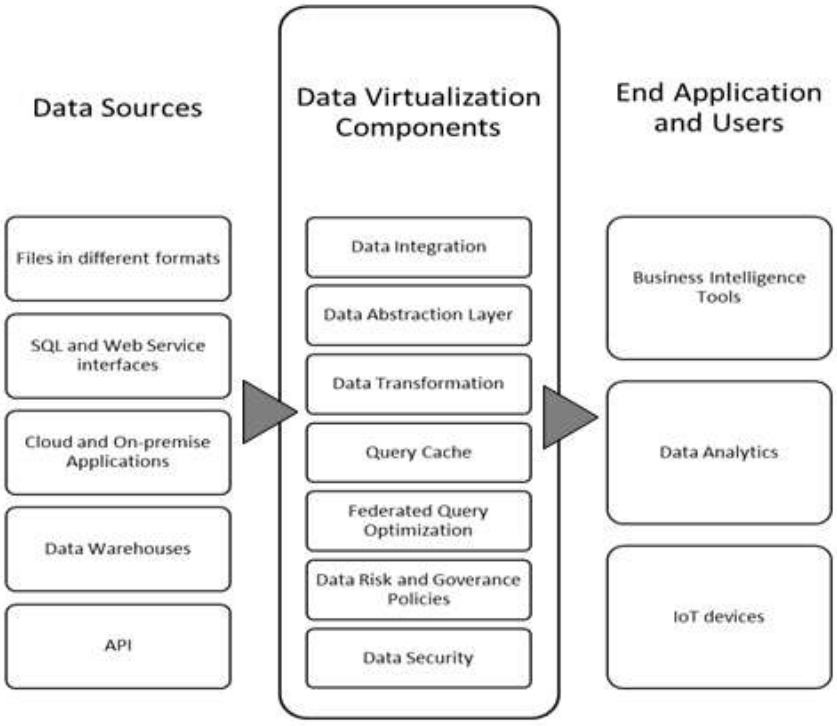


Figure 3: Data Virtualization Overview

Figure 3 shows how Data virtualization integrates different data sources which are soiled and helps in the BI and analytics decision making process.

4. DATA VIRTUALIZATION TECHNIQUES

Data analytics and Business Intelligence help in gaining insight that is been discovered from data integration, data mining and statistical analysis. Most of these technologies depend upon relational databases, data warehouse, BPM, ETL and OLAP cubes. Popular algorithms have been incorporated into data mining systems including K-means, Apriori, AdaBoost, KNN, Support Vector Machine and Page Rank which helps in clustering, classification and association analysis. Data analytics continues to be an active area of research due to Data science and statistical analysis community. The commercial databases show efficiency in query processing and having high level query interface.

Most firms today use Business Intelligence of some form and it involves cost. It depends on what is already installed and the hardware required to upgrade the data warehouse. Software cost involves subscription to various Business Intelligence packages and implementation cost includes initial training and annual software and hardware maintenance costs [7].

ETL and Data virtualization are both data integration tools. Data virtualization is more agile and cost efficient than ETL. Data virtualization computes optimal way to fetch data from different sources and achieve necessary joins and transformations and presents the results to the users without knowing about the location of the data. Data virtualization does not move data from the sources rather it delegates the queries to the source data stores. When requests are issued the data sources are queried in real time and results are returned. Also, they are more agile with the data models where new data stores can be added easily and help in the rapid iteration of project development life cycle. Data virtualization defers costly commitment to ETL process and accelerates the dialog between business users and IT to reduce the risk of an ETL process and help in developing efficient data marts [8].

Data virtualization is a decent choice for Business Intelligence and analytics when structured and unstructured data from dissimilar sources needs to be combined and queried quickly. This is very important for business decisions on inventory levels and portfolio risk analysis. It also helps in eliminating data duplications and privacy risk concerns regarding the data being accessed. The data required for analytics needs to be transformed, undergo cleansing and enriched before it can be used which are done through virtual tables.

Business Intelligence and analytics that traditionally use ETL can extend to include unstructured sources. It can be used to pull data from social media to analyse user behaviour patterns and build recommendation systems. Mobile applications that access corporate data requires a virtualization that separates these applications from the underlying data sources. Mobile applications can access corporate data through REST web services and Data virtualization can adequately help in accomplishing this [9].

Data virtualization helps in building Business Intelligence system from either the existing data warehouse or from disparate data sources virtually. It also helps in pulling data from various components such as CRM and provides an integrated view of data for data analysts and data scientists. This provides flexibility and time-to-value for any business decisions been made. Information governance policies can also be implemented to bring in compliance with industry regulations.

Table 1: Key Characteristics of BI, Technologies and Research

KEY CHARACTERISTICS OF BI	TECHNOLOGIES	RESEARCH
1. Structured data 2. Relational database and data warehouse 3. ETL and OLAP cubes 4. Dashboards and reporting 5. Data mining	1. Cloud Relational Databases 2. Cloud data warehouse 3. Cloud based ETL 4. BPM 5. Clustering 6. Classification 7. Regression analysis 8. Anomaly detection 9. Deep learning 10. Sequencing and Genetic algorithms	1. In-memory analytics 2. Parallel processing 3. Cloud computing 4. Statistical machine 5. Learning 6. Mining IoT data 7. Temporal mining 8. Spatial mining 9. Columnar data stores

Table 2: Data Virtualization and ETL categories

BI & ANALYTICS CATEGORY	DATA VIRTUALIZATION	ETL
1. Time to value	Could be implemented quickly	Takes longer time
2. Requirements	Requirements can evolve	Requirements needs to be well defined before implementation
3. Data cleansing	Generally single pass	Generally multi pass
4. Application use	Tactical decision making based on operational data	Heavy analytical BI and analytics
5. Data formats	Can handle both structured and unstructured data	Mostly limited to structured data
6. Data availability	Available in near real time	Data is available at the end of load operation
7. Data Volume	Depends on the view capabilities	Can process large amount of data

5. CONCLUSION

Data virtualization reduces complexity of data management systems and also provides single consolidated, integrated view of the data. It helps resolve the issue of data silos which are created by multiple applications. Data virtualization abstracts the users from the underlying data sources and allows for real-time data access and brings agility to decision making process. It eliminates the need for replication as data is not moved physically from the source. Finally it is infrastructure agnostic which reduces project life cycle time.

REFERENCES

[1] Chen, Hsinchun, Roger H.L. Chiang, and Veda C. Storey (2012),"Business Intelligence and Analytics: From Big Data to BigImpact,"*Management Information Systems Quarterly*, 36 (4),1165–88

[2] http://web.mit.edu/smadnick/www/wp/2013-10.pdf

[3] https://www.tibco.com/sites/tibco/files/resources/wp-ten-things-data-virtualization-final.pdf

[4] http://www.northtexasdama.org/wp-content/uploads/2017/03/1_Data-Virtualization.pdf

[5] http://www.datavirtualizationblog.com/data-movement-killed-the-bi-star/

[6] https://www.astera.com/type/blog/data-virtualization-technology-overview/

[7] https://globaljournals.org/GJCST_Volume17/3-Emerging-Virtualization-Technology.pdf

[8] https://www.astera.com/type/blog/data-virtualization-technology-overview/

[9] https://www.sciencedirect.com/topics/computer-science/data-virtualization-layer

AN INNOVATIVE APPROACH TO USER INTERFACE ENGINEERING

Pradip Peter Dey[1], Bhaskar Raj Sinha[2], Mohammad Amin[3]and Hassan Badkoobehi[4]

School of Engineering and Computing, National University, San Diego, CA, USA

ABSTRACT

If a computational system is to be successful, it must have an impressive user interface endowed with appealing usability features for providing exceptional user experience. User interface engineering requires an innovative approach because it is one of the most challenging areas given the diversity of knowledge, ideas, skills and creativity needed for building smart interfaces in order to succeed in today's rapidly paced and tough, competitive marketplace.Modern engineering aspects including analytical, intuitive, user experience, artistic, technical, graphical, mathematical, psychological and programming models need to be considered in the development process of a user interface. This paper critically examines some of the past practices and recommends a set of principles for designing alluring user interfaces.It also demonstrates how UML use case diagrams can be improved by naturally relating use cases to user interface elements. The improved design constructs of an enhanced UML view are presented with examples for highlighting and clarifying important user interface engineering issues.

KEYWORDS

Design principles, interface modelling, Unified Modeling Language (UML), usability.

1. INTRODUCTION

User interface design is one of the most challenging areas of software engineering. The challenges of building innovative user interfaces is often considered to be "beyond the reach" of ordinary software developers, particularly, when compared to the repeated achievements of an extraordinary genius such as Steve Jobs of Apple, Inc. Creating great design is not easy [1]. Great software designers have not written much about their innovative design approaches. This is one of the difficulties in understanding and replicating great design techniques [1]. We are not likely to learn much about software design from the design of physical systems such as buildings. "Because software is so malleable, software design is a continuous process that spans the entire lifecycle of a software system; this makes software design different from the design of physical systems such as buildings, ships, or bridges" [2, page-2]. After an initial design is created, software design continues to evolve through iterations, experiments with prototypes, or incremental development. Software complexity is challenging since "it isn't possible to visualize the design for a large software system well enough to understand all of its implementations before building anything" [2, page-2]. An initial software design may have to be revised after the initial development phase when better insights about the complexity of the system becomes evident. The initial user interfaces of the system may play very crucial constructive roles in the formative process. This paper critically examines a number of the past practices and suggests a set of

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 303-314, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90926

principles upon which future innovative user interface engineering can be guided. Every time a human uses a digital product, machine or tool, the interaction takes place through a machine-to-human boundary or interface. If the interface is correctly structured, then the user is likely to have a satisfactory experience which invites the user back again and again. Designing elegant user interfaces for complex computational systems presents daunting challenges [1-9]. The employment of use case analysis in the software development process has been increasingly utilized because use cases help in reducing complex systems to manageable aspects [8, 9]. Usability questions in design are drawing more attention than any others in recent years [1, 8]. Software design, including user interface design, is based on current best practices since practicing engineers have developed useful strategies based on past experiences [1-14]. Support for context-aware user interfaces is evolving to a level where it becomes feasible even in large systems [14]. User interface quality is difficult to assess, and yet, an emergent discipline is attempting to do so [1, 3, 8]. A good user interface is truly appreciated only when it is integrated with smart total system architecture including hardware and software that renders a useful service. User interfaces cannot be considered in isolation from the entire integrated system. Software development has often been considered as one of the most challenging processes of modern technology. Some approach it from a scientific perspective while others treat it in an artistically creative manner. Over the decades, a multitude of approaches to software development have been proposed. These approaches are often described with impressive metaphors. Donald Knuth initially indicated that software writing is an art [15]. David Gries argued it to be a scientific endeavor [16]. Watts Humphrey [17] viewed software development primarily as a process. In recent years, practitioners have come to realize that software is engineered [3-4], [18-23]. As a result of the adoption of engineering methods, software development techniques have evolved and software product quality has steadily improved.

The significance and role of user interface engineering in product design has recently been the focus in many of the highly successful interactive systems [1]. Certain aspects of user interfaces including graphical aspects could not be adequately developed before object oriented programming. Indeed, it has become easier to design and implement a Graphical User Interface (GUI) with object oriented concepts and languages. The Unified Modeling Language (UML) has made significant contributions in representing software design including certain aspects of usability [9]. The UML includes modeling of use case aspects in various views including the use case view [9]. However, the UML does not include modeling and representation of GUI. This paper critically examines important development issues and the UML use case view and proposes an augmented use case view which is more appropriate for modern user interface modelling. It suggests that certain interface elements should be properly included in use case diagrams. It proposes some elements of modeling GUI in an intuitive language similar to UML. In addition, it presents a set of principles for developing innovative user interface features following the suggestions in recent studies [1, 2].

2. DESIGN PROCESS

Although various process models can be found in literature, important modern processes for creatively developing interface-based software are iterative, evolutionary, prototype-based, and agile [2-4], [7], [18-23]. Practitioners have come to realize that a complex system with smart GUI elements cannot be built in one pass. In an iterative process, after requirements analysis, an initial software design is constructed which is then reviewed. Next, the design review may lead to newrequirements analysis which may be revised again on the basis of a combination of software design reviews, new or changed requirements, or other factors which in turn lead to the next software design. That is, the spiral process model [23], or an agile process [2] is found to be a more productive software development process than the traditional processes. Certain aspects of software are such that after an initial analysis and assessment, iterative enhancements lead to

significant progress in the development process. One of the major benefits of the iterative process is the improvements made in the design of user interfaces through successive iterations [25]. The current study is based on the iterative scheme shown in Figure 1, where software design and modeling is followed by design review and evaluation. Figure 1 shows an iterative process of design and review in the central core with solid bold arrows which allows developers to start with a highly abstract conceptual design after an initial requirements analysis. The details can be gradually added in successive iterations. If needed, prototypes can be built and reviewed by stakeholders in order to enhance the design. The dotted arrows show other viable alternatives including iterations over the entire development process. User interface development requires adjustments and refinements that are best done in iterations [2-3], [18-20], [23-24]. Often defects are found during the review or evaluation process and these defects need to be corrected. The design may start with just a few elements with some possible defects; other elements may be incrementally added, and new defects identified may be corrected successively, as practiced in agile processes [2]. The design review may be performed by the designer or by external reviewers, formally or informally.

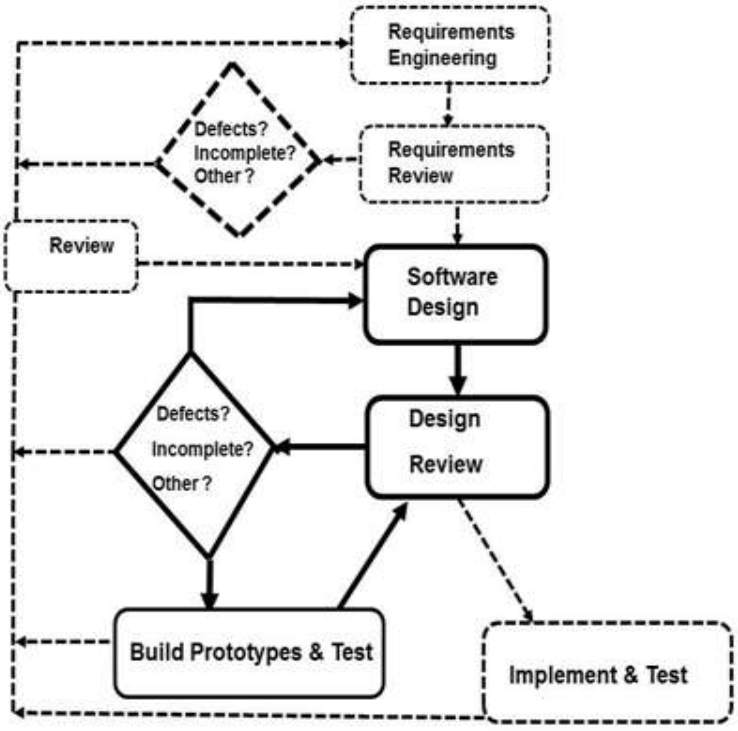


Figure 1: Iterative Design and Review

3. USE CASE VIEW

"Separation of concerns" is a fundamental premise of Software Engineering proposed by Dijkstra[32] and arguably leads to multiple views of a software product. Separation of concerns is usefulto software engineers as long as interactions among system elements are controlled. The authors posit that the segmentation of the whole system into multiple views motivated by separation of concerns should provide an undistorted total picture of the integrated system when the views are put together. However, care must be exercised because multiple views may over simplify the system without accounting for interactions of the system elements. The rules of composition need to be spelled out consistently because the whole picture needs to become clear when the multiple views are composed together in the operational software system. According to UML2.0, there are nine views for describing different aspects of software [9]. The views are: use case view, interaction view, state machine view, static view, design view, activity view,

deployment view, model management view, and profile. A view is generally defined to be a subset of the UML modeling constructs representing certain aspects of the software [9].Each view is thoroughly explained in [9] with one or more diagrams that visually illustrate the main features of the view. The UML use case view is presented with a use case diagram for capturing use case features. The use case view is well-utilized due to the role use cases play in defining requirements analysis and management [8]. It is not appropriately used for user interface design in UML[9] although use cases have a lot to contribute to user interfaces. Use cases can clarify many important software issues early in the development process if they are adequately treated in the engineering process [3, 8, 9]. However, a very narrow definition of use case view is attempted in UML that basically ignores the nature and significance of use cases. "The use case view models the functionality of a subject (such as a system) as perceived by outside agents, called actors, that interact with the subject from a particular view point" [9, page-34]. The perception of the outside agents and interactions mentioned above should be mediated through an interface such as a GUI, especially when the agents are humans. However, UML use case view fails to deal with user interfaces or interfaces between the actors and the use cases. In fact, there is no UML view that adequately deals with GUI features. The diagram that characterizes the use case view is the use case diagram which presents the major use cases in a box with the actors outside the box to indicate that the actors are external users of the current software. One of the central problems with the UML use case diagram is that it totally ignores interfaces with the actors although each actor is shown to be using one or more use cases utilizing a line or association. Interactions among the actors cannot be shown in the same use case diagram. Each use case represent a service which can be illustrated in a UML sequence diagram [9,33]. For illustration purpose, consider a sample use case diagram shown in Figure 2.

The following initial requirements description characterizes the start of a small software project: Develop a software system for computing areas of three types of play-place units: Rectangular, Circular and Triangular. A contractor in Los Angeles builds play-places (with materials such as wood, iron, pads, plastics etc.) at customer site using play place units of different dimensions. The charges are in dollars based on the area of each unit in square feet, plus the number of units. The software system is needed for computing the cost which is based on area. The cost is: $5.00 per square foot. Assume that users always use feet for entering the dimensions of the units. A Graphical User Interface (GUI) is required for user interactions. Additional typical assumptions can be made about this project.

Most software projects start with some fuzzy requirements. Software engineers start their work with an initial requirements analysis. After performing the initial requirements analysis, software engineers may determine that the system must be web-based and should be available 24/7. The access to the system is not required to be restricted with login ID. The system should be easy to maintain using web-based tools. The functional and nonfunctional requirements would be properly analyzed by the engineers. Finally, a software requirements specification (SRS) document would be prepared; it is generally use case driven [8]. The use case diagram for the play-place problem is given in Figure 2 in the standard UML notations [9].

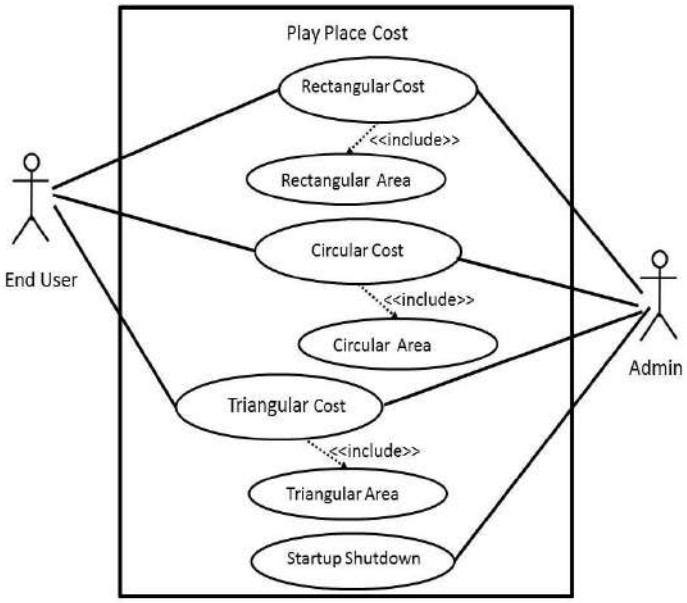


Figure 2: Use Case diagram in UML 2.0

The UML use case diagrams properly show use cases with ovals within the system boundary, represented by a rectangle. One of the issues with a UML use case diagram, such as the one shown in Figure 2, is that it ignores the interfaces between the actors and the use cases although it depicts the actors as stick figures outside the current system boundary. For example, Rumbaugh, Jacobson and Booch [9: page 34] present a use case diagram for a subject called "box office" with four actors without any interfaces. In order to model functionality of the system as perceived by the actors, interfaces appropriate for the given actors need to be depicted in a use case diagram. This research proposes that appropriate interfaces are included in augmented use case diagrams. Thus, the use case diagram given in Figure 3 is recommended for the sample software project mentioned above. It is important to note that the interfaces are shown with dotted rounded rectangles in Figure 3.These interfaces are referred to as the general interfaces in order to distinguish them from specialized interfaces such as provided interfaces and required interfaces mentioned in UML [9, 33].In order to refer to the general interfaces, they are sequentially numbered. If a general interface is to be developed as a part of the current software system, then it is shown within the system boundary; otherwise, it is shown outside the system boundary. As there are many different types of interfaces, some of them need to be marked for their importance. If an interface is a graphical user interface (GUI), then it is marked with the term <<GUI>> utilizing UML stereotypes [9].In addition, when one general interface includes another, it may be marked appropriately. If there is a third general interface that includes the first, then "3 ⊃ 1" can be shown in the third interface.

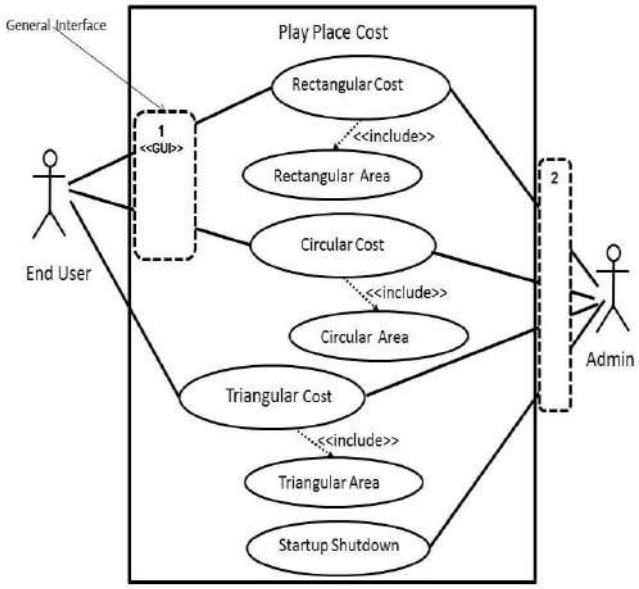


Figure 3. Augmented Use case diagram with general interfaces

Having general interfaces in the use case diagram intuitively and logically supports the idea that user's perception about the functionality is modeled appropriately in the augmented use case view. When the actor is a human user, the general interface may be a GUI for appropriate interactions between the user and the system. For interactive systems, addition of GUIs to a use case diagram helps in understanding the perceived functionality of the system. It is the role of GUIs that is not adequately detailed in the UML modeling techniques leading to a high degree of confusion for the development of modern interactive systems.

In addition to use case diagrams, the augmented use case view should have general interface diagrams. Without such a diagram concerns about user interfaces are grossly ignored and interactions among system elements are not appropriately accounted for. Without interface diagrams, the standard UML [9] misses information vital to the success of a modern software system. It also misses to give a comprehensive account of the software which is expected to be a composition of the standard UML views. It is reasonable to be flexible about the notations of the general interface diagrams, especially if they are GUIs. Two main alternative notations for the general interface diagram are (1) screen shots from a prototype, and (2) abstract graphical representation of major interface elements. We show the former notation in the general interface diagram given in Figure 4 for the general interface 1 of Figure 3. That is, we developed a prototype GUI applet using the Java programming language for the sample problem of play-place units mentioned above in section 3 and took a screen shot of the GUI for Figure 4. It is to be assumed that through each subsequent iteration the GUI applet of Figure 4 will evolve and acquire better qualities.

Figure 4: General interface diagram

The general interface diagrams such as the one shown in Figure 4 should be considered important for software design purposes. Jason Hong [1] asks an important question: "how do we effectively incorporate great design into products?" Currently, we cannot incorporate GUI design into standard UML based techniques. The role of the UML in modeling can be enhanced by appropriately accounting for the perceived functionality of a system by providing the augmented use case view along with general interface diagrams. This is true because the augmented use case view includes general interfaces in its use case diagram between the actors and the use cases. The perceived functionality is evident perceived by the actors as it passes through the general interfaces.

The balance between abstraction and details can be appropriately achieved in the general interface diagram as the interface elements can be added incrementally. "Software engineers and programmers are often competent users of the technology . . . All too often, however, they do not use this technology in an appropriate way and create user interfaces that are inelegant, inappropriate and hard to use" [4]. The augmented use case view puts extra emphasis on modeling user interfaces. This promotes focusing on many other aspects of user interfaces such as maintaining input mechanisms the same throughout the application. Nobody should argue that interfaces are adequately treated in the UML design view and that augmentation of the use case view is not required, because the design view simply places the provided and required interfaces with their appropriate components. Extra emphasis is needed for showing the details of interfaces of certain types such as GUIs. Modeling GUIs for interactive systems has become increasingly important in the past two decades [1, 2, 7, 26]. Separation of concerns [27] motivates modular

design where a software system is decomposed into components; however, well-defined interfaces need to be specified among the components. GUIs may be required for human interactions with the components. The main confusion with the UML is that its presentation of software aspects totally disregards GUIs. A visual modeling language such as the UML cannot achieve its major goals without appropriate attention to GUI design. In addition, software engineering education with the UML requires guidance for learners so that different views together would be able to define the complete software system compositionally. Due to missing elements such as GUIs, the UML provides a fragmentary view of the software which is inadequate for any account of the integrated whole system. The proposed augmented use case view is designed to fill the gap. Reasoning with the augmented use case view is better than with traditional use case view, because the functionality of the system, as perceived by the actors, is more reasonable by including the general interfaces mentioned above. Engineering practices and design activities with the general interface constructs may also encourage and promote learning about user interfaces which is valuable for students in educational settings and academic environments.

4. UI DESIGN PRINCIPLES

In this section, we propose a set of design principles for developing user interfaces. Jason Hong [26] observes that "Apple tends to **design by principle** rather than from data." Human Computer Interaction (HCI) data along with use case scenarios may help in understanding some aspects of user interfaces. However, these may not help much if the goal of the design is to present an innovative solution to exceed all expectations. HCI data are useful for accomplishing the more modest goal of "meeting expectations". Advanced design principles along with effective strategies may lead to innovative user interface design. The following user interface design principles include the principles discussed by Hong [26] in the context of Apple, plus others that we found to be valuable for innovative solutions.

1. Examine promising alternatives from the widest range of possible alternatives in order to provide the best user experience through integration of various features including hardware, software, artistic, mathematical and intuitive aspects.
2. Let subject matter experts play a leading role in all phases of the design.
3. Utilize Object Oriented Design concepts throughout the development process.
4. Push the design-review-design cycle to its limits.
5. Consider separation of concerns in order to deal with all interactions among system elements.
6. Consider design principles as well as HCI data and user experience for innovative user interface solutions.
7. Include only those action features which are intuitively learnable; transform others to this category or to an automated category.
8. Maximize cohesion and minimize coupling among components.
9. Include error prevention and simple error handling.
10. Present user interface design at multiple levels of abstraction

For innovative user interface solutions, designers need to consider unusual alternatives in addition to the obvious ones. With reference to principle 1 suggested above, it is important to mention that quick design under time pressure leads to consideration of only a few obvious alternatives

missing innovative but unapparent alternatives. Apple came up with brilliant user interface solutions that were missed by others in the same field.

Principle 2 is thoroughly discussed by Hong [26] with an example where contributions of subject matter experts are explained with an example of an experienced photographer. Experienced subject matter experts would be able to adequately explain what will, or will not, work in a given context.

Principle 3 suggests that object oriented design concepts [2, 3, 34] need to be utilized throughout the iterative development process. Object oriented design elements such as buttons, windows, allow fast development cycles.

Principle 4 suggests that improvements can be achieved by repeating the design-review-design cycle for a complex system. We have suggested an iterative design-review-design cycle as shown in Figure 1. Through an iterative process a designer may exhaustively explore many alternatives by critically examining her own designs.

Principle 5 is based on a traditional strategy for dealing with complexity [2-4]. The complexity of a system becomes increasingly difficult if the degree of interactions among its elements become unpredictable. As the concerns are separated, their relations become properly understood and, consequently, their interactions become predictable.

Principle 6 is based on a commonsense integration of HCI factors [27-29], user experience, and other advanced design principles [26]. A good study of user groups helps in the understanding of user interface aspects which may stimulate innovative user interface constructs [27], [28], [30].
Principle 7 basically suggests that users should not be burdened by difficult learning tasks. If there are tasks that are not easy to learn, the designer should try to automate them as much as possible.

Principle 8 is discussed in most textbooks [1, 2]; it is related to Principle 4 because loosely coupled systems have advantages over tightly coupled systems. Interactions among components of a tightly coupled system are often unmanageable.

The idea of Principle 9 is based on Ben Shneiderman's suggestion [27] that when users are prone to make errors, an automated or easy recovery process should be used to prevent the error from occurring.

Principle 10 makes sure that design is expressible in multiple levels of abstraction without significant loss of clarity. When one level of abstraction is transformed into another level, consistent interpretations should be applicable. Presenting user interfaces in multiple levels makes sure that no inconsistencies exist. In addition, the gap between high level design and low level design should be eliminated in the final phase. It is to be noted that the proposed design principles do not contradict with the various versions of the UML [9], [32] or the enhancements suggested above. The proposed design principles combined with augmented use case view have great potentials for smart user interface design.

5. CONCLUSION

As user interfaces become increasingly important, a set of principles that direct selective iterative design techniques are considered helpful in developing an innovative approach towards user interface engineering. The set of principles proposed in this paper may provide sufficient clarity about the nature of innovations that are achievable through user interface engineering activities.It

is reasonable to expect that various aspects of user interface modeling and design might be, procedurally, systematically reviewed and revised in an iterative evolutionary process that spans the entire lifecycle of a software system. In addition, the UML use case view is reviewed and suggestions are made for augmenting the use case view. Research of user experience (UX) is a critical component of use case development [31]. The enhancements suggested in this paper are most applicable in dealing with GUI aspects that are missing in the standard UML [9].Without GUI related constructs, the UML appears to be deficient and, therefore, the addition of general interface diagrams is suggested. This addition significantly enhances software modeling in UML. Design techniques suggested here have the potential to help in the development of smart user interfaces.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the help and/or encouragements received from John Cicero, James Jaurez, Arun Datta, Gordon Romney and many others during the preparation of this paper and the research reported in it.

REFERENCES

[1] Hong, J. (2010) “Why is Great Design so Hard?” Communications of the ACM, July 2010.

