David C. Wyld,
Dhinaharan Nagamalai (Eds)

Computer Science & Information Technology

2nd International Conference on Machine Learning &Trends (MLT 2021), July 24~25, 2021, London, United Kingdom.

AIRCC Publishing Corporation

Volume Editors

David C. Wyld,
Southeastern Louisiana University, USA
E-mail: David.Wyld@selu.edu

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

ISSN: 2231 - 5403
ISBN: 978-1-925953-45-9
DOI: 10.5121/csit.2021.111101 - 10.5121/csit.2021.111114

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

Preface

The 2nd International Conference on Machine Learning &Trends (MLT 2021), July 24~25, 2021, London, United Kingdom, 7th International Conference on Control, Modeling and Computing (CMC 2021), 7th International Conference on Networks and Communications (NCO 2021), 7th International Conference on Software Engineering (SOFT 2021), 10th International Conference on Data Mining & Knowledge Management Process (CDKP 2021), 10th International Conference on Advanced Information Technologies and Applications (ICAITA 2021), 2nd International Conference on Cloud, Big Data and Web Services (CBW 2021) was collocated with 2nd International Conference on Machine Learning &Trends (MLT 2021). 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 MLT 2021, CMC 2021, NCO 2021, SOFT 2021, CDKP 2021, ICAITA 2021 and CBW 2021 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, MLT 2021, CMC 2021, NCO 2021, SOFT 2021, CDKP 2021, ICAITA 2021 and CBW 2021 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 MLT 2021, CMC 2021, NCO 2021, SOFT 2021, CDKP 2021, ICAITA 2021 and CBW 2021.

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.

David C. Wyld,
Dhinaharan Nagamalai (Eds)

General Chair — Organization

David C. Wyld, Southeastern Louisiana University, USA
Dhinaharan Nagamalai (Eds) Wireilla Net Solutions, Australia

Program Committee Members

Abdel-Badeeh M. Salem, Ain Shams University, Egypt
Abdelhadi Assir, Hassan 1st University, Morocco
Abdelhak Merizig, University of Biskra, Algeria
Abdullah, Adigrat University, Africa
Abhas Kumar Singh, Sri Venkateswara College of Engineering, India
Addisson Salazar, Universitat Politècnica de València, Spain
Adriana Carla, Universidade Federal de Campina Grande, Brazil
Afaq Ahmad, Sultan Qaboos University, Oman
Ahmad Azzam, Jadara University, Jordan
Ahmad Fakharian, Islamic Azad University, Iran
Ahmad Khasawneh, Hashemite University, Zarqa-Jordan
Ahmed Elngar, Beni-Suef University, Egypt
Aishwarya Asesh, Adobe, USA
Ajay Anil Gurjar, Sipna College of Engineering & Technology, India
Akhil Gupta, Lovely Professional University, India
Ali Fazeli, University of Tehran, Iran
Ali Kaveh, Iran University of Science and Technology, Iran
Alireza Valipour Baboli, University Technical and Vocational, Iran
Aman Jatain, Amity University, India
Amel Borgi, Universite de Tunis El Manar, Tunisia
Amel Ourici, University Badji Mokhtar Annaba, Algeria
Amer AbuAli, Taibah University, KSA
Anamika Ahirwar, Jayoti Vidhyapeeth Women's University, Jaipur, India
Anand Nayyar, Duy Tan University, Vietnam
Anas Alsobeh, Yarmouk University, Jordan
Anirban Banik, National Institute of Technology Agartala, India
Ashad Kabir, Charles Sturt University, Australia
Atanu Nag, Modern Institute of Engineering & Technology, India
Aubrun, Christophe University of Lorraine, France
Bars, Ruth Technical Univ. of Budapest, Hungary
Berenguel, Manuel Universidad de Almeria, Spain
Beshair Alsiddiq, Prince Sultan University, Saudi Arabia
Bhagyashree S R, ATME College of Engineering, India
Blasco, Xavier Universitat Politécnica de Valencia, Spain
Bogdan, Stjepan Univ. of Zagreb, Croatia
Bokor, Jozsef Hungarian Academic of Sciences, Hungary
Bouhorma Mohammed, Abdelmalek Essaadi University, Morocco
Boukari nassim, Skikda University, Algeria
BRAHAMI Menaouer, National Polytechnic School of Oran, Algeria
Bucher, Roberto Scuola Univ. Professionale, Switzerland
Camacho, Eduardo F. Universidad de Sevilla, Spain
Carlos Juiz, University of the Balearic Islands, Spain
Casavola, Alessandro Universita' Della Calabria, Italy
Cheng Siong Chin, Newcastle University, Singapore

Muhammad Sarfraz,	Kuwait University, Kuwait
Munish Sabharwal,	Galgotias University, India
Mu-Song Chen,	Da-Yeh University, Taiwan
Mu-Yen Chen,	National Cheng Kung University, Taiwan
Nalini Chidambaram,	Bharath University, India
Narasimham Challa,	SR Engineering College, India
Neda Darvish,	Islamic Azad University, Iran
Neha Pattan,	Carnegie Mellon University, USA
Nembhard,	Florida Institute of Technology, USA
Okwonu,	Universiti Utara Malaysia, Malaysia
Oleksii K. Tyshchenko,	University of Ostrava, Czech Republic
Omid Mahdi Ebadati,	Kharazmi University, Tehran
Osama Rababah,	The University of Jordan, Jordan
Oscar Mortágua Pereira,	University of Aveir, Portugal
Otilia MANTA,	Romanian American University (RAU), Romania
Pavel Loskot,	ZJU-UIUC Institute, China
Peiman Mohammadi,	Islamic Azad University, Iran
Piotr Kulczycki,	AGH University of Science and Technology, Poland
Pitambar Behera,	Jawaharlal Nehru University, India
Prapai Sridama,	BSRU, Thailand
Quang Hung Do,	University of Transport Technology, Vietnam
R Senthil,	Shinas College of technology, Oman
R. S. Balagadde,	Kampala International University, Uganda
R.Sujatha,	VIT University, India
Raed Ibraheem Hamed,	University of Anbar, Iraq
Rafael Valencia Garcia,	University of Murcia, Spain
Rahmat Widia Sembiring,	Politeknik Negeri Medan, Indonesia
Rajeev Kanth,	Savonia University of Applied Sciences, Finland
Ramadan Elaiess,	University of Benghazi, Libya
Randle Olwuarotimi A,	Tshwane University Of Technology, South Africa
Rao Kotagiri,	University of Melbourne, Australia
Ratnesh Litoriya,	Jaypee University of Engineering, India
Ravi Kumar CV,	VIT University, India
Reyhane Agrarian,	Shiraz University, Iran
Reza Ebrahimi Atani,	University of Guilan, Iran
Richa Purohit,	D Y Patil International University India
Ritu Sharma,	Himachal Pradesh University Shimla, India
Roberto Bruzzese,	Freelancer, Italy
Rodrigo Pérez Fernández,	Universidad Politécnica de Madrid, Spain
Rosalba Cuapa Canto,	Universidad Autonoma de Puebla, Mexico
Ruksar Fatima,	KBN College of Engineering, India
S.Taruna,	JK Lakshmipat University, India
Saad Aljanabi,	Al- Hikma College University, Iraq
Sa'Adah Hassan,	Universiti Putra Malaysia, Malaysia
Sabina Rossi,	Universita Ca' Foscari Venezia, Italy
Sahar Saoud,	Ibn Zohr University, Morocco
Said elkassimi,	Usms Beni Mellal, Morocco
Said Nouh,	Hassan II university of Casablanca, Morocco
Saif aldeen Saad Obayes,	University of technology, Iraq
Saleh Al-Daajeh,	Abu Dhabi polytechnic, UAE
Sameerchand Pudaruth,	University of Mauritius, Mauritius
Samir Kumar Bandyopadhyay,	University of Calcutta, India