[2] Ousterhout, J. (2018) A Philosophy of Software Design, Yaknyam Press.

[3] Pressman, R. & Maxim, B. (2015) Software Engineering: A Practitioner's Approach, 8th edition, McGraw-Hill.

[4] Sommerville, I. (2010) Software Engineering, 9th Edition, Addison Wesley.

[5] Wang, Y. (2008) Software Engineering Foundations: A Software SciencePerspective,Auerbach Publications.

[6] Shaw, M. & Garlan, D. (1995) “Formulations and Formalisms in Software Architectures”, Computer Science Today: Recent Trends and Developments, Springer-Verlag LNCS, 1000, 307-323, 1995.

[7] Braude, E. & Bernstein, M. (2011) Software Engineering: Modern Approaches, (2nd Edition), John Wiley & Sons.

[8] Leffingwell, D. & Widrig, D. (2003) Managing Software Requirements: A Use Case Approach, Addison Wesley.

[9] Rumbaugh, R. Jacobson, I. & Booch, G. (2005) The Unified Modeling Language Reference Manual. (2nd Edition), Addison Wesley.

[10] Baniassad, E., Clements, P., Araujo, J., Moreira, A., Rashid, A. & Tekinerdogan, B. (2006) “Discovering Early Aspects,” IEEE Software, 2006.

[11] Krechetov, I., Tekinerdogan, B. & Garcia, A. (2006) “Towards an integrated aspect-oriented modeling approach for software architecture design,” 8th Aspect-Oriented Modeling Workshop, Aspect-Oriented Software Development (AOSD) 2006.

[12] Navasa, A. Pérez, M. A., Murillo, J. M. & Hernández, J. (2002) “Aspect Oriented Software Architecture: A Structural Perspective,” Proceedings of the Aspect-Oriented Software Development (AOSD), 2002.

[13] Azevedo, J. L., Cunha, B. & Almeida, L. (2007) "Hierarchical Distributed Architectures for Autonomous Mobile Robots: A case study", Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation, 2007.

[14] Cerny, T., Cemus, K., Donahoo, M. & Song, E. (2013) "Aspect-driven, Data-reflective and Context-aware User Interfaces Design", ACM SIGAPP Applied Computing Review, volume 13(4), page 53-65, 2013.

[15] Knuth, D. E. (1969) Seminumerical Algorithms: The Art of Computer Programming 2. Addison-Wesley, Reading, Mass.

[16] Gries, D. (1981) The Science of Programming. Springer, 1981.

[17] Humphrey, W. (1989) Managing the Software Process, Reading, MA. Addison-Wesley.

[18] Pfleeger, S. & Atlee, J. (2010) Software Engineering, Prentice-Hall.

[19] Agarwal, B., Tayal, S. & Gupta, M. (2010) Software Engineering and Testing, Jones and Bartlet.

[20] Tsui, F. & Karam, O. (2011) Essentials of Software Engineering, 2nd Ed., Jones and Bartlet.

[21] Bass, L. Clements, P. & Kazman, R. (2003) Software Architecture in Practice, 2nd Edition, Addison-Wesley.

[22] Miller, J. & Mujerki, J. Editors, (2003) MDA Guide, Version 1, OMG Technical Report. Document OMG/200-05-01, http://www.omg.org/mda

[23] Boehm, B. (1986) "A Spiral Model of Software Development and enhancement," ACM SIGSOFT Software Engineering Notes, ACM, 11(4):14-24, 1986.

[24] Dey, P. P, Sinha, B. R., Amin, M. & Badkoobehi, H. (2012) "Augmenting Use Case View for Modeling", World Academy of Science, Engineering and Technology, Vol.6 (12), pages 1318-21.

[25] Nielsen, J. (1993) "Iterative User Interface Design," IEEE Computer vol.26 no.11 pp 32-41, 1993.

[26] Hong, J. (2010) "Why is Great Design so Hard (Part Two)?" Communications of the ACM, August 2010.

[27] Hursch, W. L. & Lopes, C. (1995) "Separation of Concerns", Technical Report, Northeastern University.1995, Retrieved, July11, 2014 fromftp://ftp.ccs.neu.edu/pub/people/lieber/crista/techrep95/separation.pdf

[28] Shneiderman, B., Plaisant, C., Cohen, M. & Jacobs, S. (2009) Designing the User Interface: Strategies for Effective Human-Computer Interaction (5th Edition), Prentice Hall.

[29] Tidwell, J. (2011) Designing Interfaces, O'Reilly, 2nd Edition.

[30] Nielsen, N. Gr. (2019) Why User Interviews fail? Retrieved June 14, 2019 from www.nngroup.com

[31] Loranger, H. (2014) UX Without User Research is not UX, retrieved April 14, 2015 from http://www.nngroup.com/articles/ux-without-user-research/

[32] Dijkstra, E. W. (1974) "On the role of scientific thought ", Retrieved August 15, 2015, from https://www.cs.utexas.edu/users/EWD/transcriptions/EWD04xx/EWD447.html See also Effective Software Design, IASA Israel Meeting, retrieved April 12, 2019 from http://effectivesoftwaredesign.com/2012/02/05/separation-of-concerns/

[33] Agile Modelling, (2019) Introduction to the Diagrams of UML 2.X, retrieved April 14, 2019 fromhttp://www.agilemodeling.com/essays/umlDiagrams.htm

[34] Ambler, S. (2004) The Object Primer: Agile Model-Driven Development with UML 2, 3rd Edition.Cambridge University Press

AUTHORS

[1]**Dr. Pradip Peter Dey** is a Professor at National University, 3678 Aero Court Dr., San Diego, CA, 92123, USA. He primarily teaches in the MS in Computer Science program, School of Engineering and Computing. His research interests are computational models, software design, mathematical reasoning, visualizations, User Interfaces and Computer Science education. Phone: 858-309-3421; email: pdey@nu.edu.

[2]**Dr. Bhaskar Raj Sinha** is a Professor at National University, 3678 Aero Court Dr., San Diego, CA, 92123, USA. Dr. Sinha has more than 25 years of research and teaching experience in industry and academia. His interests are in Mathematical Reasoning, Digital Systems, Computer Architecture, Technology Management, and Engineering Education. Phone: 858-309-3431; email: bsinha@nu.edu.

[3]**Dr. Mohammad Amin** is with National University, 3678 Aero Court Dr., San Diego, CA, 92123, USA. He is a Professor and Academic Program Director for the Master's degree program for the MS in Electrical Engineering program, School of Engineering and Computing. His major research interests are computational modelling, wireless communications, databases, sensors and engineering education. Phone: 858-309-3422; email: mamin@nu.edu.

[4]**Dr. Hassan Badkoobehi** is with National University as a Professor in the School of Engineering and Computing at 3678 Aero Court Dr., San Diego, CA, 92123, USA. His major research interests are engineering education, environmental engineering, mathematics and statistical reasoning. Phone: 858-309-3437; email: hbadkoob@nu.edu.

ATTRIBUTE REDUCTION AND DECISION TREE PRUNING TO SIMPLIFY LIVER FIBROSIS PREDICTION ALGORITHMS A COHORT STUDY

Mahasen Mabrouk[1], Abubakr Awad[2], Hend Shousha[1], Wafaa Alakel[1,3], Ahmed Salama[1], Tahany Awad[1]

[1]Endemic Medicine and Hepatology Department, Faculty of Medicine, Cairo University, Cairo, Egypt
[2]School of Natural and Computing Sciences, University of Aberdeen, Aberdeen, UK
[3]National Hepatology and Tropical Medicine Research Institute, Ministry of Health and Population, Cairo, Egypt

ABSTRACT

Background: *Assessment of liver fibrosis is a vital need for enabling therapeutic decisions and prognostic evaluations of chronic hepatitis. Liver biopsy is considered the definitive investigation for assessing the stage of liver fibrosis but it carries several limitations. FIB-4 and APRI also have a limited accuracy. The National Committee for Control of Viral Hepatitis (NCCVH) in Egypt has supplied a valuable pool of electronic patients' data that data mining techniques can analyze to disclose hidden patterns, trends leading to the evolution of predictive algorithms.*

Aim: *to collaborate with physicians to develop a novel reliable, easy to comprehend noninvasive model to predict the stage of liver fibrosis utilizing routine workup, without imposing extra costs for additional examinations especially in areas with limited resources like Egypt.*

Methods: *This multi-centered retrospective study included baseline demographic, laboratory, and histopathological data of 69106 patients with chronic hepatitis C. We started by data collection preprocessing, cleansing and formatting for knowledge discovery of useful information from Electronic Health Records EHRs. Data mining has been used to build a decision tree (Reduced Error Pruning tree (REP tree)) with 10-fold internal cross-validation. Histopathology results were used to assess accuracy for fibrosis stages. Machine learning feature selection and reduction (CfsSubseteval / best first) reduced the initial number of input features (N=15) to the most relevant ones (N=6) for developing the prediction model.*

Results: *In this study, 32419 patients had F(0-1), 25073 had F(2) and 11615 had F(3-4). FIB-4 and APRI revalidation in our study showed low accuracy and high discordance with biopsy results, with overall AUC 0.68 and 0.58 respectively. Out of 15 attributes machine learning selected Age, AFP, AST, glucose, albumin, and platelet as the most relevant attributes. Results for REP tree indicated an overall classification accuracy up to 70% and ROC Area 0.74 which was not nearly affected by attribute reduction, and pruning . However attribute reduction, and*

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 315-326, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90927

tree pruning were associated with simpler model easy to understand by physician with less time for execution.

Conclusion: *This study we had the chance to study a large cohort of 69106 chronic hepatitis patients with available liver biopsy results to revise and validate the accuracy of FIB-4 and APRI. This study represents the collaboration between computer scientist and hepatologists to provide clinicians with an accurate novel and reliable, noninvasive model to predict the stage of liver fibrosis.*

KEYWORDS

Liver Fibrosis, Data Mining, Weka, Decision Tree, Attribute Reduction, Tree Pruning.

1. INTRODUCTION

Hepatitis C virus (HCV) is a worldwide etiology of chronic hepatic infection particularly in Egypt where genotype 4 being responsible for >90% of cases, and the remaining is due to genotype-1 [1, 2]. The natural history of chronic hepatitis C (CHC) infection passes through consecutive steps of progressive fibrosis, hepatic cirrhosis that decompensates into end-stage liver disease and the dismal malignancy of Hepatocellular carcinoma (HCC) [3]. The gold standard for staging liver fibrosis remains percutaneous liver biopsy, which is an invasive procedure [4]. Fibroscan ultrasonography is non-invasive and reliable methods for diagnosis of the stage of liver fibrosis, compared to liver biopsy [5]. The Aspartate aminotransferase-to-platelet ratio index (APRI), and FIB-4 scores are simple, noninvasive, easy to perform, inexpensive and reproducible algorithms for diagnosing advanced fibrosis stages [5–7], but they are not consistently accurate in classifying fibrosis stages [8].

1.1. MOTIVATION AND AIM

Medicine involves decision making and classification or prediction is an important part of it. However, medical classification or prediction is usually a very complex and hard process. Human reasoning even of expert clinician could not deal with highly dimensional criteria of health care data, their underlying associations, and predictive capability. In Egypt, the NCCVH program has provided a valuable pool of demographic and laboratory data which can lead to information discovery, making good use of the data stored in EHRs of CHC patients and the conducting large population based researches.

Most of medical studies rely on statistical analysis and to a much less extent on machine learning. Even those studies which consider machine learning are usually defective in the medical aspects and are complex or difficult to comprehend by physicians. This study represents a multi-disciplinary approach between hepatologists and health informatics researchers to develop a novel, reliable, and non-invasive model to predict the stage of liver fibrosis based on routine workup, without imposing extra costs for additional examinations especially in areas with limited resources like Egypt. Further we use machine learning attribute reduction and decision tree pruning to simplify the model to be easily understood by physicians.

1.2 OUR CONTRIBUTION

I. To our knowledge this study enrolled the largest sample size of CHC patients with available histopathological results. This chance will not be repeated with the new era of directly acting antiviral therapy which did not necessitate liver biopsy.

II. This study represents collaboration between physicians and medical informatics people to overcome the complexity of Machine Learning algorithm, and to provide easy to comprehend model using ML tools as feature reduction, and decision tree pruning.

III. This study provides a chance to re-validate the diagnostic accuracy of the famous and widely used FIB-4 and APRI. Further we use the power of data mining to explore this large volumes of data stored in electronic health records to discover hidden patterns and relationships to provide more accurate model for prediction of advanced liver fibrosis.

1.3 RELATED WORK

Data mining is a reliable method of predictive analysis which explores tremendous volumes of data to discover hidden patterns and relationships in highly complex dataset. Data mining differs from classical statistical analysis in that statistical inference in its hypothesis testing sense may not be appropriate, and the questions asked may not be applicable to large datasets. In most applications of data mining, there is no a priori reason to sample and all attributes of data is readily available for exploratory questions. Thus, it can enable the development of predictive models.

Decision trees are the recommended approach for building comprehensible clear predictive models, which are simple and quick to build with adequate accuracy. Conversion of decision trees into classification rules is easy. They do not require any domain knowledge and easy to assimilate by physicians. The main benefit of decision trees over logistic regression analysis is that decision trees are easy to understand [9]. The simple allocation of patients into subgroups by following the flowchart design could define the anticipated possibility of outcome [10].Prognostic factors of different diseases have been defined using decision trees.

In previous work we implemented Data mining analysis explores data, and trends that enable the development of models to diagnose HCC [11, 12], the prediction of therapeutic outcome of HCV patients utilizing simple laboratory data [13]. We further addressed the issue of performance evaluation of decision tree classifiers, where we assessed the correctly classified instances, recall, precession, and area under the curve [14]. Hashem, et al. used the decision tree learning algorithm to provide an accurate prediction of advanced Liver fibrosis in CHC [15].

2. PATIENTS AND METHODS

This retrospective multi-center study included 69106 Egyptian patients with CHC who were naive candidates for antiviral therapy registered by The Egyptian National Committee for Control of Viral Hepatitis in the period from January 2010 till December 2014. A local ethical committee approval was available before starting data collection. With respect to patient's confidentiality, all patients were represented in the study by code numbers after concealing all their personal data. The protocol of the study conformed to the ethical guidelines of the 1975 Declaration of Helsinki. Knowledge discovery of useful information from Electronic Health Records EHRs of a cohort of

69106 patients necessitates putting high quality data. characterized by accuracy, integrity, completeness, validity, consistency, uniformity and uniqueness.

This is a multistep process, composed of the following primary activities:

- Data collection pre-processing, cleansing and formatting.
- Data auditing and statistical analysis.
- Feature selection and reduction to minimize the dimensionality of the problem.
- Selecting appropriate mathematical models to represent the trends.
- Evaluating the selected models.

2.1. DATA COLLECTION, CLEANSING AND FORMATTING

Knowledge discovery of useful data from EHRs of a standardized recruitment questionnaire was completed by CHC patients physicians that included demographic features (age, gender, body mass index (BMI), Complete blood count (CBC), Liver biochemical testing (alanine aminotransferase (ALT), aspartate aminotransferase (AST), alkaline phosphatase, Serum bilirubin, albumin and INR), blood glucose, and Serum creatinine and alpha fetoprotein (AFP), thyroid stimulating hormone (TSH), antinuclear antibody (ANA), and HCV quantitative real time polymerase chain reaction (Abbot Real Time, detection limit 30 (IU/ml). In addition to their histopathological data where liver biopsy was mandatory for fibrosis assessment in the interferon era. Metavir scoring system of fibrosis F0-F4 was used as a gold standard to assess accuracy for the stage of fibrosis.

The information was largely collected from medical notes and checked for completeness and correctness. Finally, data were entered onto a computer database (in the form of excel sheets) by a person with paramedical training then it was transformed to a standard relational database management system. All laboratories undergone proper quality control measures to ensure validity of their results. Data cleansing is detecting and adjusting (or removing) corrupt or inaccurate patients' records from a record set in addition to excluding of typographical errors or validating and correcting values against a known list of entities. If inconsistencies were found or necessary corrections were needed, the form/s was returned to the physician for revision. The identified inappropriate parts of the data may be replaced, modified or deleted. High quality data needs to be characterized by accuracy, integrity, completeness, validity, consistency, uniformity and uniqueness. Data transformation techniques were used to format and prepare the patient records to be processed by the learning algorithms. Each attribute was classified as numerical or categorical then validated, to setup high quality valid consistent data.

2.2. DATA AUDITING AND STATISTICAL ANALYSIS

Numerical data are reported as means ± standard deviation (S.D). Categorical data are represented as counts and percentages. The student t-test and the Chi-square test are used when appropriate. Statistical significance is considered if the probability of occurrence by chance is 5% or less ($P<0.05$). Statistical analysis was used for cross tabulation, and estimation of sensitivity, specificity, positive predictive value, negative predictive value and ROC curves.

2.3. FEATURE SELECTION AND REDUCTION

In this stage we aim to reduce the initial number of input features (N=15) to the most relevant ones (N=6) for developing the prediction model. Attributes that showed statistically significant correlation with F2-F4 stages of fibrosis were used to create a decision tree to predict liver fibrosis stage. However, using such statistical based approaches for feature selection may impair classification performance. To avoid the limitations of statistical based techniques for feature selection, we used correlation based Feature Sub-set Selection for Machine Learning (CfsSubsetEval) to evaluate the worth of a subset of attributes through considering the individual predictive ability of each feature along with the degree of redundancy between them. The second step is searching the space of attribute subsets by greedy hill climbing augmented with a backtracking facility. Best first may start with the empty set of attributes (forward search), or start with the full set of attributes (backward search), or start search at any point in both directions [16].

2.4. SELECTING APPROPRIATE MATHEMATICAL MODELS TO REPRESENT THE TRENDS

Reduced Error pruning tree (REP tree) is considered a fast decision tree learner that builds a decision/regression flowchart using information gain/variance and prunes it using reduced error pruning. The Weka program can be used for testing data sets using a variety of open source Machine Learning algorithms. The workbench includes methods for all the standard data mining problems e.g. clustering, association rule mining, regression, classification, and attribute selection. In addition, it involves a variety of tools for converting, pre-processing datasets, feed it into a learning scheme, and analyse the resulting classier and its performance. Weka is available from http://www.cs.waikato.ac.nz/ml/weka.

2.5. PERFORMANCE EVALUATING THE SELECTED MODELS

The performance of decision trees built using all attributes was compared to those built after attribute reduction. The calculated algorithm was validated using the k-fold cross-validation approach. In brief, we divided the original sample into k sub-samples. The cross-validation process was repeated k times (folds). Each of the k sub-samples was used once as the validation data [17]. We assessed the performance of algorithm according to evaluation matrix based on values for the correctly classified instance, precision (specificity), recall (sensitivity), and Receiver operating characteristic (ROC) curve.

3. RESULTS

To our knowledge this multi-centered registry study has the largest sample size (69106 HCV patients) with liver biopsy histo-pathological results. The patients were divided according to their Metavir scores into, 32419 patients (46.9%) with minimal fibrosis stages (F0-F1) and F2 in 25073 patients (36.3%), and advanced fibrosis (F3-F4) in 11615 patients (16.8%). The demographic and laboratory features and statistical differences between the studied groups (F0-F2 / F3-F4) are shown in Table 1 arranged according to their significance. Male patients

represented 71.8% (49618 patients) of the study population. There was a statistically significant difference between the 2 groups in terms of their age, body mass index (BMI), platelet count, white blood cell count(WBCs) , AFP, AST, serum bilirubin , albumin and alkaline phosphatase.
All the 15 attributes used for liver fibrosis prediction were presented as categorical or numerical, and arranged according to statistical significance (p-value) and their weight as shown in Table 2. Using machine learning attribute selection these attributes were reduced to six attributes namely Age, AFP, AST, glucose, albumin, and platelet that proved to be the most relevant attributes.

In our study, FIB-4 and APRI diagnosed advanced fibrosis (F3-F4) with a good negative predictive value and high specificity which is comparable to the original study, but low positive predictive value and with poor sensitivity. Patients with advanced fibrosis were not diagnosed and there was a great discordance between FIB-4 and APRI compared to liver biopsy results. The correctly classified F3-F4 patients were 57.5% and 13.9% for cut-off value ≥ 1.45 and ≥ 3.25 receptively. The results of APRI test showed poor diagnostic abilities and only 32.7% F3-F4 patients were correctly classified at cut off value ≥ 1.

This high discordance in our study between the actual results of liver biopsy and the other two tools APRI and FIB-4 with overall AUC 0.58 (Figure 1) and 0.68 (Figure 2) respectively, has provided us the motivation of using data mining techniques to find a new non-invasive predictive algorithm. Machine learning techniques such as Decision Trees (classification trees) have been used for prediction, classification, and as diagnostic tools.

able 1. Baseline characteristics of the study population.

Attribute	**F 0-1**	**F 2-4**	**P-value**
Age	37.31 ± .073	43.13 ± .067	.0001
BMI	26.11 ± .02	27.04 ± .02	.0001
Platelets	221.14 ± .34	203.95 ± .34	.0001
AFP	5.99 ± .14	9.60 ± .20	.0001
Fasting blood glucose (mg/dL)	102.0 ± 27.9	110.6 ± 38.0	.001
Total Bilirubin (mg/dl)	0.84 ± .02	1.47 ± .34	.002
Albumin (g/dL)	4.38 ± .002	4.30 ± .002	.003
AST (IU/L)	50.44 ± .35	51.52 ± 1.47	.018
WBC (x1000)	6.4 ± .01	6.44 ± .01	.028
Alkaline Phosphatase (IU/L)	113.54 ± .41	118.31 ± 1.68	.035
Serum Creatinine (mg/dl)	0.85 ± 0.2	1.04 ± 0.4	.200
Hb (G/L)	13.87 ± .009	13.89 ± .008	.340
ALT (IU/L)	86.51 ± 29.4	118.87 ± 63.31	.371
HCV RNA (IU/M)	$22\times10^5 \pm 27\times10^4$	$24\times10^5 \pm 40\times10^4$	.442

Table 2. Features selection for prediction of advanced fibrosis F3-4.

	Attribute	Represented as	Statistical sig (P-Value)	Attribute weight	ML selection
1	Gender	Categorical	.021	0.00243	No
2	Age	Numeric	.0001	0.05968	Yes
3	BMI	Numeric	.0001	0.02108	No
4	Hb (G/L)	Numeric	.340	0.00153	No
5	WBC (x1000)	Numeric	.028	0.00129	No
6	Platelets	Numeric	.0001	0.05351	Yes
7	Total Bilirubin (mg/dl)	Numeric	.002	0.02191	No
8	Albumin (g/dL)	Numeric	.003	0.01682	Yes
9	AST (IU/L)	Numeric	.018	0.02399	Yes
10	ALT (IU/L)	Numeric	.371	0.02456	No
11	Alkaline Phosphatase (IU/L)	Numeric	.035	0.00475	No
12	Fasting blood glucose (mg/dL)	Numeric	.0001	0.01436	Yes
13	AFP	Numeric	.0001	0.06157	Yes
14	HCV RNA (IU/M)	Numeric	.442	0.00773	No
15	Serum Creatinine (mg/dl)	Numeric	.043	0.00191	No

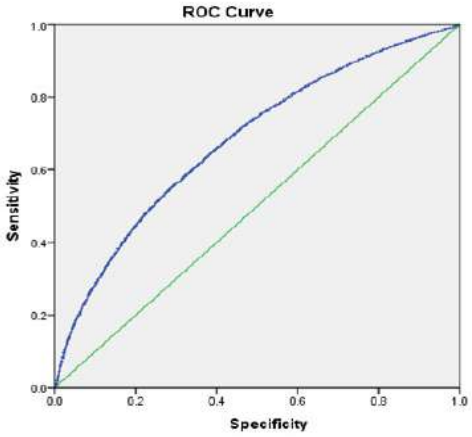


Figure 1. FIB-4 ROC Curve

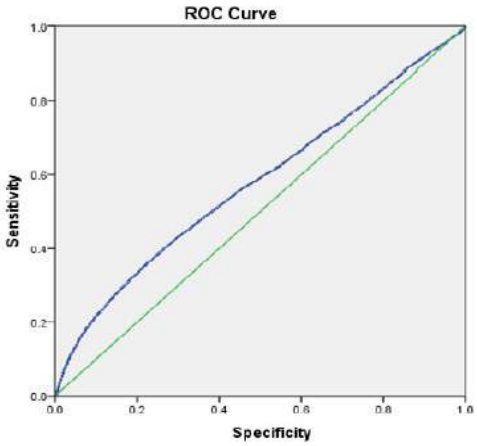


Figure 2. APRI ROC Curve

At first we applied REPTree as a predictive algorithm using all the 15 attributes. This decision tree model showed that AFP level was selected as the variable of initial split (most decisive), with optimal cut-off value of ≤ 6.55ng/mL. Age is the next decisive splitting attribute with optimal cut-off value of ≤ 38.5 years, platelet count with optimal cut-off value of ≤ 181.5, other attributes as AST, ALT, glucose, BMI, albumin, bilirubin, and INR have less decisive role for prediction of

fibrosis (Figure 4). Patients with significant liver fibrosis were significantly older in age, higher AFP levels and lower platelet counts.

Results indicated an overall classification accuracy about 67% and ROC Area 0.74 for REPtree (Figure 3), which was not affected by attribute reduction. This model was further simplified by attribute reduction using only the six attributes selected using machine learning as shown in table 2. The diagnostic performance analysis of advanced fibrosis F3F4 of the various prediction models clearly shows that the diagnostic power of REPtree over exceeds the two popular models APRI and FIB-4 (Table 3). This simple easy to comprehend prediction model could be provided to doctors so they can know the probability of stage of fibrosis by entering simple data as age, AFP, and platelet.

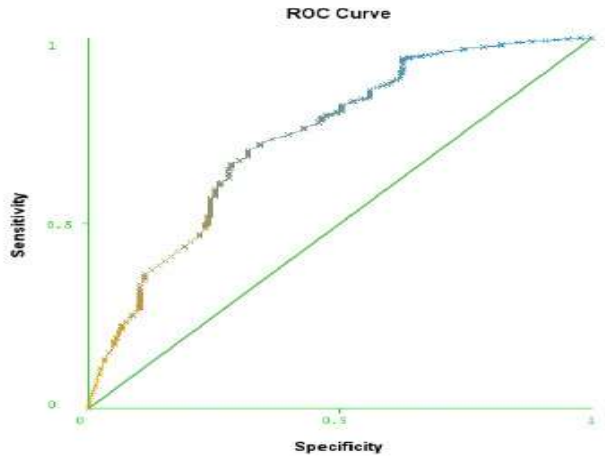


Figure 3. FIB-4 ROC Curve

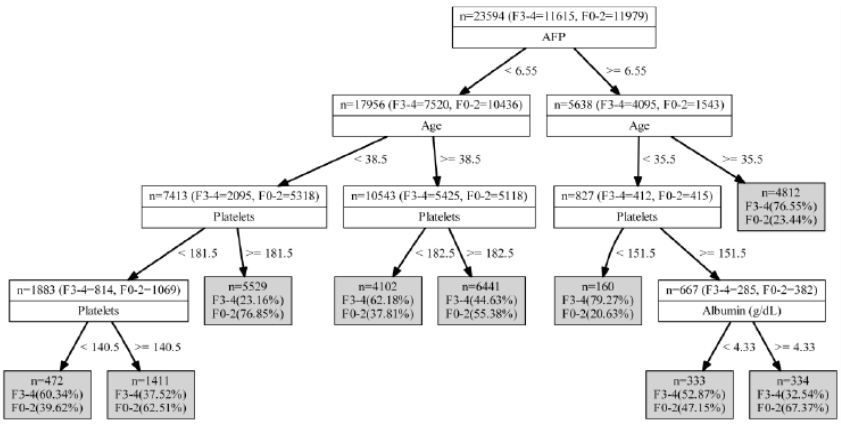


Figure 4. Decision tree (REPTree) to predict liver fibrosis.

Table 3. Diagnostic performance of advanced fibrosis F3-4 prediction models.

	REPTree	**REPTree pruned**	**REPTree**	**REPTree pruned**	**FIB-4 >1.45**	**FIB-4 >3.25**	**APRI >1**
Attributes	15	15	6	6	**4**	4	2
Time(sec)	1.68	0.21	0.6	0.1	-	-	-
Tree Size	88.3	17	875	17	-	-	-
Correctly Classified%	68.1%	70%	66.4%	67.3%	57.5%	13.9%	32.7%
TP Rate	66.4%	61.9%	62.6%	60.8%	27.62%	45.16%	25.13%
FP Rate	30%	28.3%	29.9%	26.5%	88.55%	84.30%	85.81%
Precision	68.1%	68%	67%	69%	68.58%	96.48%	80.68%
Recall	66.4%	61.9%	62.6%	60.8%	57.48%	13.89%	32.70%
ROC Area	0.742	0.732	0.732	0.731	0.68	0.68	0.58

4. DISCUSSION AND CONCLUSION

Staging of Liver fibrosis is an integral component in the appropriate management of CHC and the prediction of patient prognosis. Patients with advanced fibrosis (F3-F4) will eventually progress to cirrhosis carrying the risk of liver decompensation, primary liver cancer of hepatocellular carcinoma and death [18]. The needed evaluation and follow up of liver fibrosis stage have been traditionally performed by liver biopsy [19]. There have been many proposed non-invasive biomarkers, an ideal serological test for assessing liver fibrosis stages is still awaited [18].

Liver biopsy is still the gold standard for assessing the staging of liver fibrosis. The collected demographic, biochemical, and histological data sets for a large cohort of 69106 chronic hepatitis patients with available liver biopsy results give us the chance to revise and validate the accuracy of FIB-4 and APRI [4, 20]. In our study, FIB-4 and APRI diagnosed advanced fibrosis (F3-F4with a good negative predictive value and high specificity which is comparable to the original study, but low positive predictive value and with poor sensitivity. Patients with advanced fibrosis were not diagnosed and there was a great discordance between FIB-4 and APRI compared to liver biopsy results.

This high discordance in our study between biopsy, FIB-4 and APRI with overall AUC 0.69 and 0.58 provided the motivation to use data mining techniques to find a noninvasive predictive algorithm. Machine learning techniques such as Decision Trees (classification trees) have been used for prediction, classification, and as diagnostic tools. The decision tree method is a potent statistical technique for allocation, prediction, and, interpretation that has a lot of applications in the field of medical research. The relationship between data is represented in an easy to follow top down tree architecture. The root node of the decision tree is the most influential piece of data that affects the response variable in the model [21, 22]. It is simple, easy to interpret and can efficiently deal with large, complicated data without a complicated parametric structure [23]. An alternative approach to create a decision tree is to grow a large tree, and then prune it by

removing nodes that provide less additional information. Pruning is usually performed for enhancing tree comprehensibility while maintaining (or even improving) its accuracy [24]. Reduced error pruning (REP) is a conceptually simple strategy that should be performed in a bottom-up fashion [14, 17].

Conclusion: This is the largest multi-centered registry study including the largest sample size of CHC patients (69106 patients). This large sample size could explain the discrepancy between these study findings and the reports from the original studies or other studies that included smaller sample size (hundreds). This large sample size showed a great discordance between FIB-4, APRI and Metavir score. Decision tree (REP tree) could provide a reliable method for non-invasive diagnosis of fibrosis stages using routine laboratory parameters

ACKNOWLEDGMENT

The authors would like to thank Egyptian National Committee for Control of Viral Hepatitis, Ministry of Health and Population (MOHP) for supplying the patient's data.

REFERENCES

[1] I. Waked, W. Doss, M. H. El-Sayed, C. Estes, H. Razavi, G. Shiha, A. Yosry, and G. Esmat, "The current and future disease burden of chronic hepatitis c virus infection in egypt," Arab J Gastroenterol, vol. 15, no. 2, pp. 45–52, 2014.

[2] S. Blach, S. Zeuzem, M. Manns, I. Altraif, A.-S. Duberg, D. H. Muljono, I. Waked, S. M. Alavian, M.-H. Lee, and F. Negro, "Global prevalence and genotype distribution of hepatitis c virus infection in 2015: a modelling study," The Lancet Gastroenterology & Hepatology, vol. 2, no. 3, pp. 161–176, 2017.

[3] E. A. for the Study of the Liver, "Easl recommendations on treatment of hepatitis c 2014," Journal of hepatology, vol. 61, no. 2, pp. 373– 395, Aug 2014, lR: 20160113; JID: 8503886; 0 (Antiviral Agents); 0 (RNA, Viral); 2014/05/14 06:00 [entrez]; 2014/05/14 06:00 [pubmed]; 2015/08/12 06:00 [medline]; ppublish.

[4] V. Papastergiou, E. Tsochatzis, and A. K. Burroughs, "Non-invasive assessment of liver fibrosis," Annals of gastroenterology, vol. 25, no. 3, pp. 218–231, 2012, lR: 20170224; JID: 101121847; OTO: NOTNLM; 2011/02/27 00:00 [received]; 2012/03/13 00:00 [accepted]; 2014/04/10 06:00 [entrez]; 2012/01/01 00:00 [pubmed]; 2012/01/01 00:00 [medline]; ppublish.

[5] M. Alboraie, M. Khairy, M. Elsharkawy, N. Asem, A. Elsharkawy, and G. Esmat, "Value of egyscore in diagnosis of significant, advanced hepatic fibrosis and cirrhosis compared to aspartate aminotransferaseto- platelet ratio index, fib4 and forns' index in chronic hepatitis c virus," Hepatology Research, vol. 45, no. 5, pp. 560–570, 2015.

[6] M. Khairy, M. Abdel-Rahman, M. El-Raziky, W. El-Akel, N. Zayed, H. Khatab, and G. Esmat, "Non-invasive prediction of hepatic fibro- sis in patients with chronic hcv based on the routine pre-treatment workup," Hepatitis monthly, vol. 12, no. 11, p. e6718, Nov 2012, lR: 20130530; JID: 101277874; OTO: NOTNLM; 2012/06/09 00:00 [received]; 2012/07/19 00:00 [revised]; 2012/08/13 00:00 [accepted]; 2013/01/25 06:00 [entrez]; 2013/01/25 06:00 [pubmed]; 2013/01/25 06:01 [medline]; ppublish.

[7] A. Yosry, R. Fouad, S. A. Alem, A. Elsharkawy, M. El-Sayed, N. Asem, E. Hassan, A. Ismail, and G. Esmat, "Fibroscan, apri, fib4, and guci: Role in prediction of fibrosis and response to therapy in egyptian patients with hcv infection," Arab Journal of Gastroenterology, vol. 17, no. 2, pp. 78–83, 2016.

[8] T. G. Ragazzo, D. Paranagua-Vezozzo, F. R. Lima, D. F. de Campos Mazo, M. G. Pessoa, C. P. Oliveira, V. A. F. Alves, and F. J. Carrilho, "Accuracy of transient elastography-fibroscan, acoustic radiation force impulse (arfi) imaging, the enhanced liver fibrosis (elf) test, apri, and the fib-4 index

compared with liver biopsy in patients with chronic hepatitis c," Clinics, vol. 72, no. 9, pp. 516–525, 2017.

[9] I. H. Witten, E. Frank, M. A. Hall, and C. J. Pal, Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann, 2016.

[10] M. LeBlanc and J. Crowley, A review of tree-based prognostic models, ser. Recent advances in clinical trial design and analysis. Springer, 1995, pp. 113–124.

[11] D. A. E. H. Omran, A. H. Awad, M. A. El, R. Mabrouk, A. F. Soliman, and A. O. A. Aziz, "Application of data mining techniques to explore predictors of hcc in egyptian patients with hcv-related chronic liver," Asian Pacific Journal of Cancer Prevention, vol. 16, no. 1, pp. 381–385, 2015.

[12] A. Abdelaziz, A. Awad, H. Shousha, M. Mahmoud, D. Om- ran, A. h. K. Abdelmaksoud, and M. Mabrouk, "Meta-learning analysis to find the best predictive algorithm for prediction of hepatocellular carcinoma outcome in a cohort of 1200 hcv-related patients," in The European Association for the Study of the Liver (EASL) - HCC summit, vol. P13.02-YI, 02 2017. [Online]. Available: http://livertree.easl.eu/easl/2017/geneva/165849/hend.shousha. meta-learning.analysis.to.find.the.best.predictive.algorithm.for.html

[13] M. E. Raziky, W. F. Fathalah, Z. Zakaria, H. G. Eldeen, A. Abul- Fotouh, A. Salama, A. Awad, G. Esmat, and M. Mabrouk, "Predictors of virological response in 3,235 chronic hcv egyptian patients treated with peginterferon alpha-2a compared with peginterferon alpha-2b using statistical methods and data mining techniques," Journal of Inter- feron & Cytokine Research, vol. 36, no. 5, pp. 338–346, 2016.

[14] A. Awad, M. Mabrouk, T. Awad, N. Zayed, S. Mousa, and M. Saeed, "Performance evaluation of decision tree classifiers for the prediction of response to treatment of hepatitis c patients," in Proceedings of the 8th International Conference on Pervasive Computing Technologies for Healthcare. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2014, pp. 186–190.

[15] S. Hashem, G. Esmat, W. Elakel, S. Habashy, S. A. Raouf, S. Darweesh, M. Soliman, M. Elhefnawi, M. El-Adawy, and M. ElHefnawi, "Accurate prediction of advanced liver fibrosis using the decision tree learning algorithm in chronic hepatitis c egyptian patients," Gastroenterology research and practice, vol. 2016, 2016.

[16] M. Hall, "Correlation-based feature subset selection for machine learn- ing," Thesis submitted in partial fulfillment of the requirements of the degree of Doctor of Philosophy at the University of Waikato, 1998.

[17] M. Bal, M. F. Amasyali, H. Sever, G. Kose, and A. Demirhan, "Per- formance evaluation of the machine learning algorithms used in inference mechanism of a medical decision support system," The Scientific World Journal, vol. 2014, p. 137896, 2014, lR: 20151029; JID: 101131163; 2014/06/04 00:00 [received]; 2014/08/07 00:00 [revised]; 2014/08/20 00:00 [accepted]; 2014/10/09 06:00 [entrez]; 2014/10/09 06:00 [pubmed]; 2015/06/24 06:00 [medline]; ppublish.

[18] N. Yada, M. Kudo, N. Kawada, S. Sato, Y. Osaki, A. Ishikawa, H. Miyoshi, M. Sakamoto, M. Kage, and O. Nakashima, "Noninvasive diagnosis of liver fibrosis: utility of data mining of both ultrasound elastography and serological findings to construct a decision tree," Oncology, vol. 87, no. Suppl. 1, pp. 63–72, 2014.

[19] Y. Lurie, M. Webb, R. Cytter-Kuint, S. Shteingart, and G. Z. Lederkremer, "Non-invasive diagnosis of liver fibrosis and cirrhosis," World journal of gastroenterology, vol. 21, no. 41, pp. 11 567–11 583, Nov 7 2015, lR: 20170220; JID: 100883448; 0 (Biomarkers); OTO: NOTNLM; 2015/04/28 00:00 [received]; 2015/07/23 00:00 [revised]; 2015/09/15 00:00 [accepted]; 2015/11/12 06:00 [entrez]; 2015/11/12 06:00 [pubmed]; 2016/11/01 06:00 [medline]; ppublish.

[20] M. Adler, B. Gulbis, C. Moreno, S. Evrard, G. Verset, P. Golstein, B. Frotscher, N. Nagy, and P. Thiry, "The predictive value of fib4 versus fibrotest, apri, fibroindex and forns index to noninvasively

estimate fibrosis in hepatitis c and nonhepatitis c liver diseases," Hepatology, vol. 47, no. 2, pp. 762–763, 2008.

[21] T. Poynard, Y. Ngo, H. Perazzo, M. Munteanu, P. Lebray, J. Mous- salli, D. Thabut, Y. Benhamou, and V. Ratziu, "Prognostic value of liver fibrosis biomarkers: a meta-analysis," Gastroenterology & hepatology, vol. 7, no. 7, pp. 445–454, Jul 2011, lR: 20170220; JID: 101262648; OTO: NOTNLM; 2012/02/03 06:00 [entrez]; 2012/02/03 06:00 [pubmed]; 2012/02/03 06:01 [medline]; ppublish.

[22] E. Rezaei-Darzi, F. Farzadfar, A. Hashemi-Meshkini, I. Navidi, M. Mahmoudi, M. Varmaghani, P. Mehdipour, M. S. Alamdari, B. Tayefi, and S. Naderimagham, "Comparison of two data mining techniques in labeling diagnosis to iranian pharmacy claim dataset: artificial neural network (ann) versus decision tree model." Archives of Iranian Medicine (AIM), vol. 17, no. 12, 2014.

[23] Y. Y. Song and Y. Lu, "Decision tree methods: applications for classification and prediction," Shanghai archives of psychiatry, vol. 27, no. 2, pp. 130–135, Apr 25 2015, lR: 20170220; JID: 9891453; OTO: NOTNLM; 2015/04/01 00:00 [received]; 2015/04/09 00:00 [accepted]; 2015/06/30 06:00 [entrez]; 2015/06/30 06:00 [pubmed]; 2015/06/30 06:01 [medline]; ppublish.

[24] R. C. Barros, A. T. Winck, K. S. Machado, M. P. Basgalupp, A. C. de Carvalho, D. D. Ruiz, and O. N. de Souza, "Automatic design of decision-tree induction algorithms tailored to flexible-receptor docking data," BMC bioinformatics, vol. 13, no. 1, p. 310, 2012.

OPTIMIZING DSCP MARKING TO ENSURE VOIP'S QOS OVER HFC NETWORK

Shaher Daoud and Yanzhen Qu

School of Computer Science, Colorado Technical University,
Colorado Springs, USA

ABSTRACT

Three major factors that can affect Voice over Internet Protocol (VoIP) phone services' quality, these include packet delay, packet loss, and jitter. The focus of this study is specific to the VoIP phone services offered to customers by cable companies that utilize broadband hybrid fiber coaxial (HFC) networks. HFC networks typically carry three types of traffic that include voice, data, and video. Unlike data and video, some delays or packet loss can result in a noticeable degraded impact on a VoIP's phone conversation. We will examine various differentiated services code point (DSCP) marking, then analyze and assess their impact on VoIP's quality of service (QoS). This study mimics the production environment. It examines the relationship between specific DSCP marking's configuration. This research avoids automated test calls and rather focuses on human made call testing. This study relies on users' experience and the captured data to support this research's findings.

KEYWORDS

QoS , VoIP, DSCP Marking , jitter, HFC Network, MOS.

1. INTRODUCTION

Voice over Internet Protocol (VoIP) is a newly adopted technology; its deployment continues to accelerate [1, 2]. The acronym VoIP refers to voice communication on the Internet using the Internet protocol (IP). Voice signals change into voice packets and get transmitted through the same network that providers use for data communications [3]. For voice traffic to travel in a Hybrid Fiber Coaxial (HFC) broadband network, the analog voice signal gets converted into digital signals. Additional hardware such as routers, switches, and servers are needed to transport voice traffic to its destination. IP broadband networks allow cable providers to combine voice traffic, data traffic, and video traffic to travel over a single communication link. Packet loss, jitter, and latency continue to be the major elements that impact the quality of VoIP [1, 4]. Packet prioritization can play an important role in VoIP's quality; where it differentiates between VoIP traffic and other traffic types that share the same networks links. The Differentiated Services Code Point (DSCP) marking is based on assigning different values for a various traffic types including VoIP [5]. Packet loss between 1% and 5%, and having less than 300 milliseconds (ms) of end-to-end delay are key elements of VoIP calls [6].

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 327-339, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90928

As a result, finding methods that can address VoIP's quality is the primary focus of many scholars and researchers in the telecommunications field. DSCP marking may allow HFC broadband network carriers to prioritize their traffic. If the carriers have the ability to mark the different types of traffic across the various devices in their networks, VoIP's quality might improve. DSCP marking can be of a great benefit to VoIP. This research focuses primarily on providing and recommending the best DSCP marking that can be used in HFC network to ensure a better VoIP's voice quality.

2. PURPOSE, PROBLEM STATEMENT AND HYPOTHESIS

This study focuses on our research purpose, the problem statement and our hypothesis.

2.1 Research Purpose Statement

This research primarily focuses on studying the quality of VoIP service delivery in an HFC broadband network when mixed with data and video traffic. The primary purpose of this research is to improve VoIP's QoS. VoIP, video, and data share the same transport links in broadband HFC networks. VoIP traffic cannot tolerate packet loss or delay. Call instances where VoIP phone calls encounter considerable packet delays, both callers begin to talk over each other [6, 7].

2.2 Problem Statement

HFC networks carry multiple types of traffic that include voice, data, and video. Some of the elements that affect VoIP's quality are packet loss, jitter, latency, and delay. Treating all three types of traffic equally in each element of the broadband HFC network, especially with over utilized capacity links, can degrade VoIP's QoS.

2.3 Hypothesis Statement

Configuring VoIP traffic with a DSCP marking value of EF across all the equipment in a broadband HFC network would improve VoIP's QoS.

2.4 Research Question

This research focuses on addressing one primary research question: considering the routers' links carry Internet, video, and VoIP traffic where traffic links are under-utilized, which of the DSCP marking has the best impact on VoIP's QoS?

3. RELATED WORKS

The need for prioritizing voice traffic on IP networks became imminent. The implication of recent research studies on VoIP and QoS increased to improve VoIP services and make them affordable, cheaper, and a reliable for users' daily needs [8, 9, 10]. The quality of VoIP traffic can be dependent on five factors: mean opinion score (MOS), jitter, latency, network load, and network throughput [11]. There is an imminent the need for QoS in VoIP calls while at the same time have the ability to support as many calls as possible [12].

VoIP's degraded call quality, when compared with circuit-switched phone calls, became an issue that was not easy to tolerate or ignore. Since then, many research studies started to focus on improving the quality of VoIP's services. Due to VoIP's nature where it travels across various networks and equipment, many academics & practitioners continue to study the various aspects of VoIP to improve its service. VoIP's poor QoS through wireless fidelity (WiFi), universal mobile telecommunications system (UMTS) & WiFi UMTS networks led researchers to examine the MOS and the packets' end-to-end delay to improve VoIP's quality [13]. Researchers continue to focus on coming up with new solutions that improve VoIP's quality.

Some studies turned towards utilizing Machine Learning Quality of Experience (MLQoE) to improve VoIP traffic's quality of Experience. MLQoE selects the Machine Learning (ML) algorithm that shows the best performance and its elements in an automated process, considering the use of the dataset as input [14]. There is a recommendation to prioritize Voice traffic to handle packet losses in VoIP services. This can be achieved through providing a mechanism to drop first the least important content, in order to keep the best VoIP's quality signal for user perception using an Arduino platform [15]. Researchers investigated the performances of routing protocols Optimized Link State Routing (OLSR) and Training and Doctrine Command (TRADOC) Operations Research Agency (TORA) in a Mobile Ad hoc Networks (MANETs). The wireless mobile nodes group form a temporary network; this avoids the utilization of any centralized access-point management of the mobile networks. The research used the network simulator Optimized Network Engineering Tool (OPNET) 14.5 to analyse and evaluate some QoS metrics like end-to-end delay, Jitter, throughput and MOS. The OPNET simulation results showed that the OLSR protocol is a good candidate for VoIP application [16].

To ensure that mobile networks deliver improved VoIP QoS, each network element should follow the same single protocol. The investigation focused on WiFi and Cellular networks. Network Neutrality may become an obstacle for achieving the intended results of improving VoIP's conversations [17]. To address QoS in wireless networks regardless of whether they are heterogeneous or homogenous, the recommendation was to use a software defined network (SDN) architecture. The use of Smart Adaptive QoS for Heterogeneous and Homogeneous Networks (SAQ-2HN) architecture resulted in higher delay without the use of QoS and better results with the use of SAQ-2HN [18].

VoIP's QoS transition from an IP Version 6 (IPv6) network to an IP Version 4 (IPv4) network maintained its quality through the IP network tunnelling process. No substantial delay was noticed where it could have impacted the quality of VoIP phone calls [19].

4. RESEARCH DESIGN

This research uses an experimental testing design approach where its quantitative study investigates the impact of changing DSCP marking on VoIP phone calls. The experiments in this study rely on making manual VoIP phone calls. In each of the manual testing scenarios; one tester makes a call while the other tester answers. Primary elements of the test environment include a router and an MGC. The links between the router and the HFC broadband network carry all three types of traffic that include data, video, and VoIP. VoIP traffic marking changes take place at the MGC level. The routers pass VoIP traffic and perform prioritization dependent on the MGCF's DSCP marking. Iris tool captures the end-to-end call signalling. Iris traces will show the MOS, DSCP marking, and any packet loss or packet drops.

4.1 Phone Calls' Testing: VoIP to signaling system 7 (SS7) and SS7 to VoIP

The first testing scenario focuses on making calls from a VoIP network and terminate on SS7 network. The second testing scenario focuses on making calls from SS7 network and terminate in a VoIP network. Each of the testing scenarios is composed of five independent DSCP marking configuration changes that include class selector 0 (CS0), CS1, CS3, CS4, and expedited forwarding (EF). The process of making 10 calls takes place after each of the DSCP configuration changes.

4.2 Answering the Research Question

The experiments' data for each of the test calls are collected and populated in identical tables. The data gets analysed and used to answer the research question including the research hypotheses. The analysis is based on the telecom industry and ITU's standards. The dependent variables of this research include the average MOS captured by the Iris tool, calling party's estimated MOS, called party estimated MOS, average jitter, average interpacket arrival time, latency, and packets lost. This research compares the experiment dependent variables' values with the VoIP industry's standards. MOS values between 4 and 5 refer to clear phone conversation, and anything below 4 as poor quality [20]. The acceptable jitter's value is less than 50 ms [21]. VoIP interpacket arrival time should be between 20 or 30 ms [22]. 1.5% or less are the acceptable data loss value [21]. The maximum tolerable latency value falls between 80 ms and 120 ms [23].

5. EXPERIMENTS RESULTS AND ANALYSIS

Each experiment will be composed of five tests and each of the tests is based on 10 phone calls. Each of the tests will focus on one DSCP configurations that include CS0, CS1, CS3, CS4, and EF.

5.1 VoIP to SS7 Experiments

This section focuses on VoIP to SS7 test scenrios and their related data.

5.1.1 VoIP to SS7 test calls with a DSCP marking value of CS0

10 random calls are made; testing results are captured in Table 1. The lowest MOS value of the 10 calls is 4.380 and the highest value is 4.400. The lowest average interpacket arrival time is 20.030 ms, while the highest value is 20.400 ms. The lowest jitter's value is 0.01 ms while the highest value is 5.30 ms. The highest packet loss is 0.27%, and the highest latency value is 54 ms. Examining the values of each of the dependent variables indicates that each of the values were within specifications which lead to good and clear phone conversations between both parties.

Table 1. VoIP to SS7 test calls with a DSCP marking value of CS0

Call No.	MOS Avg CQ	MOS Calling Party	MOS Called Party	Avg Inter-packet Time (ms)	Avg Jitter (ms)	Total Packets	Packets Lost	Packets Loss (%)	Lat-ency
1	4.380	4.400	4.400	20.030	1.00	3344	6	0.18	0
2	4.400	4.400	4.400	20.000	0.02	3438	0	0.00	35
3	4.390	4.400	4.400	20.000	0.05	12694	0	0.00	54
4	4.400	4.400	4.400	20.080	5.30	3534	0	0.00	32
5	4.390	4.400	4.400	20.000	0.02	13799	0	0.00	48
6	4.400	4.400	4.400	20.050	3.84	1987	0	0.00	33
7	4.400	4.400	4.400	20.400	2.97	2947	8	0.27	0
8	4.400	4.400	4.400	20.000	0.01	1582	0	0.00	32
9	4.400	4.400	4.400	20.000	0.02	23726	4	0.02	0
10	4.400	4.400	4.400	20.000	0.02	40522	6	0.01	0

5.1.2 VoIP to SS7 test calls with a DSCP marking value of CS1

10 random calls are made; testing results are captured in Table 2. All 10 calls have the same MOS value of 4.400. The lowest average interpacket arrival time is 20.000 ms while the highest is 20.070 ms. The lowest jitter's value is 0.02 ms while the highest is 7.83 ms. Packet loss is 0%, and the highest latency value is 20 ms. Examining the values of each of the dependent variables indicate that each of the values were within specifications that lead to good and clear phone conversations between both parties.

Table 2. VoIP to SS7 test calls with a DSCP marking value of CS1

Call No.	MOS Avg CQ	MOS Calling Party	MOS Called Party	Avg Inter-packet Time (ms)	Avg Jitter (ms)	Total Packets	Packets Lost	Packets Loss (%)	Lat-ency
1	4.40	4.400	4.400	20.000	0.02	1820	0	0.00	14
2	4.40	4.400	4.400	20.010	7.09	2195	0	0.00	9
3	4.40	4.400	4.400	20.000	4.04	4799	0	0.00	20
4	4.40	4.400	4.400	20.000	7.83	4438	0	0.00	8
5	4.40	4.400	4.400	20.010	7.49	1445	0	0.00	19
6	4.40	4.400	4.400	20.000	0.02	2944	0	0.00	8
7	4.40	4.400	4.400	20.000	0.02	1747	0	0.00	12
8	4.40	4.400	4.400	20.020	4.03	1755	0	0.00	12
9	4.40	4.400	4.400	20.070	7.13	1999	0	0.00	12
10	4.40	4.400	4.400	20.000	0.02	1350	0	0.00	11

5.1.3 VoIP to SS7 test calls with a DSCP marking value of CS3

10 random calls are made; testing results are captured in Table 3. All 10 calls have the same MOS value of 4.400. The lowest average interpacket arrival time is 20.000 ms while the highest is 20.070 ms. The lowest jitter's value is 0.02 ms while the highest is 7.83 ms. Packet loss is 0%, and the highest latency value is 20 ms. Examining the values of each of the dependent variables indicate that each of the values were within specifications that lead to good and clear phone conversations between both parties.

Table 3. VoIP to SS7 test calls with a DSCP marking value of CS3

Call No.	MOS Avg CQ	MOS Calling Party	MOS Called Party	Avg Inter-packet Time (ms)	Avg Jitter (ms)	Total Packets	Packets Lost	Packets Loss (%)	Lat-ency
1	4.40	4.400	4.400	20.010	2.72	2889	0	0.00	8
2	4.40	4.400	4.400	20.000	0.04	2897	0	0.00	0
3	4.40	4.400	4.400	20.000	1.53	797	0	0.00	0
4	4.40	4.400	4.400	20.000	0.11	3588	0	0.00	0
5	4.40	4.400	4.400	20.000	4.01	24077	0	0.00	0
6	4.40	4.400	4.400	20.000	0.03	10704	0	0.00	0
7	4.40	4.400	4.400	20.000	0.91	1681	0	0.00	0
8	4.40	4.400	4.400	20.000	0.19	6499	0	0.00	0
9	4.40	4.400	4.400	20.000	1.54	457	0	0.00	0
10	4.40	4.400	4.400	20.000	0.01	12619	0	0.00	0

5.1.4 VoIP to SS7 test calls with a DSCP marking value of CS4

10 random calls are made; testing results are captured in Table 4. All 10 calls have the same MOS value of 4.400. The lowest average interpacket arrival time is 20.000 ms while the highest is 20.010 ms. The lowest jitter's value is 0.01 ms while the highest is 0.02 ms. Packet loss is 0%, and there is no indication of any latency. Examining the values of each of the dependent variables indicate that each of the values were within specifications that lead to good and clear phone calls between both parties.

Table 4. VoIP to SS7 test calls with a DSCP marking value of CS4

Call No.	MOS Avg CQ	MOS Calling Party	MOS Called Party	Avg Inter-packet Time (ms)	Avg Jitter (ms)	Total Packets	Packets Lost	Packets Loss (%)	Lat-ency
1	4.40	4.400	4.400	20.000	0.02	11929	0	0.00	0
2	4.40	4.400	4.400	20.000	0.01	1023	0	0.00	0
3	4.40	4.400	4.400	20.000	0.02	9106	0	0.00	0
4	4.40	4.400	4.400	20.000	0.01	8171	0	0.00	0
5	4.40	4.400	4.400	20.010	0.02	11843	0	0.00	0
6	4.40	4.400	4.400	20.000	0.01	5507	0	0.00	0
7	4.40	4.400	4.400	20.000	0.02	90026	0	0.00	0
8	4.40	4.400	4.400	20.000	0.01	5484	0	0.00	0
9	4.40	4.400	4.400	20.000	0.02	2904	0	0.00	0
10	4.40	4.400	4.400	20.000	0.02	5502	0	0.00	0

5.1.5 VoIP to SS7 test calls with a DSCP marking value of EF

10 random calls are made; testing results are captured in Table 5. All 10 calls have the same MOS value of 4.400. The average interpacket arrival time for each of the 10 calls is 20.000 ms. The lowest jitter's value is 0.00 ms while the highest jitter's value is 0.01 ms. Packet loss is 0%, and there is no indication of any latency. Examining the values of each of the dependent variables indicate that each of the values were within specifications that lead to good and clear phone calls between both parties.

Table 5. VoIP to SS7 test calls with a DSCP marking value of EF

Call No.	MOS Avg CQ	MOS Calling Party	MOS Called Party	Avg Inter-packet Time (ms)	Avg Jitter (ms)	Total Packets	Packets Lost	Packets Loss (%)	Lat-ency
1	4.400	4.400	4.400	20.000	0.01	1286	0	0.00	0
2	4.400	4.400	4.400	20.000	0.00	730	0	0.00	0
3	4.400	4.400	4.400	20.000	0.01	4618	0	0.00	0
4	4.400	4.400	4.400	20.000	0.02	8118	0	0.00	0
5	4.400	4.400	4.400	20.000	0.02	13543	0	0.00	0
6	4.400	4.400	4.400	20.000	0.02	1313	0	0.00	0
7	4.400	4.400	4.400	20.000	0.02	24123	0	0.00	0
8	4.400	4.400	4.400	20.000	0.02	1969	0	0.00	0
9	4.400	4.400	4.400	20.000	0.01	6799	0	0.00	0
10	4.400	4.400	4.400	20.000	0.02	3561	0	0.00	0

5.2 SS7 to VoIP Experiments

This section focuses on SS7 to VoIP test scenrios and their related data.

5.2.1 SS7 to VoIP test calls with a DSCP marking value of CS0

10 random calls are made; testing results are captured in Table 6. The lowest MOS value of the 10 calls shows a value of 4.360 and the highest value is 4.400. The lowest average interpacket arrival time is 20.000 ms while the highest is 20.400 ms. The lowest jitter's value is 0.01 ms while the highest is 5.47 ms. The highest packet loss is 0.49%, and the highest latency value is 54 ms. Examining the values of each of the dependent variables indicate that each of the values were within specifications that lead to good and clear phone conversations between both parties.

Table 6. SS7 to VoIP test calls with a DSCP marking value of CS0

Call No.	MOS Avg CQ	MOS Calling Party	MOS Called Party	Avg Inter-packet Time (ms)	Avg Jitter (ms)	Total Packets	Packets Lost	Packets Loss (%)	Lat-ency
1	4.39	4.400	4.400	20.000	0.03	12698	0	0.00	54
2	4.40	4.400	4.400	20.000	0.02	4791	0	0.00	20
3	4.38	4.400	4.400	20.400	0.26	1760	4	0.23	0
4	4.40	4.400	4.400	20.040	3.68	3442	0	0.00	35
5	4.36	4.400	4.400	20.100	0.01	1235	6	0.49	8
6	4.40	4.400	4.400	20.010	5.47	1591	0	0.00	32
7	4.39	4.400	4.400	20.000	0.06	13800	0	0.00	48
8	4.40	4.400	4.400	20.000	0.02	3540	0	0.00	32
9	4.40	4.400	4.400	20.000	0.02	3211	0	0.00	0
10	4.40	4.400	4.400	20.000	0.20	26927	4	0.01	0

5.2.2 SS7 to VoIP test calls with a DSCP marking value of CS1

10 random calls are made; testing results are captured in Table 7. All 10 calls had the same MOS value of 4.400. The lowest average interpacket arrival time is 20.000 ms while the highest is 20.120 ms. The lowest jitter's value is 0.01 ms while the highest is 6.69 ms. Packet loss is 0%, and the highest latency value is 19 ms. Examining the values of each of the dependent variables indicate that each of the values were within specifications that lead to good and clear phone conversations between both parties.

Table 7. SS7 to VoIP Test Calls with a DSCP Marking Value of CS1

Call No.	MOS Avg CQ	MOS Calling Party	MOS Called Party	Avg Inter-packet Time (ms)	Avg Jitter (ms)	Total Packets	Packets Lost	Packets Loss (%)	Lat-ency
1	4.40	4.400	4.400	20.000	0.02	1351	0	0.00	12
2	4.40	4.400	4.400	20.010	6.69	2582	0	0.00	8
3	4.40	4.400	4.400	20.020	2.71	1830	0	0.00	14
4	4.40	4.400	4.400	20.000	0.01	2884	0	0.00	8
5	4.40	4.400	4.400	20.000	0.02	1436	0	0.00	19
6	4.40	4.400	4.400	20.120	4.96	1232	0	0.00	8
7	4.40	4.400	4.400	20.000	0.02	1998	0	0.00	12
8	4.40	4.400	4.400	20.080	5.39	1352	0	0.00	11
9	4.40	4.400	4.400	20.010	3.14	1354	0	0.00	12
10	4.40	4.400	4.400	20.000	0.02	2188	0	0.00	9

5.2.3 SS7 to VoIP test calls with a DSCP marking value of CS3

10 random calls are made; testing results are captured in Table 8. All 10 calls have the same MOS value of 4.400. The lowest average interpacket arrival time is 19.990 ms while the highest is 20.000 ms. The lowest jitter's value is 0.01 ms while the highest is 1.10 ms. Packet loss is 0%,

and the highest latency value is 8 ms. Examining the values of each of the dependent variables indicate that each of the values were within specifications that lead to good and clear phone calls between both parties.

Table 8. SS7 to VoIP Test Calls with a DSCP Marking Value of CS3

Call No.	MOS Avg CQ	MOS Calling Party	MOS Called Party	Avg Inter-packet Time (ms)	Avg Jitter (ms)	Total Packets	Packets Lost	Packets Loss (%)	Lat-ency
1	4.40	4.400	4.400	20.000	0.01	2576	0	0.00	8
2	4.40	4.400	4.400	20.000	0.07	1104	0	0.00	0
3	4.40	4.400	4.400	20.000	0.24	8526	0	0.00	0
4	4.40	4.400	4.400	20.000	0.04	6304	0	0.00	0
5	4.40	4.400	4.400	19.990	0.04	26959	0	0.00	0
6	4.40	4.400	4.400	20.000	0.06	1035	0	0.00	0
7	4.40	4.400	4.400	20.000	0.18	3584	0	0.00	0
8	4.40	4.400	4.400	20.000	0.11	23136	0	0.00	0
9	4.40	4.400	4.400	20.000	0.18	45362	0	0.00	0
10	4.40	4.400	4.400	20.000	1.10	52977	0	0.00	0

5.2.4 SS7 to VoIP test calls with a DSCP marking value of CS4

10 random calls are made; testing results are captured in Table 9. All 10 calls have the same MOS value of 4.400. The average interpacket arrival time for each of the test calls is 20.000 ms. The lowest jitter's value is 0.01 ms while the highest is 0.03 ms. Packet loss is 0%, and there is no indication of any latency. Examining the values of each of the dependent variables indicate that each of the values were within specifications that lead to good and clear phone calls between both parties.

Table 9. SS7 to VoIP test calls with a DSCP marking value of CS4

Call No.	MOS Avg CQ	MOS Calling Party	MOS Called Party	Avg Inter-packet Time (ms)	Avg Jitter (ms)	Total Packets	Packets Lost	Packets Loss (%)	Lat-ency
1	4.40	4.400	4.400	20.000	0.02	17400	0	0.00	0
2	4.40	4.400	4.400	20.000	0.01	3346	0	0.00	0
3	4.40	4.400	4.400	20.000	0.02	23142	0	0.00	0
4	4.40	4.400	4.400	20.000	0.01	6308	0	0.00	0
5	4.40	4.400	4.400	20.000	0.04	1659	0	0.00	0
6	4.40	4.400	4.400	20.000	0.02	26464	0	0.00	0
7	4.40	4.400	4.400	20.000	0.02	955	0	0.00	0
8	4.40	4.400	4.400	20.000	0.02	1697	0	0.00	0
9	4.40	4.400	4.400	20.000	0.02	45362	0	0.00	0
10	4.40	4.400	4.400	20.000	0.03	1763	0	0.00	0

5.2.5 SS7 to VoIP test calls with a DSCP marking value of EF

10 random calls are made; testing results are captured in Table 10. All 10 calls have the same MOS value of 4.400. The average interpacket arrival time for each of the test calls is 20.000 ms. The lowest jitter's value is 0.01 ms while the highest jitter's value is 0.02 ms. Packet loss is 0%, and there is no indication of any latency. Examining the values of each of the dependent variables indicate that each of the values were within specifications that lead to good and clear phone calls between both parties.

Table 10. SS7 to VoIP Test Calls with a DSCP Marking Value of EF

Call No.	MOS Avg CQ	MOS Calling Party	MOS Called Party	Avg Inter-packet Time (ms)	Avg Jitter (ms)	Total Packets	Packets Lost	Packets Loss (%)	Lat-ency
1	4.40	4.400	4.400	20.000	0.02	3551	0	0.00	0
2	4.40	4.400	4.400	20.000	0.02	90024	0	0.00	0
3	4.40	4.400	4.400	20.000	0.02	1291	0	0.00	0
4	4.40	4.400	4.400	20.000	0.02	8526	0	0.00	0
5	4.40	4.400	4.400	20.000	0.01	1754	0	0.00	0
6	4.40	4.400	4.400	20.000	0.01	1041	0	0.00	0
7	4.40	4.400	4.400	20.000	0.02	10694	0	0.00	0
8	4.40	4.400	4.400	20.000	0.02	3364	0	0.00	0
9	4.40	4.400	4.400	20.000	0.02	17395	0	0.00	0
10	4.40	4.400	4.400	20.000	0.02	8107	0	0.00	0

5.3 Calls' Data Analysis

We rely on our analysis of the data to answer the research question and the research hypotheses. Research Question: Which of the DSCP marking have the best impact on VoIP QoS? Our testing data show that the tests associated with a DSCP marking of EF have the best results and the best positive impact on VoIP QoS. EF test cases are the only tests that have the best results. Each call has a MOS score of 4.400. Each of the test calls of both tests show a 0 packet loss and a 0 latency. Each of the test calls of both tests show 20.000 ms average interpacket arrival time. Our research's hypotheses statement states that cconfiguring VoIP traffic with a DSCP marking value of EF across all the equipment in a broadband HFC network improves VoIP's QoS. VoIP traffic that have a DSCP marking of EF kept its level of good quality and the mixture of video and Internet traffic have no negative impact on VoIP phone calls. When comparing the test data associated with a DSCP marking of EF with the other eight different test cases, the data show a clear difference where VoIP traffic with a DSCP marking of EF improved. None of the test calls associated with the DSCP marking of EF have any packet loss or latency. EF DSCP marking test calls have the same MOS value of 4.40. The interpacket arrival time associated with each of the EF DSCP marking test calls is 20.00.

6. CONCLUSIONS AND FUTURE WORKS

This study found that the higher VoIP traffic's DSCP marking value assignment, the less the chances of higher latency or packet loss in the VoIP traffic. Also, the study found that lower DSCP marking values have a negative impact on VoIP quality where the probability of running into higher latency or packet loss increases. This study also highlighted that VoIP traffic's DSCP marking is beneficial and have value even when the links between the MGC and the routers are underutilized. This research concludes that it is important to use DSCP marking in IP networks where various traffic share the same links. The assignment of EF DSCP marking to VoIP prioritizes VoIP over other types of traffic which eliminates packet loss, packet delay and improves VoIP's quality.

Future research should consider studying an additional three of the DSCP marking that include CS2, CS5, and CS6. This experiment tested five of the DSCP marking while the links between the MGC and the adjacent routers were not at full capacity. Future research studies should consider making the same tests but while the links between the MGC and the routers are at full capacity. Other recommendations include making the same tests that were executed in this experiment while changing the DSCP marking either in the adjacent routers or in the media gateway (MGW). This research did not test any VoIP-based calls to VoIP-based calls within the same network or between two different VoIP networks. Those are some of the options and ideas that researchers can consider and take into considerations to perform future research studies that are based on this research. Such studies can further strengthen this research and its results.

REFERENCES

[1] Mathiyalakan, S. (2015). "VoIP adoption: Issues & concerns", Communications of the IIMA, Vol. 6, No. 2, Article 3.

[2] Broß, J. F., & Meinel, C. (2008). "Can VoIP live up to the QoS standards of traditional wireline telephony?" In Telecommunications, 2008. AICT'08. Fourth Advanced International Conference on (pp. 126-132). IEEE.

[3] Khitmoh, N., Wuttidittachotti, P., & Daengsi, T. (2014, February). "A subjective—VoIP quality estimation model for G. 729 based on native Thai users", In Advanced Communication Technology (ICACT), 2014 16th International Conference on (pp. 48-53). IEEE.

[4] Singh, P. & Kaur, R. (2014). "VOIP over Wimax: A comprehensive review", International Journal of Computer Science & Information Technologies, Vol.5, Issue 4.

[5] Xiao, Y., Qu, G., & Kiseon, K. (2015). A new DiffServ edge router with controlledUDP. Chinese Journal of Electronics, 24(1).

[6] Cole, R. G., & Rosenbluth, J. H. (2001). Voice over IP performance monitoring. ACM SIGCOMM Computer Communication Review, 31(2), 9-24.

[7] Vijayakumar, M., Karthikeyani, V., & Omar, M. (2013). Implementation of queuing algorithm in multipath dynamic routing architecture for effective and secured data transfer in VoIP. International Journal of Engineering Trends and Technology, 4(4), 1226-1230.

[8] Naeem, M., Naz, S., & Asghar, S. (2013). QoS guarantee for VOIP over wireless LANs. International Journal of Hybrid Information Technology, 6(3), 25-32.

[9] Mohammed, H. A., Ali, A. H., & Mohammed, H. J. (2013). The affects of different queuing algorithms within the router on QoS VoIP application using OPNET. arXiv preprint arXiv:1302.1642.

[10] Rivas, F. J., Díaz, A., & Merino, P. (2013). Obtaining more realistic cross-layer QoS measurements: A VoIP over LTE Use Case. Journal of Computer Networks and Communications, 2013.

[11] Mahajan, S., & Chopra, V. (2013). Performance evaluation of MANET routing protocols with scalability using QoS metrics of VOIP applications. International Journal, 3(2).

[12] Chen, J. J., Lee, L., & Tseng, Y. C. (2011). Integrating SIP and IEEE 802.11 e to support handoff and multi-grade QoS for VoIP-over-WLAN applications. Computer Networks, 55(8), 1719-1734.

[13] Miraz, M. H., Molvi, S. A., Ali, M., Ganie, M. A., & Hussein, A. H. (2017). Analysis of QoS of VoIP traffic through WiFi-UMTS networks. arXiv preprint arXiv:1708.05068.

[14] Charonyktakis, P., Plakia, M., Tsamardinos, I., & Papadopouli, M. (2016). On user-centric modular qoe prediction for voip based on machine-learning algorithms. IEEE Transactions on mobile computing, 15(6), 1443-1456.

[15] Silva, S., Soares, S., Reis, M. J., Neves, F., & Assuncao, P. A. (2017, July). A dynamic programming algorithm to select optimal high-priority voice segments using Arduino. In IEEE EUROCON 2017-17th International Conference on Smart Technologies (pp. 271-276). IEEE.

[16] Baharudin, M. A. B., Quang, T. M., & Kamioka, E. (2015). Improvement of handover performance based on bio-inspired approach with received signal strength and mean opinion score. Arabian Journal for Science and Engineering, 40(6), 1623-1636.

[17] Hoque, M. A., Abbas, H., Li, T., Li, Y., Hui, P., & Tarkoma, S. (2018). Barriers in Seamless QoS for Mobile Applications. arXiv preprint arXiv:1809.00659.

[18] Khiat, A., Bahnasse, A., El Khaili, M., & Bakkoury, J. (2017). SAQ-2HN: A Novel SDN-Based Architecture for the Management of Quality of Service in Homogeneous and Heterogeneous Wireless Networks. International Journal of Computer Science and Network Security (IJCSNS), 17(3), 55.

[19] Smith, L., Jacobi, M., & Al-Khayatt, S. (2018, May). Evaluation of IPv6 transition mechanisms using QoS service policies. In 11th International Symposium on Communication Systems, Networks, and Digital Signal Processing. IEEE.

[20] ITU-T. (1996). Methods for objective and subjective assessment of quality. ITU-T Recommendation, 830.

[21] Al-Sayyed, R., Pattinson, C., & Dacre, T. (2007, February). VoIP and database traffic coexistence over IEEE 802.11 b WLAN with redundancy. In Proceedings of the International Conference on Computer, Information and Systems Science and Engineering (pp. 25-27).

[22] Chen, S., Wang, X., & Jajodia, S. (2006). On the anonymity and traceability of peer-to-peer VoIP calls. IEEE Network, 20(5), 32-37.

[23] Ahmed, D. T., & Shirmohammadi, S. (2012). Improving online gaming experience using location awareness and interaction details. Multimedia Tools and Applications, 61(1), 163-180.

AUTHORS

Dr. Shaher Daoud currently is a faculty member of the School of Computer Science, Colorado Technical University. Colorado Springs, USA. He also has over 28+ years of Telecom industrial working experience.

Dr. Yanzhen Qu currently is a professor of the school of Computer Science, Colorado Technical University, Colorado Springs, USA. He has also worked in the Telecom and Software Development industry for over 20+ years.

INTENTIONAL BLANK

SECURITY ISSUES IN CLOUD-BASED BUSINESSES

Mohamad Ibrahim AL Ladan

Department of Computer Science, Rafik Hariri University, Meshref, Lebanon

ABSTRACT

Cloud-based Business is a Business running and relying on Cloud computing IT paradigm. Cloud computing is an emerging technology paradigm that transfers current technological and computing concepts into utility-like solutions similar to electricity and communication systems. It provides the full scalability, reliability, computing resources configurability and outsourcing, resource sharing, external data warehousing, and high performance and relatively low cost feasible solutions and services as compared to dedicated infrastructures. Cloud-based Businesses store, access, use, and manage their data and software applications over the internet on a set of servers in the cloud without the need to have them stored/installed locally on their local devices. The cloud technology is used daily by many businesses/people around the world from using web based email services to executing heavy complex business transactions. Like any other emerging technology, Cloud computing comes with a baggage of some pros and cons. It is very useful in business development as it brings amazing results in a timely manner; however, it comes with increasing security and privacy concerns and issues. In this paper we will investigate, analyse, classify, and discuss the new security concerns and issues introduced by cloud computing. In addition, we present some security requirements that address and may alleviate these concerns and issues.

KEYWORDS

Cloud-based Business security issues and concerns; Cloud computing security issues and concerns. Cloud computing security requirements.

1. INTRODUCTION

Nowadays every company relies on digital data and services to operate their business. As the amount of data and software applications increase some businesses cannot afford to have them stored and installed on their local premises for various reasons starting from storing huge data and information to using expensive software applications and computing platforms. Businesses started using Cloud computing to take advantage of their many benefits like scalability, reliability, resource sharing, external data warehousing, and high performance and relatively low cost feasible solutions and services as compared to dedicated infrastructures. Cloud computing platform is a net of computing resources, including networks, servers, and applications. It is flourishing across enterprises today, serving as the IT infrastructure driving new digital businesses. It is persuasive for most businesses and an estimated 70% of all enterprises use the cloud for at least one application and its related data [1]. According to Public Cloud Market Research Report, the worldwide market for public cloud will accelerate at a compound annual growth rate of 22.78% during the projection period (2017-2023) [2]. In addition, the number of cloud service providers is growing at a rapid speed due to the increase in the rate of the businesses adopting this new platform to use their many technical and operation management benefits that it offers. As more and more businesses move towards digitization, they will adopt

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 341-352, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90929

one form or the other of the Cloud computing technology. According to a report published by Statista [3] on the current and planned usage of public cloud platform services running applications worldwide in 2018, 80% of enterprises are both running apps on or experimenting with Amazon Web Services. 67% of enterprises are running apps on (45%) and experimenting on (22%) the Microsoft Azure platform. 18% of enterprises are using Google's Cloud Platform for applications today, with 23% evaluating the platform for future use. [Figure 1]

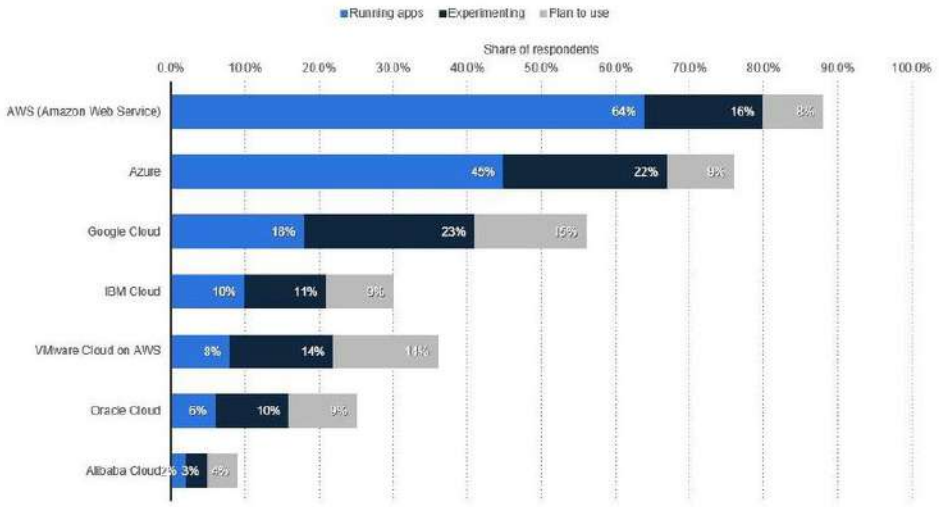


Figure 1: Current and planned usage of public cloud platform services running applications worldwide in 2018.

On the other hand, as security and privacy risks continue to increase globally, businesses cannot risk storing their critical data on remotely located servers that they do not have full control over it and could be subject to security attacks by malicious hackers [1]. Cases such as the Equifax data breach in the fall of 2017, from which the safety and privacy of more than 143 million individuals' data are compromised, have a major hit on the confidence of businesses and their customers in the new platform. Businesses can rarely afford such an enormous hit that badly affect their reputation, and hence, they should study carefully their choices and employ the best cloud security practices [4].

In addition to the general security issues like confidentiality, integrity, availability, legitimacy, and accountability that needs to be individually taken care of, new security issues and concerns are surfaced and need to be addressed properly before fully indulge in cloud computing platform/paradigm/services. Enterprises have to study and evaluate these issues to ensure the manageability and security system of the cloud provider before adopting Cloud computing technology for their businesses.

This paper provides a good presentation, discussion, and a strong overall coverage and classification of the new security issues and concerns of businesses arising from using the Cloud computing technology paradigm, and it gives a good summary of the available requirements and techniques used in handling the different types of security and concerns. The rest of the paper is organized as follows: In section II, we introduce the cloud computing architecture and the different consumption models. In section III, we present and classify the different business security issues and concerns related to cloud computing. In section IV, we discuss some of the main security requirements and measures that must be addressed or taken care of in order to

alleviate the different security issues and concerns. Finally, in section V, we present a conclusion of the paper.

2. CLOUD COMPUTING ARCHITECTURE

The general architecture of cloud computing is shown in Fig. 1 where users can access the cloud computing services using their digital devices through network providers and the internet. Cloud computing users use cloud services on the fly through the Internet and can choose between three different types of services, as explained in what follows, Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or Software as a Service (SaaS).

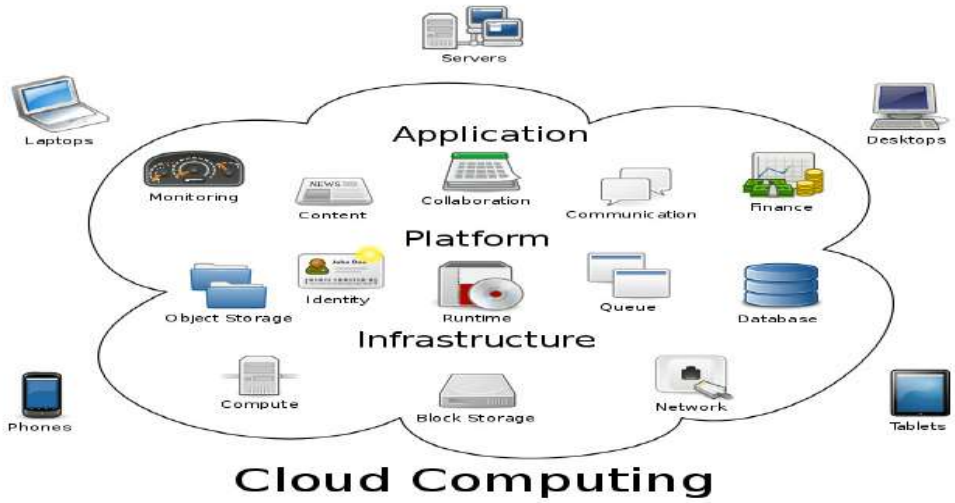


Figure 1: General Architecture of Cloud Computing

Users interact with cloud services provider using native mobile applications or embedded browser applications. Embedded browser applications are developed using standard web development languages (e.g. HTML and JavaScript). Native applications are developed using mobile platform supported programming languages and a set of APIs provided by the cloud services provider.

2.1. Cloud Computing Service Models

Based on the National Institute of Standards and Technology's (NIST) definition of the different cloud models [8], cloud computing services are generally classified into three delivery models, as shown in Figure 2 and Table 1: The Software as a Service (SaaS), the Platform as a Service (PaaS), and the Infrastructure as a Service (IaaS).

2.1.1. Software as a Service (SaaS)

SaaS offers comprehensive applications on demand. It consists of software running on the provider's cloud infrastructure, supplied to one or several clients on demand via a thin client over the Internet. It allows a software company to publish their software and let their users access the software via a web browser. Suite servers like Microsoft Office 365 or applications like Salesforce provide users with instant access to documents and files without the hassle of installing, managing, and storing applications and data on their personal devices.

Users and organizations utilize SaaS applications for additional computer space, added cloud security, ease of updating software, and the ability to synchronize data across many devices. SaaS applications help users avoid software ownership and costly, time-consuming updates and usually work on a monthly or annual subscription-based model. The provider controls and maintains the physical computer hardware, operating systems and software applications. Because of this, SaaS relieves the end users from the labor of software maintenance, continuing operation, and support. Most widely used examples of SaaS include Gmail, Google Docs, Microsoft Office 365, and Salesforce.com [9].

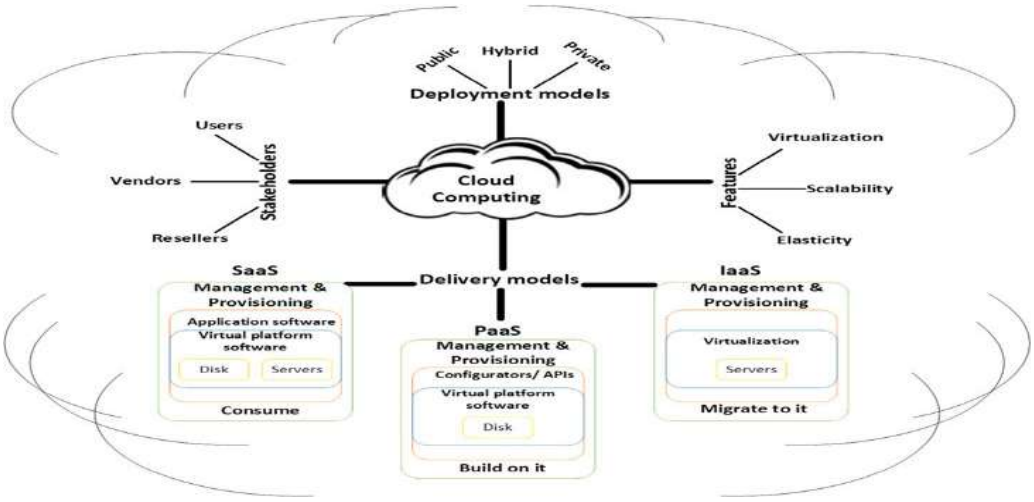


Figure 2: Service delivery models of cloud computing. [5]

2.1.2. Platform as a Service (PaaS)

PaaS provides the end users the platform that includes the operating system, the software development, the programming languages, and the testing tools needed to develop their own applications. It is the delivery of computing platform and solution stack as a service. Businesses can store their clients' data in the platform provider's cloud service, and they can use software, hardware, provided by Cloud computing services to develop, construct, test, and install their own suite of cloud-based apps/services on the Cloud without having to invest in expensive hardware, software licences/tools, operation maintenance, and connectivity. Some examples of PaaS providers include Microsoft Windows Azure, Google App Engine, and Amazon Web Services (AWS).

Table 1: Cloud Computing Service Models and Providers

Cloud Service Models	**Cloud Service Providers**
SaaS	Google Apps, Microsoft 365, IBM, Salesforce.com, and Rackspace.
PaaS	Amazon AWS, Google Apps, Microsoft Azure, SalesForce, Intuit, WorkXpress, and Joyent
IaaS	Amazon Elastic Compute Cloud, Rackspace, IBM, Savvis, VMware, Terremark, Citrix, Joyent, and BluePoint.

2.1.3. Infrastructure as a Service (IaaS)

IaaS offers end users direct access to processing, storage and other computing resources over the network. It is the delivery of computer infrastructure as a service which is sometimes referred to as utility computing. It provides virtual servers with unique IP addresses and chunks of storage on demand using pay-as-you-go method to allow users to pay a single monthly subscription fee based on how many gigabytes or megabytes of data they need to store. Businesses can install and run different software, and have control over operating systems, storage, and installed applications. IaaS is the most flexible cloud computing service that allow organizational users to customize their product combination and enable them to have the most control over their cloud infrastructure although the Cloud service provider owns the equipment and is responsible for housing, running and maintaining it. Some examples of IaaS include Amazon Elastic Compute Cloud (EC2), Joyent, Rackspace, and IBM Computing on Demand.

2.2. Cloud Computing Consumption Models

There are three basic cloud application deployment and consumption models or configurations: public, private, or hybrid clouds. Each offers complementary benefits, and has its own trade-offs [10, 11, 12]. It is very important for businesses to choose the appropriate cloud model based on their needs. This is very important and critical to the safety and security of the Business' operations. Some companies having enormous data so they prefer private clouds while small organizations usually use public clouds. A few companies like to go for a balanced approach with hybrid clouds. Before choosing a cloud model, businesses should be fully aware of the terms of use, service level agreement, and the security and privacy measures implemented in the Cloud model. In what follows, we will give a brief description of each cloud model.

2.2.1. Public Clouds

Public clouds are owned and managed by providers, and applications from different customers are likely to be mixed together on the cloud's servers, storage systems, and networks. However, this model has a variety of inherent security risks that need to be considered. A well architected private cloud properly managed by a provider provides many of the benefits of a public cloud, but with increased control over security. Public clouds are most often hosted away from customer premises, and they provide a way to reduce customer risk and cost by providing a flexible, even temporary extension to enterprise infrastructure.

2.2.2. Private Clouds

Private clouds are client dedicated and are built for the exclusive use of one client, providing the utmost control over data, security, and quality of service. The enterprise owns the infrastructure and has control over how applications are deployed on it. If the private cloud is properly implemented and operated, it has reduced potential security concerns. A managed private cloud may enable enterprise customers to more easily negotiate suitable contracts with the provider, instead of being forced to accept the generic contracts designed for the consumer mass market that are offered by some public cloud providers. Private clouds may be deployed in an enterprise datacenter, and they may be deployed at a co-location facility.

2.2.3. Hybrid Clouds

A Hybrid cloud involves a combination of both public and private cloud models. They can help to provide on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to maintain service levels in the face of rapid workload

fluctuations. Enterprise Computing and private cloud extend outward to consume public compute resource for peak need or deliver on Industry cloud. An example is using commodity resources from a public cloud such as web servers to display non-sensitive data, which interacts with sensitive data stored or processed in a private cloud. Focus primarily on proprietary data centers, but rely on public cloud resources to provide the computing and storage needed to protect against unexpected or infrequent increases in demand for computing resources.

3. CLOUD COMPUTING SECURITY CONCERNS

The Cloud computing platforms, like any other IT platforms, are vulnerable and subject to a variety of malicious attacks that may affect sensitive business data and applications. In addition, a cloud provider usually hosts numerous clients; each can be affected by actions taken against any one of them. When any threat came into the main server, it affects all the other clients also. Businesses should choose a cloud provider who can meet their security standards set by their company's internal policies and government agencies. They must carefully read the service level agreement and understand the provider's policies, terms, and security measures.
Security experts in the field of Cloud computing have identified several critical security issues and concerns. These include the following:

- Data breaches and loss.
- Incomplete data control.
- Inability to monitor data in motion.
- Denial of Service.
- Insecure Application Programming Interfaces.
- Vulnerable systems and applications.
- Host Access Management.
- Lack of consistent security controls over multi-cloud and on-premises environments.

In general, we can classify the Cloud computing security issues and concerns into four main classes as shown below in figure 3. In what follows, we will discuss each class in more details.

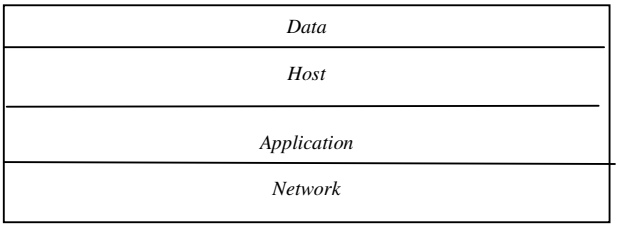


Figure 3: Different Classes of Cloud Computing Security issues and concerns.

3.1. Data Security

Most Cloud computing security issues and concerns are directly or indirectly related to data security. Whether a lack of visibility to data, inability to control data, or theft of data in the cloud, most issues come back to the data customers put in the cloud. Individuals and enterprises take advantage of the benefits for storing large amount of data on a cloud. However, by using Cloud computing businesses have concerns and fear of so many security issues related to data access control, integrity, protection, and data location [22]. Businesses count on cloud content management platforms from vendors such as Dropbox, Google, and Microsoft to access, store and share data and files within an enterprise repository. However, there are security concerns about this information falling into the wrong hands and be subject to phishing attacks and

malware. In what follows in this section, we will discuss the main security issues and concerns related to data in cloud computing.

3.1.1. Data Access Control and Authentication

Different authentication mechanisms have been presented and proposed using cloud computing to secure the data access suitable for cloud environments. Some uses the open standards and even supports the integration of various authentication methods. For example, the use of access or login IDs, passwords or PINS, authentication requests, etc. Sometimes confidential data can be illegally accessed due to lack of secured data access control. Sensitive data in a cloud computing environment emerge as major concern with regard to data security in cloud computing.

3.1.2. Data Integrity

Data integrity is essential in cloud computing. Every cloud user must ensure the integrity of their data stored on the cloud. Errors may occur when data is entered or transmitted from one computer to another. It could also occur because of some hardware malfunctions, such as disk crashes, software bugs or viruses. Every access a cloud user make must be authenticated and verified. Different approaches in preserving integrity for one's information that is stored on the cloud is being proposed. For example, every access a user make must be authenticated assuring that it is his/her own information and thus verifying its integrity.

3.1.3. Data Confidentiality and Protection

Cloud computing allows users to store their own information on remote servers, which means content such as user data, financial data, business data, videos etc., can be stored with a single cloud provider or multiple cloud providers. When users store their data in such servers, data confidentiality is a necessity. Storing of data in remote servers also arises some privacy and confidentiality issues among individual, business, government agency, etc., each customer data in the public cloud environment are exposed to internet. Cloud computing services should require reliable processes for protecting data before, during, and after any operation.

3.1.4. Data Theft

Cloud computing uses external data server for cost effective and operation flexibility. Therefore, there is a risk of data being stolen from the external server.

3.1.5. Data Loss

Data loss is a very serious concern in cloud computing since they are stored on premises that they have no control over. Customers may lose data as a result of a major server crashes, a hacker's attack on main and backup servers, or due to financial or legal problems with the service provider.

3.1.6. Data Location

Cloud computing customers do not always know the location of their data. The provider does not reveal where all the data are stored. In addition, cloud computing offers a high degree of data mobility, so data could be very far away from the location of the customer and could be on different servers in different countries [23]. In addition, location of data may have considerable effects on the privacy and confidentiality, on information protection, and on privacy obligations for those who process or store the data.

3.2. Host Security

Host security concerns are those which affect the host infrastructure when it is connecting itself to the cloud computing. They are directly related to virtualization vulnerabilities and weak access control in public cloud environment.

In the IaaS model, customers are primarily responsible for securing the host provisioned in cloud. They are accountable for security management of the guest VM. Cloud service provider recommends the customer to use SSH to manage the VM instances. The attacker may steals the SSH private keys that are used to access and manage virtual instances. This can be eliminated by storing the private keys on system in an encrypted form [13]. Other host security threats related to virtual machine security is attacking the vulnerable services like FTP and NetBIOS. It is recommended to run only the necessary services and turn off the unused services that are not required. Some more security threats like capture user accounts that are not properly protected with strong password, attack the systems that are not properly protected by host firewalls and deploy Trojans embedded in the VM software component or within the VM image itself. Cloud service provider must ensure that the strong operational security procedures are followed to secure the virtual machine from these threats.

In PaaS and SaaS models, cloud service providers do not share their host platform and the host operating system with their customers, therefore, host security responsibility is transferred to the cloud service provider. As a result of that, PaaS and SaaS customers should get the appropriate level of guarantee from the cloud service provider about their host security [13].

3.3. Application Security

In cloud computing platform, any application or software that is used does not reside on the machine of the actual user, and if this software/application has vulnerabilities then it can have a negative impact on the security of all the customers using the cloud. These vulnerabilities can lead to compromising security, and can affect the availability of cloud computing. Traditional security mechanisms such as network firewalls, network intrusion detection and prevention mechanisms do not adequately satisfy being used as a solution for application vulnerabilities [20, 21]. The typical security issues arising with applications technology are: Session riding, hijacking and injecting vulnerabilities. Other web application specific vulnerabilities are browser's front-end components in which, data sent from the user component to server component is manipulated. XML signature attacks, browser based attacks for cloud authentication are other examples of application vulnerabilities that can affect the cloud computing security. Application security is the main threat to SaaS platform.

3.4. Network Security

Network related security issues are considered to be the biggest security challenges in clouds since cloud computing is more prone to network related attacks compared to the traditional computing paradigms [14]. In addition, cloud computing are tightly coupled and highly depend on networking. The ratio of network attacks and fraud radically increases as people and organizations migrate their data into clouds. Security experts anticipate that clouds will be the focus of hackers in future due to the concentration of valuable data, application, and information within the clouds. Some of these security issues and concerns are the results of the following gaps: The possible lack of proper installations of network firewalls and the overlooked security configurations within clouds and on networks make it easier for hackers to access the cloud on behalf of legitimate users. Hackers can run malicious code to control hardware and software

resources. Internet access problems due to some kind of attacks make Cloud computing services unavailable. Therefore all the network reliability issues will have direct implication on the cloud computing. Other more specific security issues that are network-related and may affect directly the access control restrictions of cloud resources include the following:

3.4.1. Denial of Service Attacks

Most of the serious attacks in cloud computing come from denial of service (DoS), particularly HTTP, XML and Representational State Transfer (REST)-based DoS attacks. The cloud users initiate requests in XML, then send requests over HTTP protocol and usually build their system-interface through REST protocols such as those used in Microsoft Azure and Amazon EC2. Due to weaknesses in the system interface, DoS attacks are easier to implement and very difficult for security experts to countermeasure [15]. XML-based distributed denial of service (DDoS) and HTTP-based DDoS attacks are more destructive than traditional DDoS because these protocols are widely used in cloud computing with no strong deterrence mechanisms available to avoid them. HTTP and XML are critical and important elements of cloud computing, so security over these protocols becomes critical to providing safe and secure cloud computing model.

3.4.2. Issue with Reused IP Addresses

With respect to cloud provider the IP address is the billable entity. It will be reassigned and reused by new user when the existing users no more using that IP address. From the customer perspective it can pose the security risk to their resource access by some other user due to the time delay between the change of an IP address in DNS and clearing that address in DNS cache. The similar time delay may occur for changing physical address in ARP tables and clearing that address from an ARP cache. With the impact of this issue, the Amazon web services a leading cloud provider has announced the elastic IP address, by which the customers are assigned with a set of routable IP address and they have control over that IP address until they release it. [16] However, the issue can persist in non-routable IP addresses where the customers can reach the provider's network via the private address. [17]

3.4.3. Limited Auditing Capability

A business using a public cloud irrespective of any type of service models face the significant risk in their data. They have limited ability to access the network-level logs and audit the cloud provider operations [18].

3.4.4. Attack Against SSL\TLS

Secure Socket Layer and Transport Layer security is the protocol used to create an encrypted channel to provide communication over the public cloud. Many cloud providers support this protocol to provide secure communication. Authors in [19] presented a new attack by which the hackers are able to break the SSL encryption in millions of websites. This attack named as BEAST (Browser Exploit Against SSL\TLS). This suggests that even HTTPS cookies are no longer secure of this template.

4. DISCUSSION

For a wider adaptation of cloud computing services by businesses, the security issues and concerns need to be addressed more seriously at various levels. When you do not own the network, it is open to the rest of the world, and you do not control the security layers of the cloud infrastructure, the cloud computing will not be as secure as storing data and applications on your

own premises. Hence providing the suitable security measures that overcome the security risks in cloud computing are necessary when a business is transferring to cloud. Moreover, not every business has sufficient knowledge about the implementation of the cloud solutions, and not every business has the expert staff and the right tools to use the cloud computing in a proper and safe way. Businesses should be aware of the threats, and risks involved in using public cloud environments when considering outsourcing data, applications and infrastructure to a Cloud computing platform in general and to a public cloud in particular. For businesses to protect their data on the cloud, they should inspect and study their cloud provider's security measures, and their terms of use and conditions in case hacking and breaching incidents occur. In addition, they should train their employees on the different processes and tools of cloud computing, and they should be able to verify the integrity and safety of their data and information before and after being stored on cloud resources. In addition, they should be able to determine who can enter data into the cloud, track transactions and operations to identify abnormal behaviors, secure and strengthen network traffic analysis tools. All of the above are rapidly becoming standard measures in protecting utilizations of cloud computing infrastructure. [6]

In general, businesses should follow some guidelines in order address and alleviate the main security issues and concerns in cloud computing. These guidelines include the following: Understanding the different Cloud computing platforms and the type of services offered by the cloud provider, making sure that the selected Cloud computing solution fulfill their security requirements, and maintaining responsibility and accountability over the security of data and applications implemented and deployed on the Cloud.

5. CONCLUSIONS

Cloud computing is a new concept for most businesses and it is very difficult for them to verify that Cloud providers meet the security requirements standards to address security threats and concerns. Hence, every business should treat security issues and concerns very seriously. A lot of research works have been done related to cloud computing security issues that have resulted in several security methods and measures that can be used to alleviate the security risks in cloud computing. Many researchers and practitioners worked and are working on identifying cloud threats, vulnerabilities, attacks, and other security issues, in addition to proposing countermeasures in the form of frameworks, strategies, service oriented architectures, and recommendations [28, 30, 31]. However, providing a comprehensive security framework intended to support all types and levels of security issues and concerns is not available yet.

In this paper, we have introduced and presented the cloud computing architecture and the different consumption models, in general, and we have presented, discussed, and classified the different security issues and concerns that businesses should be aware of when using Cloud computing. Furthermore, we have presented and discussed the different measures and requirements that can be put in place to address the major security risks. The paper can be considered as a very good starting reference for those researcher that are planning to work on security issues in cloud computing and for businesses planning to enter to the world of Cloud computing.

REFERENCES

[1] The 2018 Cloud Security Guide: Platforms, Threats, and Solutions. Cloud security is a pivotal concern for any modern business. Learn how the cloud works and the biggest threats to your cloud software and network, July 31, 2018. https://www.secureworks.com/blog/cloud-security-guide-to-platforms-threats-solutions.

[2] Public Cloud Market 2018: Global Size, Share, Growth Opportunities, Emerging Trends, Sales Revenue, Key Players Analysis, Future Prospects and Regional Forecast to 2023. Oct 24, 2018. https://www.marketwatch.com/press-release/public-cloud-market-2018-global-size-share-growth-opportunities-emerging-trends-sales-revenue-key-players-analysis-future-prospects-and-regional-forecast-to-2023-2018-10-24

[3] Statista, Current and planned usage of public cloud platform services running applications worldwide in 2018. https://www.statista.com/statistics/511467/worldwide-survey-public-coud-services-running-application/

[4] Sara Ashley O'Brien, Giant Equifax data breach: 143 million people could be affected. September 8, 2017. https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html

[5] Iqbal, S et al. Service delivery models of cloud computing: security issues and open challenges. Security and Communication Networks 2016; 9:4726–4750. 30 August 2016.

[6] Cloud Computing Security Issues and Solutions. https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/security-issues-in-cloud-computing.html.

[7] ReportsnReports, http://www.kuam.com/story/26655451/pricing-the-cloud-2014-market-research-report-with-2019-cloud-computing-pricing-and-revenue-forecastsDALLAS, September 29, 2014.

[8] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication 800-144, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494, Dec. 2011.

[9] R. D. Caytiles and S. Lee, Security Considerations for Public Mobile Cloud Computing, International Journal of Advanced Science and Technology, Vol. 44, July 2012.

[10] NEC Company, Ltd. and Information and Privacy Commissioner, Ontario, Canada. "Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach, http://www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf, 2010.

[11] https://wiki.cloudsecurityalliance.org/guidance/index.php/Cloud_Computing_Architectural_Framework.

[12] H. T. Dinh, C. Lee, D. Niyato and P. Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches", Wireless Communications and Mobile Computing – Wiley, Available at http://www.eecis.udel.edu/~cshen/859/papers/survey_MCC.pdf.

[13] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)," O'Reilly Media, Sep. 2009; ISBN: 9780596802769.http://oreilly.com/catalog/9780596802776.

[14] I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud Computing Security: A Survey", computers journal, www.mdpi.com/journal/computers, ISSN 2073-431X, Feb 3, 2014.

[15] Karnwal, T.; Sivakumar, T.; Aghila, G. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In Proceedings of the 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 1–2; pp. 1–5, March 2012.

[16] Announcing Elastic IP addresses and Availability Zones for Amazon EC2," http://aws.amazon.com/about-aws/whatsnew/2008/03/26/announcing-elastic-ipaddresses-and-availability-zones-for-amazonec2/

[17] RFC1918, "Address Allocation for private Internets," http://tools.ietf.org/html/rfc1918

[18] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)," O'Reilly Media; ISBN: 9780596802769, Sep. 2009.

[19] "Hackers break SSL encryption used by millions of sites," http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/

[20] Danny Harnik, Elliot K. Kolodner, Shahar Ronen, Julian Satran, Alexandra Shulman-Peleg, and Sivan Tal. Secure access mechanism for cloud storage. Scalable Computing: Practice and Experience, 12(3), 2011.

[21] B. Hay, K. Nance, and M. Bishop. Storm clouds rising: Security challenges for IaaS cloud computing. In 2011 44th Hawaii International Conference on System Sciences (HICSS), pages 1-7. IEEE, January 2011.

[22] Serrao, G.J., "Network access control (NAC): An open source analysis of architectures and requirements", IEEE International Carnahan Conference on Security Technology (ICCST), pp 94 - 102 , San Jose, CA, USA, Oct. 5-8, 2010.

[23] Anitha Y, "Security Issues in Cloud Computing - A Review", International Journal of Thesis Projects and Dissertations (IJTPD), Vol. 1, Issue 1, PP: (1-6), Month: October-December 2013.

[24] Tim Mather, Subra Kumaraswamy, and Shahed Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, October 2009

[25] Zhang Yandong and Zhang Yongsheng. Cloud computing and cloud security challenges. In Information Technology in Medicine and Education (ITME), 2012 International Symposium on, volume 2, pages 1084-1088.

[26] Syed Mujib Rahaman and Mohammad Farhatullah. PccP: a model for preserving cloud computing privacy. In Data Science & Engineering (ICDSE), 2012 International Conference on, pages 16-170, 2012.

[27] G. Kulkarni, J. Gambhir, T. Patil, and A. Dongare. A security aspects in cloud computing. In 2012 IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS), pages 547-550, June 2012.

[28] Wang, C.; Wang, Q.; Ren, K.; Lou, W. Towards secure and dependable storage services in cloud computing. *IEEE Trans. Serv. Comput.* 2012, *5*, 220–232.

[29] J R Jiang, J P Sheu, C Tu, J W Wu, " A secure anonymous routing protocol for wireless sensor networks", IEEE Journal of Information Science and Engineering, Vol. 680, Issue 2, 2010, Pages: 657-680.

[30] Sabahi, F. Virtualization-level security in cloud computing. In Proceedings of the 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), Xi'an, China, 27–29 May 2011; pp. 250–254.

AUTHOR

Prof. Mohamad Al Ladan has over 19 years of teaching and training experience in the area of computer hardware & software and Information Technology. He received the M.Sc. and the Ph.D. degrees in Computer Engineering from Syracuse University, Syracuse, N.Y., USA, in 1990 and 1995 respectively. He is a reviewer for different international conferences and journals. He is currently a full professor of computer science and the Dean of the College of Sciences and Information Systems at Rafik Hariri University in Lebanon.

ENABLING EDGE COMPUTING USING CONTAINER ORCHESTRATION AND SOFTWARE DEFINED WIDE AREA NETWORKS

Felipe Rodriguez Yaguache[1] and Kimmo Ahola[2]

[1,2]5G Networks & Beyond, Technical Research Centre of Finland (VTT), Espoo, Finland

ABSTRACT

With SD-WAN being increasingly adopted by corporations, and Kubernetes becoming the de-facto container orchestration tool, the opportunities for deploying edge-computing applications running over SD-WAN are vast. Unfortunately, service orchestration in SD-WAN has not been provided with enough attention, resulting in the lack of research focused on service discovery in these scenarios. In this document, an in-house service discovery solution that works alongside Kubernetes' master node for allowing an improved traffic handling and better user experience is developed. The service discovery solution was conceived following a design science research approach. Our research includes the implementation of a proof-of-concept SD-WAN topology alongside a Kubernetes cluster that allows us to deploy custom services and delimit the necessary characteristics of our in-house solution. Also, the implementation's performance is tested based on the required times for updating the discovery solution according to service updates. Finally, some conclusions and modifications are pointed out based on the results, while also discussing possible enhancements.

KEYWORDS

SD-WAN, Edge computing, Virtualization, Kubernetes, Services

1. INTRODUCTION

Virtualization is the cornerstone of Internet and the cloud-based services, it has evolved from a cost saving solution to the technology capable of providing the required agility and flexibility needed for service delivery in data centers as well as the infrastructure supporting business essential applications. The main goal of virtualization is the optimization of IT assets, helping in achieving a superior system utilization, cost reduction, and ease of deployment and management by allowing multiple operating system images to run in parallel using only one piece of hardware. Container-based virtualization and Virtual Machines (VMs) are perhaps the most common types of virtualization, although there are many differences among them, they both have the necessity to communicate within an IP network. Before the execution of a container or VM, they need to be assigned IP and MAC addresses. When these virtualized entities are assigned IP addresses, the traditional Ethernet and IP networks are stretched to exist inside the physical hosts located in data centers, not only between them. Virtualization alongside cloud-computing suppose a challenge in the application of traffic engineering for maximizing the utilization of the available conventional networks [1].

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 353-372, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90930

Traditional communication networks are distributed systems with multiple routing algorithms running over many different devices such as routers and switches. Every single one of these devices possesses its own configuration and state, and must be configured separately, which makes networks difficult and expensive to maintain and migrate. Software Define Networking (SDN) tackles this issue through the separation of the control plane from the data plane. This is achieved by moving the control logic of the network to a centralized controller, transforming the switches into mere forwarding devices that follow the rules set by the controller. By centralizing the control logic, configuration and maintenance becomes easier, with new features being able to be deployed much faster as well. A centralized control has information regarding the whole network, being able to optimize the available network resources. SDN is therefore widely spread among data centers, especially in order to cope with the virtualization and cloud-computing related issue [1].

Edge computing has arisen as a new approach that alongside SDN could be able to offer a solution to network optimization in cloud environments. This new perspective is nothing more than reducing the number of processes running in the centralized cloud, and moving them to local available edge servers. However, as data processing power is moving towards the edge of a network in the form of containers instead of remaining in a cloud or data center, migration is also occurring for services or applications. This trend requires the usage of processing power from devices that are not capable of being constantly connected to the network, this is the case of laptops, smartphones, wireless sensors, etc. The more this approach is adopted, the more businesses think their Wide Area Networks (WANs) are not prepared to carry such a burden, especially when taking into account traditional corporate WANs. Such networks are built by backhauling routed services and Internet traffic throughout the main office, which can cause performance issues when combined with edge computing. It is obvious that traditional approaches lack the agility and flexibility to achieve the required performance and availability needed by edge computing [2].

1.1. Methodology

In this work we propose a simple service discovery system that will improve bandwidth usage when accessing containerized services over a SD-WAN environment. This work was performed in three main steps that include: the selection of use cases and design of the SD-WAN topology, a testbed implementation for the observation of data flow that will allow us to identify the required behavior of our service discovery, and results analysis focusing on a user experience approach. The first step takes into account the limited amount of research aiming at the merge of edge computing, SD-WAN and container orchestration. The envisioned use cases cover scenarios applicable on an enterprise level and the topology is conceived to simulate a distributed network. The second step comprises the simulation of the aforementioned network topology in order to provide the experiment with a real-life WAN environment. This allows the deployment of in-house services and testing of bandwidth usage and request redirectioning when performing container orchestration. ONOS was selected as the SDN controller, it is written in Java and was chosen for being an extremely reliable and well tested solution, with an active network of developers working on it as well as a more than enough number of already available applications. Simulation will be done using Mininet, a virtual network simulator that uses Linux namespaces for separating individual nodes in simulated network. Although the SD-WAN gateways simulated using Mininet will be running in the same host, they can as well be deployed in different physical machines as well as NoviFlow or Pica8 switches. In the final step, the implementation is

validated based on discovery and convergence time, the whole system will be examined looking for problems and limitations that shall be discussed so improvements can be proposed.

1.2. Related Work

A few works have somehow dive into service discovery orchestration in SDN networks. In [10] Jarraya et al. analyzed the importance of computing and storage orchestration alongside networking resources as a quite important part in SDN, while also taking into account the lack of research that aims at easing the creation and deployment of network services. In [11] Kreutz et al. identify computing infrastructure and networking challenges, presenting a series of constraints that must be overcome in order to improve efficiency by means of network orchestration. The aforementioned works focus on cloud computing resources orchestration on a data center environment having and underlying SDN network. In [12] Taleb et al. discusses the role of service orchestration in the success of Multi-access Edge Computing environment, but this mainly focuses on the orchestration of networking resources and containerized services orchestration is not explored. On the other hand, our work focuses on the discovery of deployed containerized services, indirectly achieving a slight improvement in the usage of network resources performing orchestration between the container orchestrator and the in-house service discovery.

1.3. Structure

This paper is organized as follows: In section 2 we define our use case and the network topology that will be simulated. In section 3, a summary of the implementation is presented as well as of every constituent part of the system. Finally, in section 4 we define the parameters for carrying out measurements, the results and their corresponding discussion are also presented.

2. USE CASE

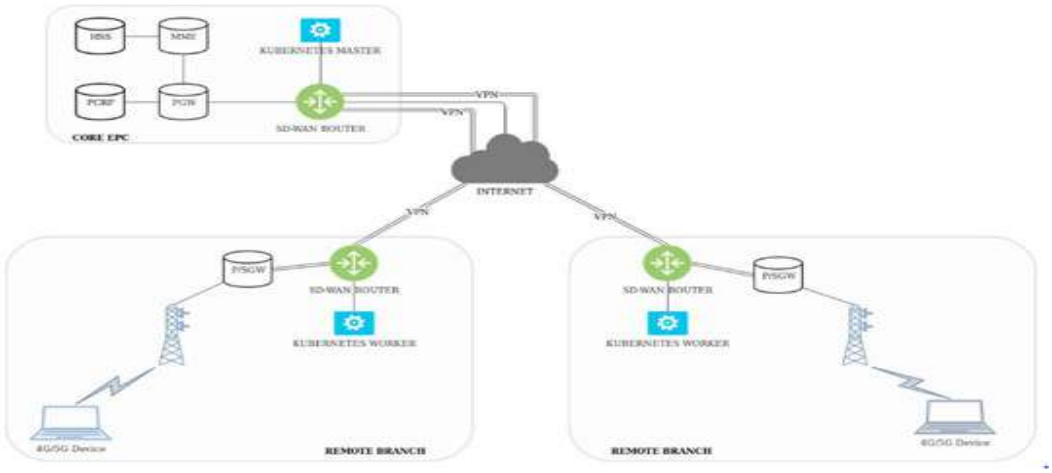


Figure 1. Use case topology

With SD-WAN being the natural extension of SDN and Kubernetes becoming the de-facto container orchestrator, the possible use cases for an Edge Computing case are really high in

number. In the present use case, a Kubernetes master node will be deployed in the Central Office (CO) alongside the proposed orchestrator that will be aware of the changes happening in the Kubernetes cluster and will react accordingly. The development of this orchestrator will enable the possibility of deploying container workloads on remote branch locations and, at the same time, facilitating access towards its services by properly discovering the nodes containing them. In Figure 1, the proposed topology including the required 5G network for allowing the implementation of local breakout is depicted.

The advent of internet connected endpoint devices that are commonly not associated with internet and possess a unique identity, is known as Internet of Things (IoT). This enables the deployment of workloads that can be of an almost infinite variety, all of them focusing on the processing of IoT generated data. The use cases this work will focus comprises the following: smart web pages, authentication applications and the already mentioned IoT data processing. Each of these use cases have different requirements and set ups. The smart web page can possess three main components, a front-end, a web application, and the logic, each of these three components can be deployed in different Kubernetes workers while the Kubernetes master perform load balancing. Network requirements will be low latency and dynamic route adaptation in case a Kubernetes worker is replaced or moved. The authentication application can be deployed into one remote branch, then all authentication queries coming from closer branches will be redirected towards it instead of going to the CO, this will require the discovery of the closest node running the authentication application. Finally, for IoT data processing use case, some branches can generate the data by using sensors and storing it in an Kubernetes worker, while the data processing unit can be deployed in a different worker node. The massive amount of traffic generated by sending and receiving raw data as well as processed data should not be directed through Kubernetes master node in the central office unless this is strictly necessary. The need of dynamic, external service discovery is evident. Although SD-WAN is just starting to be adopted, the integration with Kubernetes will definitely easy the deployment of applications and provide an improvement in the user experience. Due to the lack of commercial solutions that provide Kubernetes service discovery in a SD-WAN environment, the proposed paradigm can be further developed as a viable business idea.

3. IMPLEMENTATION

The testbed for the orchestrator proof-of-concept was implemented as three interconnected virtual machines running on a Linux server located at VTT Espoo premises and having Ubuntu 18.04 LTS as host operating system. Each of the aforementioned virtual entities plays a different role: SD-WAN network simulation, Kubernetes master node and Kubernetes worker node. A complete, in depth description of every entity will be done, taking into account the complexity of the final system. First, we have the SD-WAN network simulation virtual machine. This entity contains the OpenFlow speaking SDN controller as well as all the Mininet simulated gateways and hosts, providing an underlying physical network. Gateways are connected to each other through a set of Open vSwitch virtual switches that emulate the internet. The protocol used for the communication between these gateways is BGP, which was implemented by using Quagga [3]. Each of the gateways represents a corporation's branch office, which are perfectly capable of hosting either a Kubernetes master or worker node and the services on them. The SDN controller is ONOS [4], for this work the version of ONOS used is 14. ONOS controller is deployed by using Docker alongside ATOMIX for supporting the creation of extra ONOS instances, effectively forming a cluster [5]. ONOS is a controller written in Java and offers high modularity

in the form of a wide variety of applications that can be activated depending on the developer's needs [4].

The SDN controller runs on the virtual machine and the gateways communicate with it through the main BGP speaker that is located at the main office. An ATOMIX cluster consisting of three nodes is used for relieving the ONOS instances from cluster management, service discovery and data storage functions. The created ATOMIX cluster is configured through a JSON configuration file describing each constituent node. This configuration file includes information regarding each node's discovery and communication methods, management partition configuration and storage and replication partition configuration. In this work, the discovery protocol specified is Raft, ONOS entities are not listed during the discovery configuration due to the connection between ATOMIX and ONOS being of a client-server type. Raft was also used in ONOS's former releases for cluster formation, however, it requires strict cluster membership information in order to successfully form a cluster. With the adoption of ATOMIX as a separate cluster using Raft, all the ONOS nodes can easily discover peers by using dynamic discovery mechanisms, supporting the failure of all by one node [5].

Next, we have the Kubernetes master node virtual machine. The master node is connected to one of the gateways through a Linux bridge created for this solely purpose, the virtual interface located on the SD-WAN virtual machine is loaded to Mininet, therefore simulating a direct connection. In order to successfully deploy the master node, kubeadm, kubelet and kubectl alongside Docker must be installed in the virtual machine. The master node is not a single entity, it is the result of a combination of a group of pods, each of them having a specific function. Each of the pods that conform the master will have one or more containers that are created using Docker, among them, the Container Network Interface (cni). The cni will provide an IP address to every single one of the created pods and is also in charge of the whole networking for the pod network, including the internal DNS service. Once the master node is ready, the gateway to which it is attached will serve as a gateway for both, a host machine and the master node. Host machines are able to connect remotely to the master and create pods, deployments or expose services, although this is not straightforward. The security certificates must be copied to the host machine first, among the copied files there is the configuration archive containing the master's IP address and port number, allowing kubectl command to know the right destination of its queries. Due to security reasons, the master node will not be scheduled any pod and only a limited, selected number of hosts are able to access the cluster to deploy or delete services.

Finally, there is the Kubernetes worker node virtual machine. In the same way as the master node, the worker node is attached to a gateway through a Linux bridge and the corresponding virtual interface in the SD-WAN virtual machine is also loaded to Mininet. Configuration required for this node is quite minimalist in comparison with what is required for the master node, although kubeadm, kubelet, kubectl and Docker must also be installed. At least in the beginning, the worker node will not run as many pods as the master node, as most of the required services are handled by the master node. Through the use of labels, pods can be scheduled to the worker node, which allows a better resource usage, taking into account that Docker containers are not created in the master node, but in the worker node. Worker node's pods are also assigned an IP address inside the specified pod-cidr-range by the cni. In this work, the separation of the conforming entities into different virtual machines, was done with solely purpose of increasing the isolation between running software, specially conflicts between Kubernetes and Docker. Considering a dockerized version of ONOS is used, any issue affecting the performance of Docker would

definitely hinder any effort carried out while building the proof-of-concept testbed. In Figure 2 the different virtual machines and some of the elements running on them can be seen.

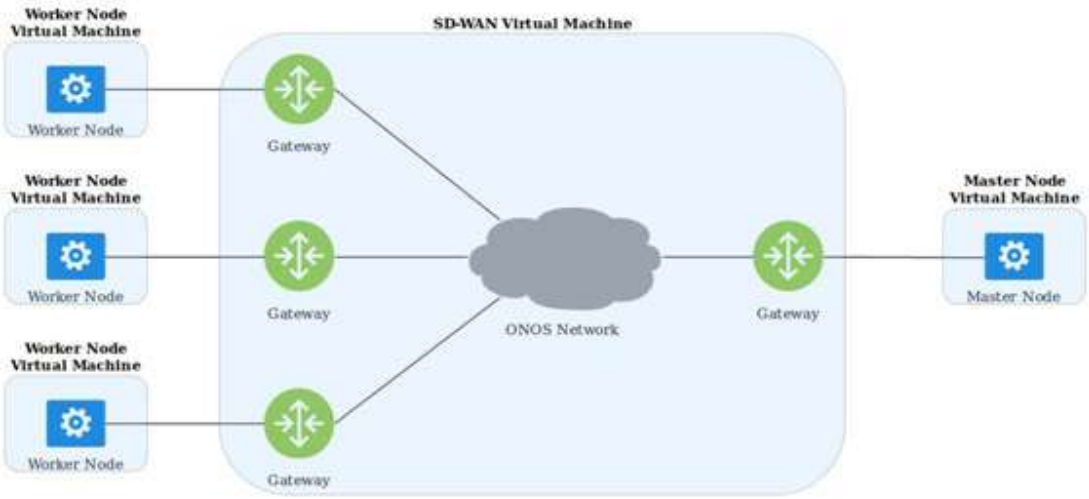


Figure 2. High level network overview representing the different virtual machines.

3.1. Domain Name Service (DNS)

Kubernetes schedules a DNS pod and service in the master node with the purpose of serving individual containers by resolving a DNS name to its corresponding IP address, therefore directing their requests to the proper node. When a service is created in the cluster, it is assigned a DNS name, which will be used by a client pod during its queries in both, the client's pod namespace as well as the cluster's default domain. As an example of the DNS principles in Kubernetes, we can imagine a service called "Hello-world" scheduled in the namespace "kuber-system", a query coming from a pod also located in "kuber-system" must only ask for Hello-world. On the other hand, a pod running in namespace "test-system" must look up for the service with a query for hello-world.kuber-system [6].

This scenario represents the behaviour of the internal DNS, this means that only entities belonging to the Kubernetes cluster will be able to take advantage of it. In the proposed smart branch scenario, most of the requests will come from hosts located outside the cluster, they can not make use of this internal DNS service. For connecting to services from outside the cluster, Kubernetes offers three solutions: accessing services through a public IP, accessing services through the Proxy Verb, and accessing the services from a node or pod in the cluster. The first option requires the use of the NodePort or a LoadBalancer service type, the service will be exposed either on the internet or limited to a corporate network. Its limitations are due to the fact that a request to the service will be performed using the syntax <master/worker node ip>:NodePort, making it necessary for the end user to know the node's IP address. A query sent to the master node will produce another request heading from the master node towards the worker, creating an unnecessary overhead [7]. Next, we have the Proxy Verb. This solution works exclusively for HTTP/HTTPS services and may cause issues with some web services, it also performs some authentication and authorization at apiserver level before granting access to the service. The last option is to access a service using a pod or node. It must be taken into account that although some nodes or pods might be accessed in this way, this is a non standard method,

and the environment varies depending on the host, some tools might or might not be installed. Neither of the aforementioned methods is viable from the end user's perspective, being either too complex of posing a security risk for the company when exposing IP addresses of nodes containing vital services [7].

To overcome the aforementioned IP sharing issue, an external DNS service, written in python, was conceived. Every gateway in the SD-WAN virtual machine will run their own DNS server, the service is bound to the interface heading towards the host subnetwork and listening on port 53. The server will load the zones from a .txt file containing the zone entries regarding all the available Kubernetes worker nodes, the DNS names for worker nodes have been formed by adding the node's name and a predetermined suffix. Hosts will access the available services located at the closest node under the entry "vtt.kubernetes.services". The remote non-local available services will have entries that correspond to their respective worker node name followed by the suffix ".kubernetes.services". As an example, let us assume a cluster with two worker nodes worker1 and worker2. For hosts located closer to worker1, the zone file will be as shown in Figure 3, whereas for those closer to worker2, Figure 4 shows the corresponding entry.

```
# Zones entries for external DNS service
#

vtt.kubernetes.services A 192.168.200.2
worker2.kubernetes.services A 192.168.201.2

#
#
```

Figure 3. Custom DNS entries for hosts close to worker1.

```
# Zones entries for external DNS service
#

vtt.kubernetes.services A 192.168.201.2
worker1.kubernetes.services A 192.168.200.2

#
#
```

Figure 4. Custom DNS entries for hosts close to worker2.

By making use of this service, whatever host is connected to the corporate network, close to worker1 will be able to access the services located in the node by making a request to <vtt.kubernetes.services>:<NodePort>, and services in worker2 by using <worker2.kubernetes.services>:<NodePort> saving efforts of sharing the IP address of any node in the cluster or limiting access for only certain types of traffic. When a host located behind one of the gateways sends a query for certain services, the request will not go to the master node, but instead will go directly to the worker node running the service, as it can be appreciated in Figure 5, where the dashed lines represent a normal request, going through the master node. The continuous lines represent a direct request, enabled by the orchestrator, performed towards the worker node. This approach avoids the overhead of sending a request to the master and it sends

another request to the worker node on behalf of the host. A python based DNS server was preferred at this stage due to the simplicity of using a .txt file for loading zones, being able to format the zones at will, and the easiness of making changes and binding the server to any IP address or interface without the need to install, stop or restart a service. However, solutions like bind 9 would definitely be a preferred option on a production environment.

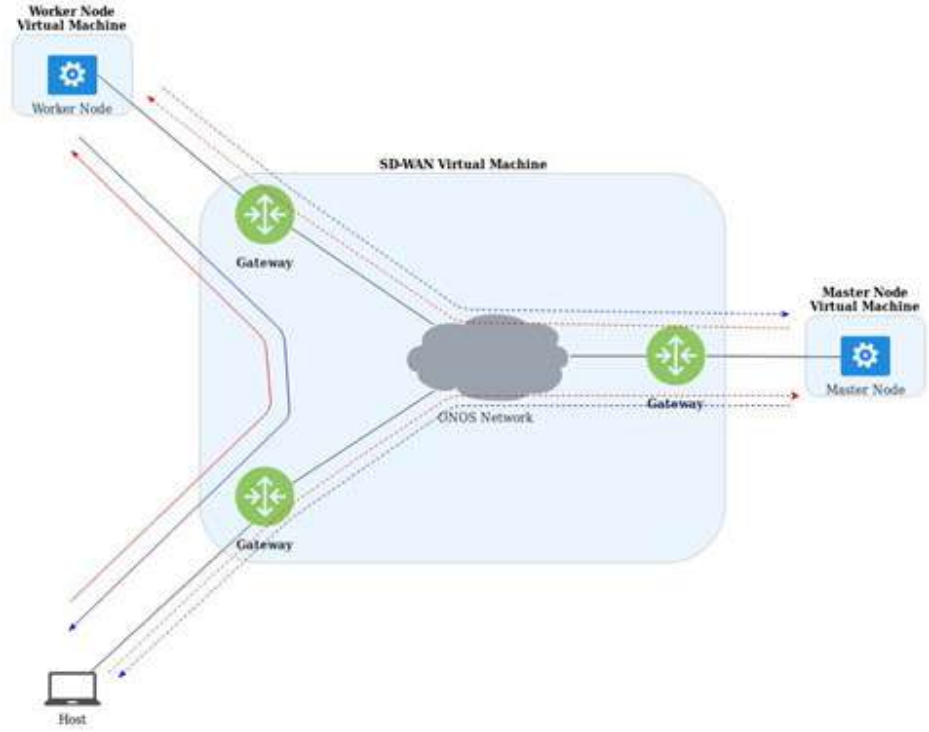


Figure 5. Requests sent by a host.

3.2. Reverse Proxy Service

Traditionally, when putting an application server on a network, attackers may exploit the underlying vulnerabilities of the available services. Although this is not the case when using containerized services, security is still something we all must be concerned about. In production environments a security measure is to deny internet access inside a corporate branch and instead use a proxy server. A proxy service is the one attending requests from a web browser and it can be used to bypass security restrictions, on the other hand, a reverse proxy service is used by a web server and has the advantage of enabling load-balancing. Containerized Nginx is the open source solution web server used in this work due to its user-friendly configuration and the ability of handling a great number of connections with a significantly less overhead than its counterparts. The idea behind this implementation is reducing to the minimum the amount of requirements needed for running the worker nodes, installing Nginx on them would have for sure undermined this principle as every worker joining the cluster would need to have Nginx installed before being able to serve its purpose.

On the other hand, a normal Kubernetes Nginx service running in the cluster would have been limited to internal requests due to the lack of an “external-ip” not being granted to bare metal Kubernetes load-balancers, and which only work with Kubernetes implementations running on

IaaS such as GCP, AWS, or Azure. MetalLB [8] is the load balancer-implementation selected for supporting the reverse proxy service, and enables a layer 2 load-balancing through the creation of a controller and speaker deployments on every node it is running. Nginx entities are deployed one per worker node on top of MetalLB, receiving the worker's node IP address as their external-ip, enabling a reverse proxy behavior for requests coming from outside hosts towards port 80 and creating a corresponding Nginx pod. The need for the NodePort on the end user's side has been avoided. Instead of this, the "location" command in Nginx is being used to redirect users to the right HTTP service based on service's name. As an example, let us consider the Nginx configuration file for a worker node called worker1 that is running a service called "hello-world" and a worker node called worker2 running a service called "my-app".

From the point of view of worker1, a host close to worker1 will use the entry <vtt.kubernetes.services> for accessing services located in worker1, and an entry in the form <worker2.kubernetes.services> for all the other remote nodes, in this case a node called worker2.

For avoiding the usage of NodePort corresponding to "hello-world" service, this Nginx configuration file will enable the adding of "/hello-world/" to the requested URL for accessing this service, via the location command. For a host whose closest node is worker1, the request's URL is now in the form "vtt.kubernetes.services/hello-world/" when accessing this service located in worker1, for accessing the service "my-app" in worker2, the request's URL would be "worker2.kubernetes.services/my-app/". Figure 6 shows the example Nginx configuration file for worker1.

```
server {
   listen 80;
   location /help/ {
      index help.html;
      alias /etc/nginx/conf.d/;
   }
   location /hello-world/ {
      if ( $host ~ ".kubernetes.services" ) {
         proxy_pass http://192.168.200.2:34567;
      }
   }
}
```

Figure 6. Nginx configuration file for worker1.

By adding a comparison including the URL of the request to contain the string ".kubernetes.services" the access from remote hosts to the service is guaranteed. Hosts might not know what services are available or the names of the remote worker nodes, therefore, a request heading towards "vtt.kubernetes.services/help/" will deploy a html list of available services in the closest node as well as in the remote nodes and their corresponding URI. As it has been mentioned before, pods and services are not static, they are prone to being deleted or changed. Because of this, the Nginx configuration files located in every worker node must be updated dynamically as services are being added or deleted, and the Nginx service in its corresponding pod must be reloaded when these changes occur in its worker node.

3.3. Master Node Service Discovery

As explained in the previous sections, the zone files used in the external DNS service as well as the Nginx configuration files cannot be static. A master node service discovery is therefore necessary for the continuous update of all zone files in the gateways running the external DNS service, as well as for the service location updates in the Nginx pod running in every worker node. The service discovery works based on the principle that deployment and services' containers are not created at the master node, but at worker nodes. Kubernetes does not provide a default way of associating a certain service with the scheduled worker node, therefore, knowing the pods running on a determined worker node alongside the list of all available services in the cluster provides a way to start a service-node matching. Before performing the matching, the pods output must be filtered in order to avoid cluster management related pods to be counted as services, pods such as calico, Nginx or the MetalLB's controller and speaker must not be included. The discovery starts when all the available worker nodes and their corresponding IP addresses are obtained as an array using the Kubernetes API. The node array structure corresponds to a node's name followed by its IP address, therefore, worker's node names will always be located in an even index within the array, with their respective IP addresses located at the subsequent, odd position. Next, for every node in existence, we obtain the running pods and all the available services in the whole cluster.

During the first iteration and for every single node, the current amount of running pods is saved within an associative array, the next step is to create the zones files, creating and copying the Nginx configuration to the corresponding pod as well as reloading the Nginx service and sending the zones file to the respective routers. For copying files into the Nginx pods, kubectl tool is used, thus avoiding the creation of extra communication channels between the master and the worker nodes. The service discovery supports dynamically adding new worker nodes to the cluster, those new members will be automatically detected and after deploying a new MetalLB controller and speaker entity in the node alongside the Nginx service, the worker node will be ready for being scheduled pods.

During the subsequent iterations, the number of the obtained pods per worker node is compared against the values previously saved in the associative array, if there is a change in one of the values, then the discovery service is able to identify if a service might have been added, moved or deleted. After this, it deletes the current worker node's zones file and Nginx configuration in order to create new files with updated information. The Nginx service corresponding to the worker node where a change occurred is reloaded and the zone files are sent to the respective routers, these actions only occur in the nodes where a service was added or deleted leaving the unchanged nodes working continuously without any disruption. The service discovery was conceived in a way that no extra efforts such as copying master's certificates or installing extra software is necessary for a given worker node when joining the cluster, only the compulsory kubeadm, kubectl, kubelet and Docker are required. Being written in Bash script language, portability is assured as no modifications are required for running it in any Unix-like operating system. It is worth noting that due to actions being taken only in the worker nodes where a change has occurred, sending the DNS zones files will happen only once per change, a detail that helps in reducing the bandwidth use due to the lack of continuous advertisement. Another reason behind this behavior is the fact that the content of a zone file are mere urls and their corresponding IP addresses, which are not prone to change, and if they do, this does not happen quite often. In Figure 15, a high level version of the discovery algorithm used for the master service discovery is shown.

```
procedure Service Discovery
begin

A ← Associative array containing nodes information
N ← Array of available nodes at the cluster

for each item i in N do
  if i%2 == 0 then
    P ← List of available pods for Nᵢ
    S ← List of available services at the cluster
    if length of A < ( length of N )/2 then
      A[ Nᵢ ] ← Length of P
      Zones ← DNS records for hosts close to Nᵢ
      SVC ← Proxy configuration for Nᵢ
      p ← Nginx pod for Nᵢ
      send Zones to corresponding routers
      copy SVC to corresponding p
      reload nginx service in p
    end if
  end if

    if length of A ≥ ( length of N )/2 then
      if A[ Nᵢ ] != length of P then
        remove Zones
        remove SVC
        A[ Nᵢ ] ← Length of P
        Zones ← DNS records for hosts close to Nᵢ
        SVC ← Proxy configuration for Nᵢ
        p ← Nginx pod for Nᵢ
        send Zones to corresponding routers
        copy SVC to corresponding p
        reload nginx service in p
      end if
    end if
end for
end procedure Service Discovery
```

Figure 7. Service discovery algorithm.

3.4. Service Update System

The updated zones file generated at the master node must be sent to the gateways that are running the external DNS service. For this purpose, a Mosquitto [9] broker working in bridge mode was set up on the master node listening on port 1883. Mosquitto was selected due to it being a lightweight publish/subscribe transport protocol, its capability of coping with unreliable networks, and most important, its reduced bandwidth consumption. A MQTT publisher was implemented using the paho-mqtt python library, and set up on the CO. This publisher reads the whole zones file, transforms it into an array of bytes and publishes it under a determined topic. On the other hand, the border gateways running the external DNS service have a MQTT subscriber running, they subscribe to the determined topic and save the received array of bytes as an .txt file. After the file is saved, the subscriber will reload the DNS service running in the worker node. By default, MQTT does not provide encryption, however, security can be enforced

by using an username/password scheme or certificate authentication using the TLS protocol, with the latter being the most practical and secure option. The usage of the TLS protocol in MQTT requires the creation of the respective key pairs and certificates for both the broker and the clients.

4. TESTING AND RESULTS

The proof-of-concept and testing topology can be found in Figure 8, with all the developed services running in their corresponding locations. The Kubernetes master and worker nodes attached to their respective gateways running all the needed pods for proper functioning, such as coreDNS and kube-proxy, among others. The gateways run their custom DNS servers that are bound to their specific interface, the worker nodes run the Nginx service and the master node is running the service discovery alongside its MQTT publisher and Mosquitto broker. As it was aforementioned, no Kubernetes-related configuration work is performed on the worker nodes as the master node service discovery is going to perform all the required tasks without needing any action by the workers.

Under the precedent testing considerations, it must be taken into account that Mininet's virtualization is done only at a network level, and each host process sees the same set of processes and directories. Thus hindering the functions of the DNS service and the MQTT-based update system. The issue arises due to the lack of directory isolation. The update system will send the corresponding zone files to the gateways, and they will vary according to the gateway's location. This means that gateway 1 shall receive a different zones file than gateway 2 due to it being located closer to a worker node. However, this does not happen in Mininet, where the files received would be overwritten causing the DNS service to upload the wrong zones. In the same way, the resolv.conf file that contains the DNS server's addresses must be unique per host, otherwise, all of them will be pointing at the same DNS server causing the network to be flooded with wrong requests.

A similar situation occurs with the custom DNS server. It has to be bound to the gateway's interface that is going towards the host network, therefore, a different custom DNS service file is needed per gateway. These issues were overcome by creating the needed files in the directory /etc/netns/<host-name> containing the resolv.conf and the custom DNS files. The principle behind this is that ip-netns creates the namespaces as a logical copy of the network stack, but it inherits the whole network namespace from its parent. In the case of network namespace aware applications, a global network configuration is first looked for in the above mentioned directory and after this in /etc/, so by creating the files in /etc/netns/<host-name> we are loading them as global network configuration. Taking into account that this work is based on the dynamic discovery of updated, newly created and deleted services, the measurements carried out will be the time required for creating the zones files and the Nginx configuration files, as well as the time until the changes have been applied to both, the DNS server and the Nginx service. The first measurement in Table 1 and Table 2 will be carried out with only one worker node while another separate measurement in Table 3 and Table 4 will be performed for two worker nodes. This in order to find out whether the number of nodes has an effect on the system's performance, and in a more realistic scenario this number could scale up until having tenths of worker nodes.

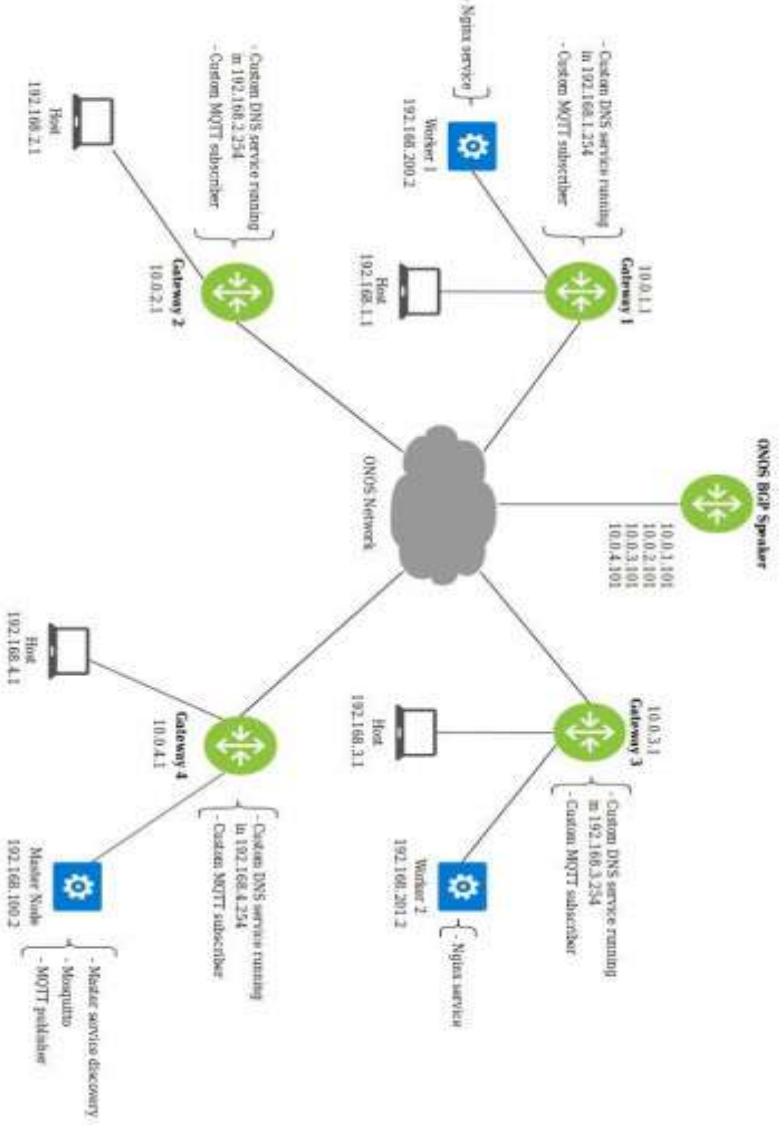


Figure 8. Testing network topology and the services running.

Table 1. Time required for the orchestrator to perform the necessary tasks in order to fully discover a newly created service when only one worker node is available.

One worker node – creating service	
Time to create zones files and nginx configuration files after a change in the worker node.	2 seconds
Time for changes being available in nginx after a change in the worker node.	3 seconds
Time for the zones being loaded in the DNS server after a change in the worker node.	3 seconds

Table 2. Time required for the orchestrator to perform the necessary tasks in order to fully eliminate a recently deleted service when only one worker node is available.

One worker node – deleting service	
Time to create zones files and nginx configuration files after a change in the worker node.	12 seconds
Time for changes being available in nginx after a change in the worker node.	3 seconds
Time for the zones being loaded in the DNS server after a change in the worker node.	3 seconds

When measuring the availability of the services, it must be taken into account that the reload functions in the orchestrator are carried out almost simultaneously. Thus, the time for a service to be available to the end user, in Table 2 for example, is the time required to create the file + the time required to reload the Nginx and DNS, in this case ~5 seconds. From Figure 9, it can be inferred that at the moment of creating a service, the number of worker nodes available does not influence the overall time. One reason for this might be the fact that Docker containers backing those services are created only in the scheduled worker nodes, therefore eliminating any possible queuing time. On the other hand we have Figure 10, a slight difference in the files creation function when two worker nodes are present can be found. The reason behind this behavior might be the fact that Kubernetes master node also has to delete the corresponding API object for every deleted service.

Table 3. Time required for the orchestrator to perform the necessary tasks in order to fully discover a newly created service when two worker nodes are available.

Two worker nodes – creating service	
Time to create zones files and nginx configuration files after a change in the worker node.	2 seconds
Time for changes being available in nginx after a change in the worker node.	3 seconds
Time for the zones being loaded in the DNS server after a change in the worker node.	3 seconds

Table 4. Time required for the orchestrator to perform the necessary tasks in order to fully eliminate a recently deleted service when two worker nodes are available.

Two worker nodes – deleting service	
Time to create zones files and nginx configuration files after a change in the worker node.	15 seconds
Time for changes being available in nginx after a change in the worker node.	3 seconds
Time for the zones being loaded in the DNS server after a change in the worker node.	3 seconds

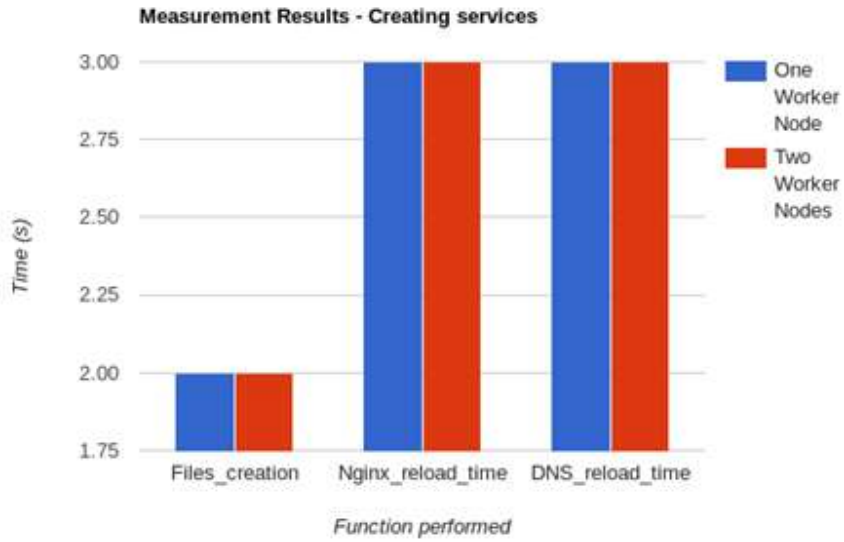


Figure 9. Time required for the orchestrator to perform the necessary tasks in order to fully discover a newly created service.

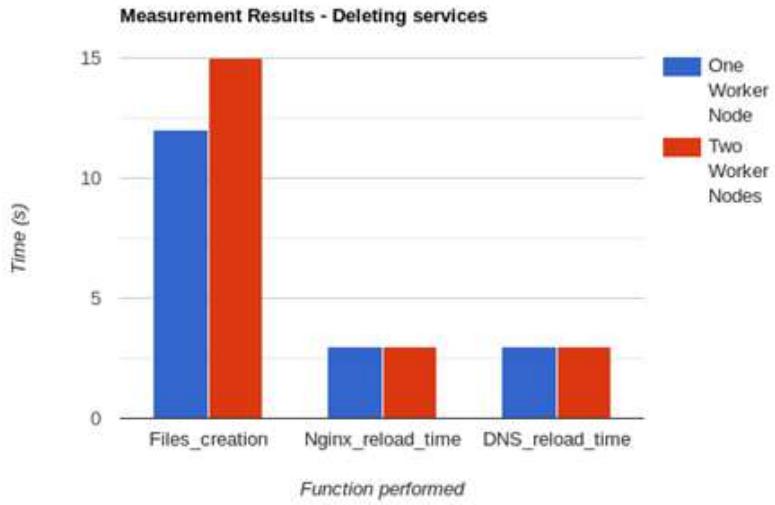


Figure 10. Time required for the orchestrator to perform the necessary tasks in order to eliminate a recently deleted service.

4.1. DISCUSSION

Taking into account the nature of this work, and the fact that no commercial solutions are available for a comparison, the times presented in the measurements are good. With such times, the creation and update of services will be almost invisible from the host's point of view. Delays can appear at various stages in the system. One of the first delays encountered is the time it takes to make a request using kubectl in the master node. The first request usually takes around 2 or 3 seconds to complete, with the subsequent requests being much faster, almost immediate. The same happens when performing a request with a JSON output, the first request will always induce a certain amount of delay. In the same way, when creating a deployment and exposing it as a service, it takes time for Kubernetes to create the new pod. This time varies depending on the available bandwidth, whether the required image has already been downloaded on the host machine or not, as well as its size, and the time it takes to the pod for being scheduled.

It takes a slightly longer time to update the files during the delete of a service and their corresponding back-end pods. This occurs because pods are granted a grace time in order to not only delete the process but also the API object. Time required for deleting a back-end pod will always be higher than the required time for creating it, even if the process running inside the pod is lightweight. One solution to this is to use the flag --wait=false when deleting the pod, though it is highly recommended to grant this grace time in order to ensure a proper deletion. When a service is deleted and its back-end pods stay in the terminating phase for a determined period of time, no concern exists as the service will not be available anymore, and even if the Nginx service has not been updated yet, requests being forwarded towards the deleted service will not be successful.

The convergence times can also be modified by altering certain values in the elements such as the master service discovery, the MQTT subscriber running in the gateways and the MQTT publisher running in the master node. As an example, a delay can be added or reduced before restarting the Nginx service in the master service discovery script, although taking into account that the restart

will occur only after performing a request for obtaining the corresponding pod's name, deleting the previous Nginx configuration file from that pod, copying the newly created configuration file and finally, restarting the service. Similarly, some delays can be added before publishing the created files in the MQTT publisher code or before saving the received files in the subscriber code. One possibility for dropping the times associated with the restart of the services, at least for Nginx, is to use the daemon-based Nginx installation in Linux, instead of the Docker-based version. This would reduce the amount of time spent to obtain the name of the Nginx pod, copying the files and restarting the service to only restarting the daemon.

5. CONCLUSION

We have presented a solution for the easy access and discovery of corporate services and applications. Knowing that containerized applications are prone to suffer modifications, the current work aims to provide a method that can be used for easily discover and access containerized services deployed in a Kubernetes environment while also helping with traffic steering. However, the proof-of-concept cannot yet be efficiently implemented in a real life scenario as an increased degree of automation as well as some performance improvements must be carried out.

5.1. Future work

Further work will focus on effectively measuring the geographical distance between worker nodes and gateways for improving the update system as well as implementing a telemetry framework for real time measurement applying dataplane programmability.

5.1.1. Node distance computing function

A way to dynamically obtain and update the distance between the gateway and the available worker nodes is a quite important feature that would allow the MQTT subscribers located in the gateways to select the closest node available so they can receive updates regarding this specific worker node as the local node. A common misconception lies in the belief that using ping is an acceptably accurate tool for this purpose. IP addresses can not be characterized by geographical reasons as a determined region might or might not be assigned a certain IP addresses block to it. With this in mind, an IP address assigned to Finland may easily be announced by a device at any other country, thus not guaranteeing that an entire network has been assigned to a single geographical location.

Similarly, there are many limitations considering the use of ping times. A ping time is determined by a great number of factors, which include: the number of routers, or hops, between the host and the target machine, the "quality" of the routing performed between these two points, any networking issue located between the source of the request and the target, excessive traffic or congestion happening between the target and the source, different transmission mediums along the route, with copper having a different propagation time than, for example fiber or a satellite link, among other factors.

Results from [13] can be used for the implementation of this feature, where some coordinates-based approaches for network distance estimation are discussed. The idea behind the coordinates-based distance measurement is that hosts maintain a determined set of numbers, also known as coordinates, that are used for characterizing their locations in the network and allowing a distance prediction based on the result of a distance function run over the host's coordinates. This approach works particularly well on peer-to-peer architecture, when a host discovers another host's identity, their coordinates would be exchanged and then the distance will be computed instantly. The mentioned work points out that coordinates have proven to be quite efficient at summarizing large amounts of distance information. A concern regarding the proposed approach is related to the assumption of stability in the network, such as consistent propagation delays, if this does not hold true due to the constant changes in network topology, distance estimations will be affected.

5.1.2. Telemetry function

Data plane programmability can be considered as the natural evolution of SDN, as it enables a much more flexible networking when being contrasted with a normal control plane based programmable network. Programming Protocol-independent Packet Processors, also known as P4, is the de-facto language for dataplane programmability, it allows several features extension of SDN networks as well as a dynamic configuration of actions that goes far beyond those allowed by the OpenFlow specifications. However, data plane programmability is not a silver bullet and although it allows to easily add new protocols, or remove unused protocols in a network chip, its effectiveness can only be appreciated at networks carrying huge amounts of traffic, therefore, some companies would not really require to implement it. The proof-of-concept system can take advantage of the support of P4 by ONOS, by implementing some novel features that will improve the experience and manageability of the system by creating a custom P4-based Load balancer and Telemetry system. By diving into these topics, it is assumed that a real-life implementation of the proof-of-concept is meant to possess a high traffic rate.

Normally, load balancers used in the cloud data centers as well as the load balancer used for this work are software based. Software based load balancers work by mapping a virtual IP address to a direct IP address that corresponds to a server or group of servers offering the required service. The usage of software based load balancers has some drawbacks such as: high use of server resources, high delay and weak performance isolation. In [14], Miao Rui et al, demonstrate that it is possible to implement a fully functional 400 lines P4-based load balancer that can support millions of simultaneous connections while providing per-connection consistency. The same principle can be applied for developing an in-house layer 4 load balancer instead of the currently used MetalLB, bringing a higher performance, lower delay and the relief of the MetalLB related pods in all the running worker nodes, while decreasing the changes of user experience degradation based on broken connections.

An in-house in-band network telemetry system is also possible to implement by using P4 as it has been demonstrated in [15] by Changhoon et al. In-band network telemetry allows data packets to query for switch internal state statistics such as link utilization and queue size. Thanks to each P4 switch having a control channel that allows the insertion, deletion and modification of matching tables, it is possible to send probe packets periodically that contain the switch ID and the specific time spent in determined switch. Once the packet arrives to the end user, an almost real-time measurement of this will be processed, allowing the detection of switches having large queues.

The resulting telemetry system can be used for easing the debug and diagnostics of network issues in a fast and intuitive manner.

REFERENCES

[1] Padhy, R., Patra, M., Satapathy, S. Virtualization Techniques & Technologies: State-of-The-Art. Journal of Global Research in Computer Science, 2018, vol. 2, nro.12. ISSN: 2229-371X. Available at: https://www.researchgate.net/publication/264884756_VIRTUALIZATION_TECHNIQUES_TECHNOLOGIES_STATE-OF-THE-ART.

[2] Horrel, J., Karimullah, A. SD-WAN Set to Transform WAN in Australia. IDC Custom Solutions, Framingham, 2017.

[3] Jakma, P. Quagga Routing Software Suite. Quagga Routing Suite. Visited: 15.02.2019. Available at: https://www.quagga.net/

[4] Open Network Operating System (ONOS). ONOS features. Open Networking Foundation & The Linux Foundation, San Francisco, 2019. Visited 15.02.2019. Available at: https://onosproject.org/features/

[5] Open Networking Foundation. Atomix. Open Networking Foundation. Visited 15.02.2019. Available at: https://atomix.io/docs/latest/user-manual/introduction/what-is-atomix/

[6] Kubernetes. DNS for services and pods. The Linux Foundation, San Francisco, 2019. Visited 15.02.2019. Available at: https://kubernetes.io/docs/concepts/services-networking/dns-pod-service/

[7] Kubernetes. Access services running on clusters. The Linux Foundation, San Francisco, 2019. Visited 15.02.2019. Available at: https://kubernetes.io/docs/tasks/administer-cluster/access-cluster-services/

[8] MetalLB Metal Load-Balancer (MetalLB). Google. Visited 15.02.2019. Available at: https://metallb.universe.tf/

[9] Stanford-Clark, A., Nipper, A. Message Queuing Telemetry Transport (MQTT). Organization for the Advancement of Structured Information Standards (OASIS). Visited 15.02.2019. Available at: http://mqtt.org

[10] Jarraya, Y., Madi, T., Debbabi, M., 2014. A Survey and a Layered Taxonomy of Software Defined Networking. IEEE Communications Surveys & Tutorials 16,1955–1980. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6805151, doi: 10.1109/COMST.2014.2320094.

[11] Kreutz, D., Ramos, F.M.V. , Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., Uhlig, S., 2015. Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE 103,14–76. URL: http://ieeexplore.ieee.org/document/6994333/, doi:10.1109/JPROC.2014.2371999.

[12] Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., & Sabella, D. (2017). On Multi-Access Edge Computing:A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration. IEEE Communications Surveys and Tutorials, 19(3), 1657-1681. [7931566]. https://doi.org/10.1109/COMST.2017.2705720

[13] Eugene, TS., Zhang, Hui. Predicting Internet Network Distance with Coordinates-Based Approaches. Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, 2002, DOI: 10.1109/INFCOM.2002.1019258, ISSN: 0743-166X. Available at: https://www.cs.rice.edu/~eugeneng/papers/INFOCOM02.pdf

[14] Miao, Rui., Hongyi, Zeng., Changhoon, Kim., Jeongkeun, Lee., Minlan, Yu. SilkRoad: Making Stateful Layer-4 Load Balancing Fast andCheap Using Switching ASICs. Association for Computing Machinery's Special Interest Group on Data Communications (SIGCOMM), 2017, DOI: 10.1145/3098822.3098824, ISBN: 78-1-4503-4653-5/17/08. Available at: https://eastzone.bitbucket.io/paper/sigcomm17-silkroad.pdf

[15] Changhoon, Kim., Sivaraman, Anirudh., Katta, Naga., Bas, Antonin., Wobker, Lawrence J. In-band Network Telemetry via Programmable Dataplanes. 2015, Visited 12.05.2019. Available at: https://pdfs.semanticscholar.org/a3f1/9dc8520e2f42673be7cbd8d80cd96e3ec0c1.pdf?_ga=2.76525468.802012735.1559031914-713298922.1559031914

AUTHORS

Felipe Andres Rodriguez Yaguache is currently finishing his master studies in Communication Engineering at Aalto University (Finland), and is working at the Technical Research Centre of Finland (VTT) as a Master Thesis Worker. His interests include edge computing, SDN, networking and data plane programmability.

Kimmo Ahola currently works as a Senior Scientist at VTT Technical Research Centre of Finland. His research interests include Computer Communications (Networks), Software Defined Networking, Edge Computing, Network Functions Virtualisati on, Computer Security and Reliability and Operating Systems.

Ensemble learning using frequent itemset mining for anomaly detection

Saeid Soheily-Khah and Yiming Wu

SKYLADS Research Team, Paris, France
{saeid,yiming}@skylads.com

Abstract

Anomaly detection is vital for automated data analysis, with specific applications spanning almost every domain. In this paper, we propose a hybrid supervised learning of anomaly detection using frequent itemset mining and random forest with an ensemble probabilistic voting method, which outperforms the alternative supervised learning methods through the commonly used measures for anomaly detection: accuracy, true positive rate (i.e. recall) and false positive rate. To justify our claim, a benchmark dataset is used to evaluate the efficiency of the proposed approach, where the results illustrate its benefits.

Keywords

Ensemble learning, anomaly detection, frequent (closed / maximal) itemset mining, random forest, classification

1. Introduction

Anomaly detection, also known as 'outlier' detection [1], is a technique used to identify unusual or abnormal patterns that do not conform to the expected behaviors [2]. It has a wide variety of applications in business, from security intrusion detection to system health monitoring, and from fraud detection in credit card transactions or (online) ads clicks to fault detection in operating environments, military surveillance and etc [3, 4, 5, 6, 7]

Detecting anomalies (or outliers) has been studied in statistics community as early as in the 19th century [8], and it was proposed for Intrusion Detection Systems (IDS) in 1980s [9]. Over time, in the recent years, anomaly detection has attracted great attention in the machine learning and data mining community [10, 11, 12]. Anomaly detection works by taking the baseline of normal traffic and activities, from which a model of normal behaviors is built. It detects known and previously unknown attacks. However, in many cases, it may fail to detect malicious behaviours or even raise alarms for normal data assuming erroneously that it is an attack. Thus, applying data mining techniques on network traffic data is a promising solution which helps to develop better anomaly detection systems. Several anomaly detection techniques have been proposed in the literature, such as density-based techniques (k-nearest neighbor [13] or local outlier factor[14]), correlation-based outlier detection [15], one-class support vector machines [16], neural networks, bayesian networks, hidden markov models [17], fuzzy logic-based outlier detection and etc. In this paper, we discuss the wel-known machine learning methods for network anomaly detection and propose a hybrid supervised learning approach to detect anomalies in networks more effectively. The main contribution of this work is actually to boost base (weak) learners to strong learners by ensemble learning, which can make very accurate classifiers.

The remainder of the paper is organized as follows: Section 2 provides the state-of-the-art of the work. Next, in Section 3, we characterize the proposed ensemble learning approach

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 373-389, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90931

for anomaly detection in detail. Section 4 presents the experimental results, and lastly Section 5 concludes the paper.

2. State-of-the-art

In this section we first present an overview of the learning approach used in this paper, i.e. the ensemble learning approach. Moreover, we describe the data mining, machine learning and pattern mining algorithms used in this research work such as Support Vector Machine (SVM), k-Nearest Neighbor (k-NN), Multi Layer Perceptron (MLP), and Random Forest (RF). In addition, we simply mention their computational complexities, advantages and disadvantages.

2.1. Ensemble Learning

Ensemble learning is a statistic and machine learning approach that uses multiple learning algorithms to solve a problem with better predictive performance. Unlike traditional machine learning approaches in which a single hypothesis is learned from training data, ensemble approaches attempt to build a set of hypotheses and combine them to build a new hypothesis [18].

Ensemble learning systems can be useful to deal with the big data. When the size of training data is too large to make a single classifier, the data can be partitioned into smaller subsets by different strategies, and each subset can be used to train a separate classifier. Then the different classifiers can be combined using an appropriate combination rule. On the other hand, while the data is not that big, several base learners are built on the whole data, and then these learners are combined through several combination techniques such as majority voting [19].

In a simple way, the main objective of an ensemble learning is to improve the performance of a predictive model by combining multiple learners. Previous researches and studies show that generally an ensemble learning performs better than the individual (base) learners [20]. In the following, we describe the state-of-the-art of the well-known individual (base) learning methods.

2.2. Individual (base) learning

2.2.1. Machine learning-based approaches

A common data mining task, with the foundations of machine learning is classification. Classification-based anomaly detection techniques analyze, evaluate and classify the data in two classes (i.e. normal or abnormal). They are used when the available training data are labeled. In the following, we present the most common classification techniques for anomaly detection applications.

Support Vector Machine-based anomaly detection Support Vector Machine (SVM) is an effective technique for detecting anomalies (or outliers). Typically, SVM is associated with supervised learning, but its extensions (e.g. OneClass-SVM) can be used to identify anomalies as an unsupervised problems, where the training data is not labeled. However, the SVM is one of the most successful classification algorithms, but it is a time-consuming task in the training step, which limits its use. In addition, generally the SVM considers the features of data equally, while in real datasets, many features are unneeded, redundant or less important. Due to the shortcomings of the standard SVM for detecting anomalies, in the recent years, variant of SVM are suggested [21, 22].

Density-based anomaly detection Density-based anomaly detection is based on the k-Nearest Neighbors (k-NN) classification algorithm. The nearest set of k data points are evaluated using a metric such as Eucledian and Hamming distance. The k-NN is a simple and non-parametric lazy learning technique and it is one of the oldest methods of classification. While k-NN classifier usually works well in the terms of accuracy, it is slow in the recognition step, because the distances between the new data point and all the training data need to be computed. So, in the literature, there have been attempts to make it faster [23, 24], and research works are in progress to investigate its reliability and scaling properties [25, 26].

Naive Bayesian-based anomaly detection Bayesian networks have been used for anomaly detection in the multi-class setting by predicting the class membership probabilities. They work based on the Bayes' theorem, with strong independence assumptions between the features to simplify the task. The Bayes' rule allows unknown probabilities to be computed from known conditional probabilities, usually in the causal direction. Naive Bayesian networks are fast to train and classify, space efficient, not sensitive to irrelevant features and easy to implement. But their main disadvantage is that the Naive Bayes classifiers make a very strong assumption on the shape of data distribution (i.e. independence of features). However, in practice, they can work surprisingly well and comparable in performance with other classification algorithms, even when the conditional independence assumption is not true [27, 28, 29]. Over the last decade, several variants of the basic Naive Bayes technique have been proposed for anomaly detection [30, 31].

Neural network-based anomaly detection Neural Networks have been applied to anomaly detection in multi-class as well as one-class setting. They consist of a connected set of processing units distributed several layers, namely input, hidden and output layers, where each connection is characterized by a 'synaptic' weight that determines how the signal will propagate from one unit to another one. By adjusting these weights, the neural networks benefit from their learning algorithms to learn the relationship between inputs and outputs and to predict the correct class label of the input data. The neural networks are a simple manner to signify nonlinear relationships between features. However, they are computationally expensive to train and generally, require a large set of training data. A basic neural networks-based anomaly detection technique works in two steps. Firstly, a neural network is trained on the normal training data to learn the different normal classes, and then, each test data is provided as an input to the neural network. If the network accepts the test input, it is normal and otherwise, it is an anomaly [32]. In the literature, several variants of the basic neural network technique have been proposed for anomaly detection [33, 34].

Rule-based anomaly detection Rule-based anomaly detection methods learn rules that capture the normal behavior. While a test instance is not covered by any such learned rule, it is considered as an anomaly. These techniques have been applied in one-class and multi-class setting. One of the most common rule-based techniques used in anomaly detection is associated with decision trees, where they can be used to detect anomalies in large datasets. A decision tree algorithm generates a tree structure where each internal node stands for a decision on a feature and each leaf node take a class label. So, there is a path from the root node to the labeled leaf node, considered as a set of rules, which makes it easy to classify new unlabeled data. Decision trees have several advantages compared to the other machine learning based classification approaches, which make them more suitable for anomaly detection. In particular, they have a simply explainable framework and they are less sensitive to problem of the curse of dimension [1].

Random Forests (RF) [35] is a widely used ensemble learning method for classification and regression and operates by constructing a plenty of decision trees during train and test procedure. The term came from random decision forests that was first proposed in 1995 [36]. While in the standard decision tree, each node is bisect using the best split among all the features, in a random forest algorithm, each node is bisect among a small subset of randomly selected input features. In general, the more trees in the forest the more robust the forest looks like, and the higher the number of trees in the forest gives the more accurate results. The main advantages of the random forest algorithm are:

- It has ability to handle unbalanced datasets
- It is robust against over training and over-fitting
- It runs efficiently on very large datasets with many features
- It can handle thousands of input features without feature deletion
- It gives estimates of which features are important in the classification

and lastly, it is unexcelled in accuracy among many current anomaly detection algorithms [37, 38, 39].

In summary, random forest is a way of averaging multiple deep decision trees, trained on different parts of the same training set, with the aim of reducing the variance, where it is becoming a popular algorithm for both classification and regression, because it does not have many tuning parameters, is a highly flexible classifier and often works quite well. However, random forest has been observed to over-fit in classification for some noisy datasets. In addition, for data including categorical features with different number of levels, it is biased in favor of those features with more levels [40, 41]. Since, random forest has been regarded as one of the most efficient approaches in classification (and anomaly detection) [42], in this work, we try to deploy the random forest into an ensemble learning algorithm using a pattern mining-based method to acquire even higher performance.

2.2.2. Pattern mining-based approaches

The problem of pattern mining has been widely studied in the literature because of its numerous applications to a variety of data mining and machine learning problems such as clustering and classification. It consists of developing (or using) data mining algorithms to discover interesting, useful or unexpected patterns in the data. Pattern mining can be applied to various types of data such as strings, transaction, sequence (time series), spatial data, and graphs. Typically, an interesting pattern is a pattern that appears frequently in the data. Therefore, in simple words, pattern mining is a way to find all of frequent patterns whose occurrence frequency in the data is 'no less' than the pre-defined threshold value. But there are many types of patterns such as sequential patterns, frequent itemsets, frequent subgraphs, frequent episodes, etc, and all of those types of patterns can be said to be frequent patterns. The most common one is the support-based framework, in which itemsets with frequency above a given threshold are found. In the following, we discuss more about the frequent itemset mining in detail.

Frequent itemset mining-based anomaly detection Frequent itemset plays an essential role in many mining tasks which trys to find interesting patterns from the datasets. The original motivation for searching the frequent itemsets came from the need to analyze the supermarket transaction data, that is, to examine customer behavior in terms of the purchased products [43], while the frequent itemsets of products describe how often items are purchased together. But what is an itemset and the frequent itemsets?

An Itemset (or element) is a non empty set of items $(x_1, x_2, ..., x_m)$, and a frequent itemset is an itemset whose support is greater than or equal to a minimum support threshold.

Here, the support (σ) is the frequency of occurrence of an itemset in a dataset. The task of discovering all frequent itemsets is quite challenging. The search space is exponential in the number of items occurring in the database. Furthermore, the major problem with the frequent itemset mining methods is the explosion of the number of the results, while it is difficult to find the most interesting frequent itemsets. Hence, we need to seek the most efficient techniques to solve this problem.

Frequent closed itemset mining is a task of discovering frequent itemsets whose support counts are different than those of their supersets. It means that an itemset is 'closed frequent' if none of its immediate supersets has the same support count as the itemset. Therefore, the size of frequent closed itemsets are much smaller than all the frequent itemsets, while we do not lose any information. In a nutshell, the frequent closed itemsets provide a compact yet lossless representation of the frequent itemsets.

Maximal frequent itemset is a frequent itemset for which none of its immediate supersets in the database is frequent. This representation is valuable because it provides the most compact representation of the frequent itemsets, and so when the search space is an issue or when we have a very large dataset, it is very helpful.

Let us make it more clear by one example. Consider 4 sequences as {a,b,c,d,e}, {a,b,d}, {b,e,a,c}, and {b,c,d,e}, where the minimum support (minsup) is equal to 2. {b,c} is a frequent itemset because it appears in two sequences (it has a support of 2). {b,c} is not a closed frequent itemset, because it is contained in a larger sequential pattern {b,c,d} having the same support. {b,c,d} has a support of 2. It is also not a closed frequent itemset, because it is contained in a larger sequential pattern {b,c,d,e} having the same support. {b,c,d,e} is a closed frequent itemset, because it is not included in any other sequential pattern having the same support. In this case, {b,c,d,e} is also a maximal frequent itemset, since none of its immediate supersets in the data is frequent.

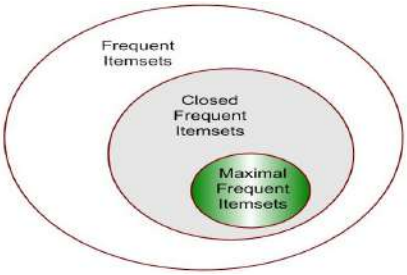


Figure 1: The relationship between frequent itemsets representations

Lastly, Figure 1 illustrates the relationship between frequent itemsets, closed frequent itemsets and maximal frequent itemsets representations. As we mentioned earlier closed and maximal frequent itemsets are subsets of frequent itemsets, but maximal frequent itemsets is a more compact representation, since it is a subset of the closed frequent itemsets. Notice that the closed frequent itemsets are more widely used than maximal frequent itemset [44]. So, the quesion now is how to get the frequent itemsets.

The most popular algorithm for itemset mining is without a doubt Apriori algorithm [45], which is designed more than 20 years ago, and is the basis of many efficient algorithms developed later. However, it is originally designed to be applied on a transaction data to discover patterns in transactions made by customers in stores, it can also be applied in several other applications. Apriori-based algorithms take as input a minimum support threshold and output all frequent itemsets, i.e. groups of items shared by no less than minimum support transactions in the input data. Algorithm 1 illustrates the apriori-all algorithm in a simple way.

Algorithm 1 Apriori(-All)

input: <**minsup**> minimum support threshold
output: frequent itemsets

do scan data once to get frequent 1-itemsets
repeat
    generate length-(k+1) candidate itemsets from length-k frequent itemsets
    test candidates againts DB to find frequent (k+1)-itemsets
    set k = k + 1
until no frequent or candidate set can be generated
return frequent itemsets

This can be done easily for a small data. If we have n items in the data, there will be 2^n possible itemsets. This is not a lot while the data size is small. But consider a large dataset having 1,000 items, the number of possible itemsets would be: $2^{1000} = 1.26e30$, which is huge, and practically not possible to use a apriori-based approach to find the frequent itemsets. In general, candidate counting , problem of I/O minimization, reducing the number of comparisons as well as handling large data are the most challengs in frequent itemset mining.

Later in [46], authors proposed a faster algorithm than Apriori-All, called GPS, which scales linearly with the number of data-sequences. The basic structure of the GSP for finding frequent itemsets is as follows: multiple-passing, candidate generation and testing (see Algo 2). Notice that in the loop cycle, one can generate length-(k+1) candidate sequences using the Apriori method. But still using the GPS algorithm, a huge set of candidates could be generated, we need to have multiple scans of data, as well as difficulties at mining long sequence patterns are exist.

Algorithm 2 GPS: Generalized Sequential Pattern

input: <**minsup**> minimum support threshold
output: frequent itemsets

repeat for each level (e.g. length-k)
    scan data to find length-k frequent sequence
    generate length-(k+1) candidate sequences from the length-k frequent sequences
    set k = k + 1
until no frequent or candidate set can be generated
return frequent itemsets

The above Apriori-based approaches are horizontal format-based and use the breadth-first search to mine with a hierarchical structure. Nearly two decades ago, the vertical format-based methods are proposed, where they tried to read the data, convert it to a vertical representation, and perform a depth-first search by joining items to each patter. The most well-known ones are SPADE (Sequential PAttern Discovery using Equivalence classes) [47], SPAM (Sequential PAttern Mining using a bitmap representation) [48] and LAPIN (LAst Position INduction) [49] and its improved version LAPIN-SPAM [50]. SPADE algorithm, which uses equivalence classes to discover the sequential patterns (itemsets), is an Apriori-based hybrid miner and can be either breadth-first or depth-first. It exploits sequential patterns by utilizing a vertical id-list database format and a vertical lattice structure. By using the SPADE algorithm a huge set of candidates could be generated, and also it waste

a lot of time on merging ID lists of the candidates, which prevent its usage. SPAM is similar to SPADE, but SPAM uses bitmap representation and bitwise operations rather than regular and temporal joins. First of all, SPAM consider all the sequences arranged in a sequence tree. Each sequence in the sequence tree can be considered as a sequence-extended sequence and an itemset-extended sequence. Then using prune candidate extension, it generates the frequent pattern (itemsets). Space utility in SPAM may not be good, and also it needs to load all data into memory, which will be inefficient (even impractical) for large data. The authors of LAPIN algorithm tried to reduce searching by scan only part of the search space. The key feature of LAPIN is that the last position of item s is the key to judge whether a k-length frequent sequence can grow to be frequent appending it with s or not. But still the support counting is time consumption.

Beside the above mentioned Apriori-based approaches, researchers proposed a variety of algorithms using pattern-growth techniques. In the early years of the 20th century, a pattern-projected sequential pattern mining algorithm named FreeSpan was introduced in [51], which obtains all frequent sequences (itemsets) based on so-called projected pattern growth. Note that a projected data is the set of suffixes w.r.t. a given prefix sequence. Later the most representative algorithm using the pattern-growth strategy, called PrefixSpan, was proposed in [52], which explores prefix-projection in sequential pattern mining. It tests only the prefix sub-sequences, and then projects their corresponding postfix subsequences into the projected sub-databases. By exploring only local frequent sequences (itemsets), sequential patterns can be recursively grown in each projected sub-database. PrefixSpan algorithm mines the complete set of patterns, but greatly reduces the efforts of candidate subsequence generation. Moreover, prefix-projection substantially reduces the size of projected data and leads to efficient processing. Although the projection-based approaches (i.e., FreeSpan, PrefixSpan) can achieve a significant improvement over Apriori-based approaches [53], the projection mechanism still suffers from some drawbacks, while the major cost is caused by constructing projected databases.

In the recent years, some other pattern-growth algorithms have been developed, such as FS-Miner [54], PLWAP [55], etc. Furthermore, the interesting idea of constraint-based techniques has been widely studied, including closed sequential patterns, maximal sequential pattern and top-k sequential patterns, etc. Up to now, some algorithms for mining closed and maximal sequential patterns have been proposed, such as CloSpan [56], ClaSP [57] and CloFAST [58], which try to prune the search space. However, the maximal representation may cause the information loss of support. In simple words, each method of pattern mining algorithms has advantages and disadvantages where the efficiency also could be related to the data type and size.

3. The proposed approach

In this section, we explain in detail the proposed ensemble learning anomaly detection, called fim-RF. Algorithm 3 presents in a very simple way the different steps of the proposed anomaly detection approach.

First of all, we do data pre-processing which involves cleaning the data and removing redundant and unnecessary entries. To do so, we use feature engineering based on a) feature selection, b) feature encoding, c) feature construction and d) feature normalization. The aim of feature selection is to come from many features to a few that are useful, since not all the features are created equally. Those features that are irrelevant to the problem need to be removed. Also, there are some features that will be more important than others to the model accuracy. Furthurmore, some features will be redundant in the context of other features. Feature selection addresses these problems by automatically selecting a

Algorithm 3 Function fim-RF($\mathbf{S}$, $\mathbf{S}_l$, $\mathbf{x}$)

input

$\mathbf{S}$: training data, $\mathbf{S}_l$: labels of data (0:normal, 1:abnormal), $\mathbf{x}$: a test instance

min_{sup}: minimum support threshold in frequent itemset mining

α, β: ensemble learning regularization parameters

τ: classification probability threshold

output

$\mathbf{x}_l$: label of the test instance

do pre-processing

feature selection

feature encoding

feature construction

feature normalization

$\mathbf{x}_{l_{rf}}$, $P_{rf}(\mathbf{x})$ = random_forest_classifier($\mathbf{S}$, $\mathbf{S}_l$, $\mathbf{x}$)

do frequent closed/maximal itemset mining

$P_{nf}(\mathbf{x})$ = probability of $\mathbf{x}$ to be a normal frequent closed/maximal itemset

$P_{af}(\mathbf{x})$ = probability of $\mathbf{x}$ to be a abnormal frequent closed/maximal itemset

$$P(\mathbf{x}) = \frac{\alpha.\Big(\frac{P_{nf}(\mathbf{x}) + (1 - P_{af}(\mathbf{x}))}{2}\Big) + \beta.P_{rf}(\mathbf{x})}{\alpha + \beta}$$

if $P(\mathbf{x}) < \tau$ **then**

$\mathbf{x}_l = 0$ (normal)

else

$\mathbf{x}_l = 1$ (abnormal)

return $\mathbf{x}_l$

subset that are most useful to the problem. Here, we rely on chi-square test, which is a statistical test of independence to determine the dependency of two features. We rank the features and then we choose the top-k features. Feature encoding involves converting the features of the data into numerical data and saving in a machine-readable format, which is essential for many data mining algorithms. Because they require data to consist of purely numerical features. Since packet data consists of both numerical and categorical features we adopt an effective method of converting categorical features into numerical ones. When the categorical feature takes its values in some finite set of categories, one typical conversion method is to adopt binary number representation where we use m binary numbers to represent a m-category feature (one-hot encoding). However, in case the number of categories for each categorical feature is very large the dimension of the input will be potentially intractable. To solve this problem, we use a histogram based encoding to model the distribution of values. First, we encode each categorical value into its integer representation, and then, we evaluate the frequency distribution histogram of numbers. To help detecting network, IP scans and distributed attacks, we create a new feature as the number of distinct IP-sources associated to the IP-destination. Lastly, feature normalization which plays a crucial role in the data pre-processing. Since, without normalization, features with significantly larger values dominate the features with smaller values, we normalize the data in the boundary of [0,1] by:

$$\hat{x}_i = \frac{x_i - \min(x)}{\max(x) - \min(x)} \tag{1}$$

After the pre-processing steps, we build our proposed ensemble classifier as follows: We

firstly partition the data according to their application types (such as HTTPWeb, SSH,...) due to the difference behaviour of data in different applications, prior to run the random forest classification algorithm to get the predicted label ($\mathbf{x}_{l_{rf}}$) and the probability $\mathrm{P}_{rf}(\mathbf{x})$ which is the proportion of votes of the trees in the forest for test instance $\mathbf{x}$. In the context of pattern mining, we rely on frequent itemset mining. To do so, we obtain the top-k frequent close (and maximal) itemsets for normal data as well as abnormal (i.e. attack) data using an improved ECLAT algorithm. ECLAT algorithm, originally proposed in [59], is based on the breadth-first search strategy, which adopts the technologies of vertical data format, lattice theory, equivalence classes, intersection and so on. The main strategy steps of ECLAT are as follows: Scan the data to get all frequent k-itemsets, generate candidate (k+1)-itemsets from frequent k-itemsets, then get all frequent (k+1)-itemsets by clipping non-frequent candidate itemsets, and repeat the above steps, until no candidate itemset can be generated. By partitioning list of the set of itemset, we reduce the search space as well as the time of generating candidate itemsets, and speed up the calculation of intersection.

Once, we obtain the frequent closed (and maximal) itemsets for normal and abnormal data, we need to calculate the probability of normal classes of test instance $\mathbf{x}$ as well as the abnormal one. The probability of $\mathbf{x}$ to be a normal frequent closed/maximal itemset, $P_{nf}(\mathbf{x})$, is defined by:

$$P_{nf}(\mathbf{x}) = \frac{S_{\mathbf{x}_{nf}}}{N} \tag{2}$$

where $S_{\mathbf{x}_{nf}}$ is the support number of $\mathbf{x}$ to be a normal frequent itemset, with respect to the minimum support threshold equal to the pre-defined given min_{sup} value, and N is the total number of data points. Similarly, the probability of $\mathbf{x}$ to be an abnormal frequent itemset, $P_{af}(\mathbf{x})$, is defined as:

$$P_{af}(\mathbf{x}) = \frac{S_{\mathbf{x}_{af}}}{N} \tag{3}$$

where, $S_{\mathbf{x}_{af}}$ the support number of $\mathbf{x}$ to be an abnormal frequent itemset.

For each test instance $\mathbf{x}$, different situations can happen, such as a) $\mathbf{x}$ be a normal frequent itemset and not to be an abnormal frequent itemset, b) $\mathbf{x}$ be an abnormal frequent itemset and not to be a normal frequent itemset, and c) $\mathbf{x}$ be a normal frequent itemset and also be an abnormal frequent itemset, The situation 'a' leads that the test instance $\mathbf{x}$ with high probability be normal, situation 'b' leads that the test instance $\mathbf{x}$ with high probability be abnormal (i.e. attack), where in the situation 'c', one need to have confidence in the probabilities $P_{nf}(\mathbf{x})$ and $P_{af}(\mathbf{x})$.

Finally, as we mentioned above in the algorithm 3, the classification probability of the proposed ensemble learning method is defined by:

$$P(\mathbf{x}) = \frac{\alpha.\Big(\frac{P_{nf}(\mathbf{x}) + (1 - P_{af}(\mathbf{x}))}{2}\Big) + \beta.P_{rf}(\mathbf{x})}{\alpha + \beta} \tag{4}$$

where α, β are the ensemble learning regularization parameters. Notice that, one can optimize the parameters using the cross-validation test. In the next section, to have a closer look at the ability of the proposed ensemble learning (fim-RF), we detailed extensive experiments.

4. Experimentation

Here we describe the dataset used to lead our experiments, prior to specify the validation process, and to present the obtained results.

4.1. The benchmark ISCX dataset

In this work, we used the public benchmark ISCX dataset [60], to perform experiments and evaluate the performance of our proposed ensemble learning approach. The dataset includes more than million of the traffic packets with twenty features, where it covers one week of network activities with normal and abnormal (i.e. attack) traffic data. Four primary kinds of network attack (i.e. Brute Force SSH, Infiltrating, HTTP DoS, and DDoS) are conducted with normal traffic. Table 1 describes the ISCX dataset considered in our experiments, with its characteristics: number of normal traffic data, number of attack data and number of features.

appName	# of Normals	# of Attacks	# of Features
HTTPWeb	681151	40351	20
SSH	2585	7305	20
ICMP	7919	295	20
FTP	13181	226	20
DNS	309286	73	20

Table 1: ISCX (flows): data description

As mentioned, as input to the proposed ensemble learning anomaly detection algorithm, we use of the pre-processed data. Since, the normal traffic patterns look very different depending on the application or service, data are classified according to their application layers such as HTTP Web, SSH, FTP, ICMP and so on, which makes it more efficient to build an anomaly detector for each of these application layers.

4.2. Validation process

Here we compare the proposed anomaly detection algorithm (fim-RF) with the state-of-the-art anomaly detection methods (i.e. SVM, 1-NN, NB, MLP, Decision Tree and RF). To evaluate each method, we rely on the commonly used measures for anomaly detection: ACCuracy (ACC), True Positive Rate (TPR) and False Positive Rate (FPR). The accuracy is the proportion of true results (both true positives and true negatives) among the total number of cases examined. True positive rate which is called 'recall', or 'sensitivity' in binary classification, measures the proportion of actual positives that are correctly identified. While recall can be viewed as the probability of detection, false positive rate is the probability of false alarms. The mentioned comparison measures are defined as:

$$\text{ACC} = \frac{TP + TN}{TP + FN + FP + TN}, \ \text{TPR} = \frac{TP}{TP + FN}, \ \text{FPR} = \frac{FP}{FP + TN}$$

The 'accuracy' and 'true positive rate' lies in [0, 100] in percentage. The higher index, the better the agreement is. In the other side, the lower 'false positive rate' illustrates the better result. Finally, Table 2 presents the classical confusion matrix, where N shows 'normal' data and P illustrates 'abnormal' (or 'attack').

		Predicted class	
		Positive class	Negative class
Actual	Positive class	TP (True Positive)	FN (False Negative)
	Negative class	FP (False Positive)	TN (True Negative)

Table 2: Confusion matrix

Training and testing sets are formed by k-fold cross validation in the ratio of 80% and 20% of the network traffic, respectively. For all the state-of-the-art methods, the parameters are estimated through a standard grid search process, and finally, the results reported hereinafter are averaged after 10 repetitions of the corresponding algorithm.

4.3. Experimental results

In the context of anomaly detection, the 'accuracy', the 'true positive rate' and the 'false positive rate' for each method, and for the various tested protocols, are reported in Tables 3, 4 and 5, respectively. Results in bold correspond to the best assessment values.

appName	SVM	1-NN	Naive Bayes	Decision Tree	Neural Network	RF	fim-RF
HTTPWeb	98.99	99.70	98.04	99.89	99.02	99.88	**99.93**
SSH	99.47	99.90	99.22	99.87	99.89	99.89	**99.98**
ICMP	99.83	99.95	99.90	99.99	99.93	99.99	**100.0**
FTP	99.62	99.95	99.54	99.97	99.94	99.97	**99.98**
DNS	99.98	**99.99**	96.18	99.98	99.98	**99.99**	**99.99**

Table 3: Comparison of 'Accuracy' (in %)

appName	SVM	1-NN	Naive Bayes	Decision Tree	Neural Network	RF	fim-RF
HTTPWeb	98.20	97.47	92.74	99.12	98.75	99.38	**99.72**
SSH	99.78	99.95	99.34	99.92	99.95	99.97	**99.98**
ICMP	97.44	99.74	**100.0**	**100.0**	98.68	**100.0**	**100.0**
FTP	87.20	99.36	99.79	99.36	98.52	99.79	**100.0**
DNS	52.31	86.15	52.31	89.61	18.46	89.23	**98.49**

Table 4: Comparison of 'True Positive Rate' (in %)

appName	SVM	1-NN	Naive Bayes	Decision Tree	Neural Network	RF	fim-RF
HTTPWeb	0.96	0.16	1.64	0.05	0.96	0.08	**0.04**
SSH	1.39	0.23	1.11	0.26	0.26	0.33	**0.03**
ICMP	0.08	0.04	0.10	0.01	0.03	0.01	**0.00**
FTP	0.18	0.04	0.46	**0.02**	0.03	**0.02**	**0.02**
DNS	0.01	3.81	0.01	0.01	0.01	**0.00**	**0.00**

Table 5: Comparison of 'False Positive Rate' (in %)

According to the Tables 3, 4 and 5 the proposed fim-RF algorithm leads to the best 'accuracy', 'true positive rate' and 'false positive rate' results, for all the application layers in comparison with the other methods.

4.3.1. Relationships between the methods and application layers

To compare globally the different anomaly detection approaches, here we rely on a Multiple Correspondence Analysis (MCA), to analyze the *seven* methods (considered as individuals) and *five* application layers (considered as categorical variables). MCA is a data analysis technique for nominal categorical data and can be viewed as an extension of correspondence analysis (CA) which allows one to analyze the pattern of relationships of several categorical dependent variables. It can also incorporate quantitative variables. MCA is concerned with relationships within a set of variables, which usually are homogeneous, and allows the direct representation of individuals as points in geometric space.

To do so, each method is described by a vector ("–", "+","++",...), with as many dimensions as there are application layers, in which the modalities "++", "+" and "–" indicate whether the accuracy, detection rate or false alarm rate of a method on an application layer is respectively highly greater, greater or lower than the mean obtained for that application layer over all the methods. Distinct groups of methods, corresponding to distinct ways to perform on the different application layers, can be distinguished.

From Figure 2, one group (left-bottom) is defined by fim-RF, RF, DT and 1-NN and is opposed to the other methods as it yields the highest accuracy performances (corresponding to modality "++"). In addition, as one can see NB anomaly detection classifier yields the lowest accuracy (corresponding to modality "–"), particulary on DNS, HTTPWeb and SSH.

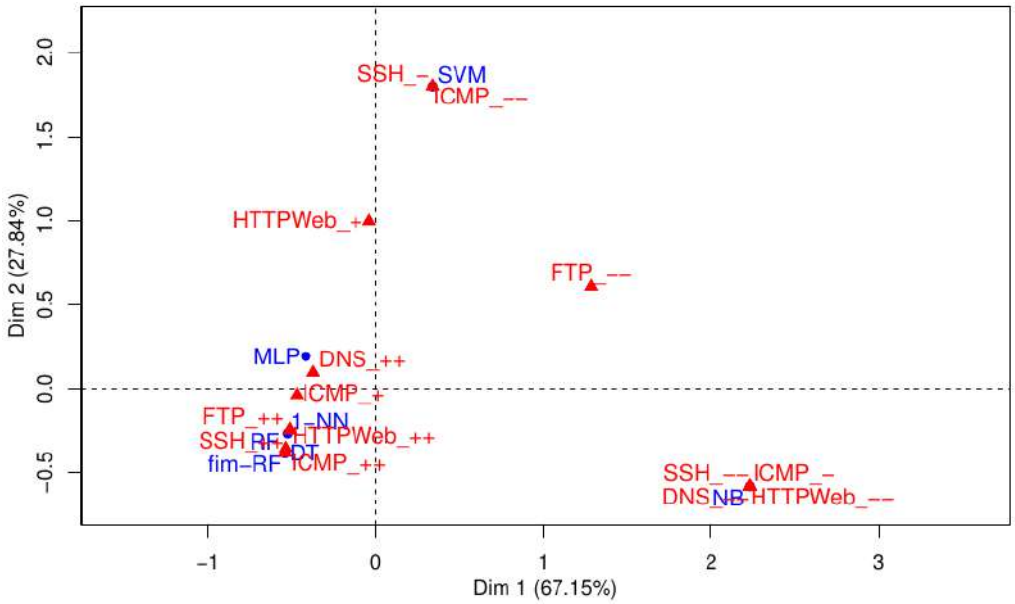


Figure 2: Global comparison of the 'Accuracy'

From Figure 3, similar as the previous figure, one can see that the fim-RF, RF, DT and 1-NN and outperform the other methods as they yield the highest true positive rates (corresponding to modality "++"). Finally, Figure 4 shows that fim-RF, RF and DT have the lowest false positive rate almost for all the application layer, while for instance, NB has the highest false alarm rate for HTTPWeb, FTP, ICMP and SSH, but good results for DNS (low false positive rate).

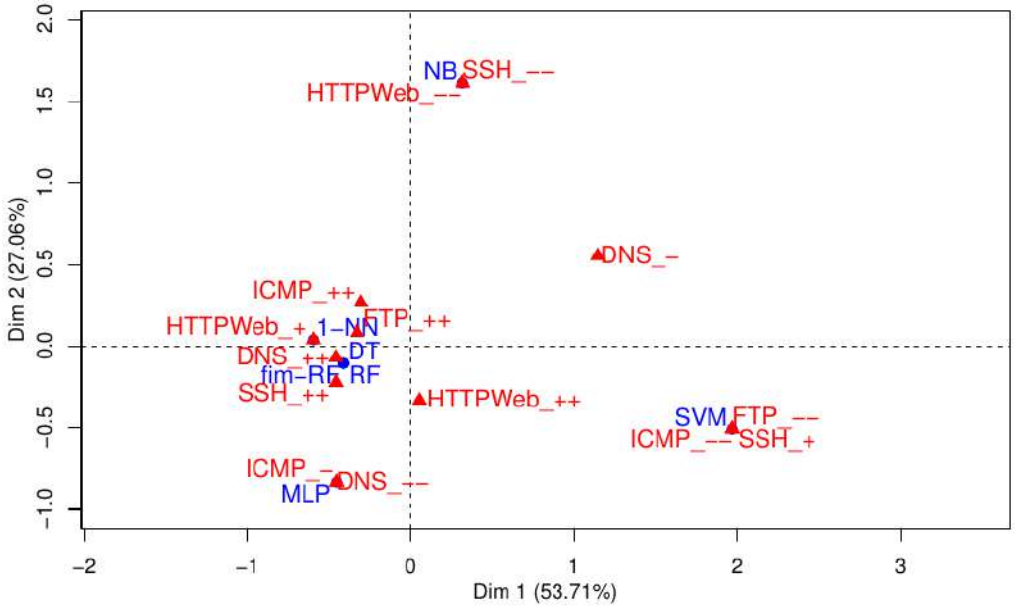


Figure 3: Global comparison of the 'Detection Rate'

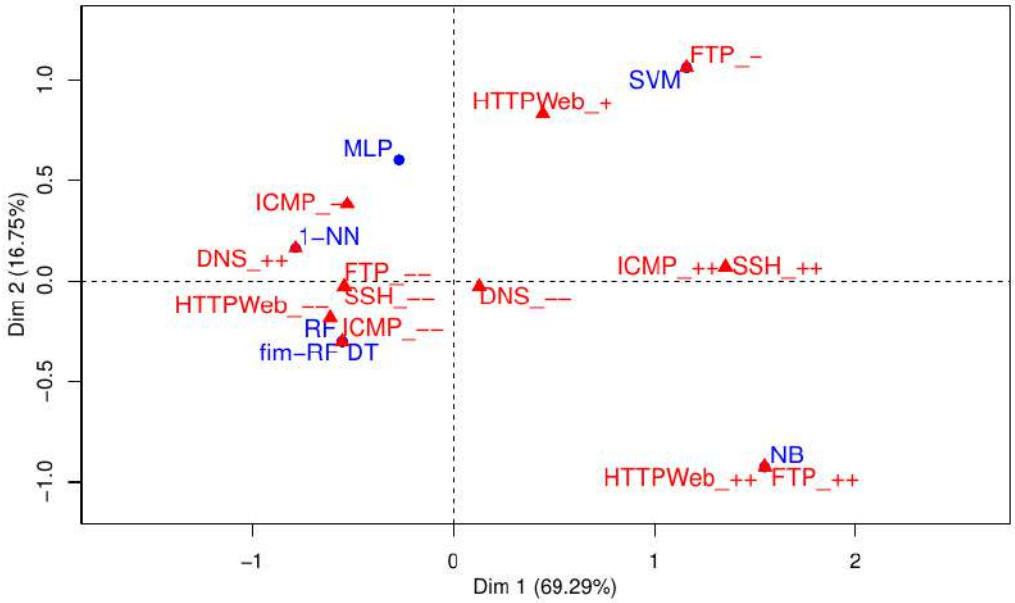


Figure 4: Global comparison of the 'False Alarm Rate'

5. Conclusion

Ensemble learning is a powerful machine learning paradigm which has exhibited apparent advantages in many applications. This paper has proposed an ensemble learning anomaly detection by using a machine learning role-based (i.e. random forest) and a pattern mining-based (frequent closed/maximal itemset) method. The efficiency of the introduced ensemble learning method (fim-RF) is analyzed on a dynamic, scalable and labeled dataset, called ISCX, which is now-days commonly explored for data intrusion benchmarking. The results illustrate that the fim-RF, in overall, outperforms the other state of the art methods (i.e. SVM, 1-NN, NB, MLP, Decision Tree and RF), through the commonly used measures: accuracy, true positive rate and false positive rate.

6. References

[1] V. J. Hodge and J. Austin, "A survey of outlier detection methodologies," *Artificial Intelligence Review*, vol. 22, pp. 85–126, Oct 2004.

[2] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, pp. 15:1–15:58, July 2009.

[3] E. Aleskerov, B. Freisleben, and R. B. Rao, "Cardwatch: a neural network based database mining system for credit card fraud detection," in *CIFEr*, 1997.

[4] C. Spence, L. Parra, and P. Sajda, "Detection, synthesis and compression in mammographic image analysis with a hierarchical image probability model," in *Proceedings of the IEEE Workshop on Mathematical Methods in Biomedical Image Analysis (MMBIA'01)*, MMBIA '01, (Washington, DC, USA), pp. 3–, IEEE Computer Society, 2001.

[5] B. Liu, S. Nath, R. Govindan, and J. Liu, "DECAF: Detecting and characterizing ad fraud in mobile apps," in *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*, (Seattle, WA), pp. 57–70, USENIX Association, 2014.

[6] R. Oentaryo, E.-P. Lim, M. Finegold, D. Lo, F. Zhu, C. Phua, E.-Y. Cheu, G.-E. Yap, K. Sim, M. N. Nguyen, K. Perera, B. Neupane, M. Faisal, Z. Aung, W. L. Woon, W. Chen, D. Patel, and D. Berrar, "Detecting click fraud in online advertising: A data mining approach," *J. Mach. Learn. Res.*, vol. 15, pp. 99–140, Jan. 2014.

[7] R. Fujimaki, T. Yairi, and K. Machida, "An approach to spacecraft anomaly detection problem using kernel feature space," in *Proceedings of the Eleventh ACM SIGKDD International Conference on Knowledge Discovery in Data Mining*, KDD '05, (New York, NY, USA), pp. 401–410, ACM, 2005.

[8] F. E. M.A., "Xli. on discordant observations," *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. 23, no. 143, pp. 364–375, 1887.

[9] D. E. Denning, "An intrusion-detection model," *IEEE Trans. Softw. Eng.*, vol. 13, pp. 222–232, Feb. 1987.

[10] W. Feng, Q. Zhang, G. Hu, and X. Huang, "Mining network data for intrusion detection through combining svms with ant colony networks," *Future Generation Comp. Syst.*, vol. 37, pp. 127–140, 2014.

[11] S. Agrawal and J. Agrawal, "Survey on anomaly detection using data mining techniques," in *KES*, 2015.

[12] S. Duque and M. N. bin Omar, "Using data mining algorithms for developing a model for intrusion detection system (ids)," *Procedia Computer Science*, vol. 61, pp. 46 – 51, 2015. Complex Adaptive Systems San Jose, CA November 2-4, 2015.

[13] E. M. Knorr, R. T. Ng, and V. Tucakov, "Distance-based outliers: Algorithms and applications," *The VLDB Journal*, vol. 8, pp. 237–253, Feb. 2000.

[14] M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "Lof: Identifying density-based local outliers," in *PROCEEDINGS OF THE 2000 ACM SIGMOD INTERNATIONAL CONFERENCE ON MANAGEMENT OF DATA*, pp. 93–104, ACM, 2000.

[15] H.-P. Kriegel, P. Kroger, E. Schubert, and A. Zimek, "Outlier detection in arbitrarily oriented subspaces," in *Proceedings of the 2012 IEEE 12th International Conference on Data Mining*, ICDM '12, (Washington, DC, USA), pp. 379–388, IEEE Computer Society, 2012.

[16] B. Schölkopf, J. C. Platt, J. C. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Neural Comput.*, vol. 13, pp. 1443–1471, July 2001.

[17] S. Hawkins, H. He, G. J. Williams, and R. A. Baxter, "Outlier detection using replicator neural networks," in *Proceedings of the 4th International Conference on Data Warehousing and Knowledge Discovery*, DaWaK 2000, (London, UK, UK), pp. 170–180, Springer-Verlag, 2002.

[18] Z. Zhou, "Ensemble learning," in *Encyclopedia of Biometrics*, pp. 411–416, Springer US, 2015.

[19] R. Polikar, "Ensemble learning," in *Ensemble machine learning*, Springer, Boston, MA, 2012.

[20] D. Opitz and R. Maclin, "Popular ensemble methods: An empirical study," *J. Artif. Int. Res.*, vol. 11, pp. 169–198, July 1999.

[21] T. Shon, Y. Kim, C. Lee, and J. Moon, "A machine learning framework for network anomaly detection using svm and ga," *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, pp. 176–183, 2005.

[22] H. F. Eid, A. Darwish, A. E. Hassanien, and A. Abraham, "Principle components analysis and support vector machine based intrusion detection system," 2010.

[23] I. Levner, "Feature selection and nearest centroid classification for protein mass spectrometry," *BMC Bioinformatics*, vol. 6, p. 68, Mar 2005.

[24] S. Soheily-Khah, *Generalized k-means based clustering for temporal data under time warp*. Theses, Universite Grenoble Alpes, Oct. 2016.

[25] R. Gil-Pita and X. Yao, "Using a genetic algorithm for editing k-nearest neighbor classifiers," in *Intelligent Data Engineering and Automated Learning - IDEAL 2007* (H. Yin, P. Tino, E. Corchado, W. Byrne, and X. Yao, eds.), (Berlin, Heidelberg), pp. 1141–1150, Springer Berlin Heidelberg, 2007.

[26] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A new intrusion detection system based on knn classification algorithm in wireless sensor network," *Journal of Electrical and Computer Engineering*, 2014.

[27] R. Entezari-Maleki, A. Rezaei, and B. Minaei-Bidgoli, "Comparison of classification methods based on the type of attributes and sample size.," *JCIT*, vol. 4, no. 3, pp. 94–102, 2009.

[28] M. Kukreja, S. A. Johnston, and P. Stafford, "Comparative study of classification algorithms for immunosignaturing data," *BMC bioinformatics*, vol. 13, p. 139, 2012.

[29] A. Ashari, I. Paryudi, and A. M. Tjoa, "Performance comparison between nave bayes, decision tree and k-nearest neighbor in searching alternative design in an energy simulation tool," *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 11, 2013.

[30] D. Barbara, N. Wu, and S. Jajodia, "Detecting novel network intrusions using bayes estimators," in *Proc. SIAM Intl. Conf. Data Mining*, 2001.

[31] N. A. Heard, D. J. Weston, K. Platanioti, and D. J. Hand, "Bayesian anomaly detection methods for social networks," *Ann. Appl. Stat.*, vol. 4, pp. 645–662, 06 2010.

[32] C. De Stefano, C. Sansone, and M. Vento, "To reject or not to reject: That is the question-an answer in case of neural classifiers," *Trans. Sys. Man Cyber Part C*, vol. 30, pp. 84–94, Feb. 2000.

[33] A. K. Ghosh and A. Schwartzbard, "A study in using neural networks for anomaly and misuse detection," in *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, (Berkeley, CA, USA), pp. 12–12, USENIX Association, 1999.

[34] M. F. Augusteijn and B. A. Folkert, "Neural network classification and novelty detection," *International Journal of Remote Sensing*, vol. 23, no. 14, pp. 2891–2902, 2002.

[35] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, pp. 5–32, Oct. 2001.

[36] T. K. Ho, "Random decision forests," in *Proceedings of the Third International Conference on Document Analysis and Recognition (Volume 1) - Volume 1*, ICDAR '95, (Washington, DC, USA), pp. 278–, IEEE Computer Society, 1995.

[37] A. Liaw and M. Wiener, "Classification and Regression by randomForest," *R News*, vol. 2, no. 3, pp. 18–22, 2002.

[38] J. Zhang, M. Zulkernine, and A. Haque, "Random-forests-based network intrusion detection systems," *Trans. Sys. Man Cyber Part C*, vol. 38, pp. 649–659, Sept. 2008.

[39] N. B. Saeid SOHEILY-KHAH, Pierre-Francois Marteau, "Intrusion detection in network systems through hybrid supervised and unsupervised machine learning process: A case study on the iscx dataset," *International Conference on Data Intelligence and Security, ICDIS*, 2018.

[40] T. Shi and S. Horvath, "Unsupervised learning with random forest predictors," *Journal of Computational and Graphical Statistics*, vol. 15, no. 1, pp. 118–138, 2006.

[41] P. Geurts, D. Ernst, and L. Wehenkel, "Extremely randomized trees," *Mach. Learn.*, vol. 63, pp. 3–42, Apr. 2006.

[42] M. Fernández-Delgado, E. Cernadas, S. Barro, and D. Amorim, "Do we need hundreds of classifiers to solve real world classification problems?," *J. Mach. Learn. Res.*, vol. 15, pp. 3133–3181, Jan. 2014.

[43] R. Agrawal, T. Imieliński, and A. Swami, "Mining association rules between sets of items in large databases," *SIGMOD Rec.*, vol. 22, pp. 207–216, June 1993.

[44] M. J. Zaki, "Mining maximal and closed frequent itemsets," in *New Generation of Data Mining Applications* (M. Kantardzic and J. Zurada, eds.), ch. 23, pp. 571–598, IEEE/Wiley Press, 2005.

[45] R. Agrawal and R. Srikant, "Fast algorithms for mining association rules in large databases," in *Proceedings of the 20th International Conference on Very Large Data Bases*, VLDB '94, (San Francisco, CA, USA), pp. 487–499, Morgan Kaufmann Publishers Inc., 1994.

[46] R. Srikant and R. Agrawal, "Mining sequential patterns: Generalizations and performance improvements," in *Proceedings of the 5th International Conference on Extending Database Technology: Advances in Database Technology*, EDBT '96, (London, UK, UK), pp. 3–17, Springer-Verlag, 1996.

[47] M. J. Zaki, "Sequence mining in categorical domains: Incorporating constraints," in *Proceedings of the Ninth International Conference on Information and Knowledge Management*, CIKM '00, (New York, NY, USA), pp. 422–429, ACM, 2000.

[48] J. Ayres, J. Flannick, J. Gehrke, and T. Yiu, "Sequential pattern mining using a bitmap representation," in *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '02, (New York, NY, USA), pp. 429–435, ACM, 2002.

[49] Z. Yang, Y. Wang, and M. Kitsuregawa, "Lapin: Effective sequential pattern mining algorithms by last position induction for dense databases," in *Advances in Databases: Concepts, Systems and Applications* (R. Kotagiri, P. R. Krishna, M. Mohania, and E. Nantajeewarawat, eds.), (Berlin, Heidelberg), pp. 1020–1023, Springer Berlin Heidelberg, 2007.

[50] Z. Yang and M. Kitsuregawa, "Lapin-spam: An improved algorithm for mining sequential pattern.," in *ICDE Workshops*, p. 1222, IEEE Computer Society, 2005.

[51] J. Han, J. Pei, B. Mortazavi-Asl, Q. Chen, U. Dayal, and M.-C. Hsu, "Freespan: Frequent pattern-projected sequential pattern mining," in *Proceedings of the Sixth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '00, (New York, NY, USA), pp. 355–359, ACM, 2000.

[52] J. Pei, J. Han, B. Mortazavi-asl, H. Pinto, Q. Chen, U. Dayal, and M. chun Hsu, "Prefixspan: Mining sequential patterns efficiently by prefix-projected pattern growth," in *17th international conference on data engineering*, pp. 215–224, 2001.

[53] W. Gan, J. C. Lin, P. Fournier-Viger, H. Chao, and P. S. Yu, "A survey of parallel sequential pattern mining," *CoRR*, vol. abs/1805.10515, 2018.

[54] M. El-Sayed, C. Ruiz, and E. A. Rundensteiner, "Fs-miner: Efficient and incremental mining of frequent sequence patterns in web logs," in *Proceedings of the 6th Annual ACM International Workshop on Web Information and Data Management*, WIDM '04, (New York, NY, USA), pp. 128–135, ACM, 2004.

[55] C. I. Ezeife, Y. Lu, and Y. Liu, "Plwap sequential mining: Open source code," in *Proceedings*

of the 1st International Workshop on Open Source Data Mining: Frequent Pattern Mining Implementations, OSDM '05, (New York, NY, USA), pp. 26–35, ACM, 2005.

[56] X. Yan, J. Han, and R. Afshar, "Clospan: Mining closed sequential patterns in large datasets," in *In SDM*, pp. 166–177, 2003.

[57] A. Gomariz, M. Campos, R. Marin, and B. Goethals, "Clasp: An efficient algorithm for mining frequent closed sequences," in *Advances in Knowledge Discovery and Data Mining* (J. Pei, V. S. Tseng, L. Cao, H. Motoda, and G. Xu, eds.), (Berlin, Heidelberg), pp. 50–61, Springer Berlin Heidelberg, 2013.

[58] F. Fumarola, P. F. Lanotte, M. Ceci, and D. Malerba, "Clofast: Closed sequential pattern mining using sparse and vertical id-lists," *Knowl. Inf. Syst.*, vol. 48, pp. 429–463, Aug. 2016.

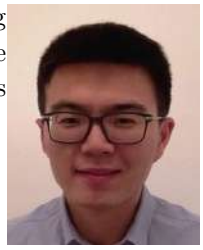
[59] M. J. Zaki, "Scalable algorithms for association mining," *IEEE Trans. on Knowl. and Data Eng.*, vol. 12, pp. 372–390, May 2000.

[60] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Comput. Secur.*, vol. 31, pp. 357–374, May 2012.

Authors

Saeid SOHEILY KHAH graduated in computer engineering, and received master degree in artificial intelligence & robotics in 2005. He then received his second master in information analysis and management from Skarbek university in Warsaw.In 2013, he joined to the LIG (Laboratoire d'Informatique de Grenoble) at Université Grenoble Alpes as a doctoral researcher. He successfully defended his dissertation and got his Ph.D in Oct 2016. In Nov 2016, he joined to the IRISA/Expression at Universit Bretagne Sud as a postdoctoral researcher. Lastly, in Oct 2017, he joined Skylads as a research scientist. His research interests are machine learning, data mining, cyber security system, anomaly detection, digital advertising and artificial intelligence.

Yiming WU received his B.S.E.E. degree from Northwestern Polytechnical University, Xian, China, 2011. He received his Ph.D. degree in Electrical Engineering from University of Technology of BelfortMontbliard, Belfort, France, 2016. He joined Skylads as a data scientist in 2018, and his research has addressed topics on machine learning, artificial intelligence and digital advertising.



AUTHOR INDEX

Abubakr Awad *315*
Ahmed Abdelgawad *77*
Ahmed Salama *315*
Alexandre Ricardo Soares Romariz *51*
Amal Alhosban *213*
Anderson R. Avila *233*
Anurag Kumar Pandey *195*
Anvitha Akurathi *213*
Atidel Lahoulou *233*
Besma Sadou *233*
Bhaskar Raj Sinha *303*
Chang-Yu Hsieh *41*
Charles Tappert *85, 221 & 297*
Chen-Fu Chiang *41*
Chih-Ling Huang *33*
Daniel Rosa Canêdo *51*
Di LIU *275*
El abderrahmani *267*
Faiza Ainennas *13*
Fatin Farhan Haque *77*
Fei Dai *257*
Felipe Rodriguez Yaguache *353*
Frank Walsh *77*
Hairong Zhao *91*
Hassan Badkoobehi *303*
Hend Shousha *315*
Husam Suleiman *99 & 133*
John Gauch *243*
John M. Acken *157 & 187*
Jun-Shuo Ng *77*
K.Satori *267*
Kimmo Ahola *353*
Kuljit Kaur Chahal *287*
Kumar Yelamarthi *77*
Lei Liu *275*
Mahasen Mabrouk *315*
Malika Yaici *13*
Manoj Muniswamaiah *85, 221 & 297*
Meng-Jia Lian *33*
Mohammad Amin *303*
Mohamad Ibrahim AL Ladan *341*
Naresh K. Sehgal *157 & 187*
Nassima Zidi *13*
Navinderjit Kaur Kahlon *287*
Nidhal Azawi *243*
Otman Basir *99 & 133*

Pradip Peter Dey *303*
R.Lasri *267*
Raid Khalid Hussein *119*
Robert Amador *41*
Ruichao Wang *01*
Ruppa K. Thulasiram *195*
Saeid Soheily-Khah *373*
Sam Lubbe *169*
Shaher Daoud *327*
Shahram Latifi *63*
Shirin Nasr Esfahani *63*
Shiv Shankar *157*
Tahany Awad *315*
Thavaneswaran *195*
Tiago H. Falk *233*
Tilak Agerwala *85, 221 & 297*
Tlamelo Phetlhu *169*
Toufik Bouden *233*
Tzer-Min Lee *33*
Vladimiro Sassone *119*
Wafaa Alakel *315*
Weijia Zhou *77*
Xiaobing Wang *257*
Xiao-Chun HOU *275*
Xiaolin Mi *257*
Xinyi He *257*
Yan-Bo LIU *275*
Yan-Cheng Wang *275*
Yanzhen Qu *327*
Yiming Wu *373*
Yulin Zhou *01*
Zahid Akhtar *233*
Zhihong Mao *01*