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)

7th International Conference on Control, Modeling and Computing (CMC 2021)

Model-Based Systems Engineering Approach with SysML for an Automatic Flight Control System…….....01-19
Haluk Altay and M. Furkan Solmazgül

7th International Conference on Networks and Communications (NCO 2021)

Secure Protocol for Four D2D Scenarios……..…….21-33
Hoda Nematy

Enhancing Security in Internet of Things Environment by Developing an Authentication Mechanism using COAP Protocol……..……..…..…….35-54
Samah Mohammed S ALhusayni and Wael Ali Alosaimiv

7th International Conference on Software Engineering (SOFT 2021)

Product Quality Evaluation Method (PQEM): A Comprehensive Approach for the Software Product Life Cycle…..…….....…….55-71
Mariana Falco and Gabriela Robiolo

10th International Conference on Data Mining & Knowledge Management Process (CDKP 2021)

A Generalized Approach to Data Supply Chain Management – Balancing Data Value and Data Debt……..……..……...…..73-79
Roberto Maranca and Michele Staiano

Appraisal Study of Similarity-Based and Embedding-Based Link Prediction Methods on Graphs ……..……..……..……...…..81-92
Md Kamrul Islam, Sabeur Aridhi and Malika Smail-Tabbone

2nd International Conference on Machine Learning &Trends (MLT 2021)

Credit Card Fraud Detection using Supervised and Unsupervised Learning 93-99
Vikas Thammanna Gowda

Dense-Res Net for Endoscopic Image Classification…….....101-108
Quoc-Huy Trinh and Minh-Van Nguyen

Using Multilinear Feature Space to Accelerate CNN Classification.....109-122
Michel Andre L .Vinagreiro, Edson C. Kitani, Armando Antonio M. Lagana and Leopoldo R. Yoshioka

Parallel Evolutionary Biclustering of Short-term Electric Energy Consumption.....123-137
Diego P. Pinto-Roa, Hernán Medina, Federico Román, Miguel García-Torres, Federico Divina, Francisco Gómez-Vela, Félix Morales, Gustavo Velázquez, Federico Daumas, José L. VázquezNoguera, Carlos Sauer Ayala and Pedro E. Gardel-Sotomayor

10th International Conference on Advanced Information Technologies and Applications (ICAITA 2021)

Stack and Deal: An Efficient Algorithm for Privacy Preserving Data Publishing.....139-148
Vikas Thammanna Gowda

Impact of E-maintenance over Industrial Processes.....149-156
Yassine MOUMEN, Mariam BENHADOU and Abdellah HADDOUT

Lattice Based Group Key Exchange Protocol in the Standard Model.....157-174
Parhat Abla

2nd International Conference on Cloud, Big Data and Web Services (CBW 2021)

The 5 Dimensions of Problem Solving using DINNA Diagram: Double Ishikawa and Naze Naze Analysis.....175-183
Mohammed Hamoumi, Abdellah Haddout and Mariam Benhadou

MODEL-BASED SYSTEMS ENGINEERING APPROACH WITH SYSML FOR AN AUTOMATIC FLIGHT CONTROL SYSTEM

Haluk Altay and M. Furkan Solmazgül

Teknopark Istanbul, Turkish Aerospace, Istanbul, Turkey

ABSTRACT

Systems engineering is the most important branch of engineering in interdisciplinary study. Successfully performing a multidisciplinary complex system is one of the most challenging tasks of systems engineering. Multidisciplinary study brings problems such as defining complex systems, ensuring communication between stakeholders, and common language among different design teams. In solving such problems, traditional systems engineering approach cannot provide an efficient solution. In this paper, a model-based systems engineering approach is applied with a case study and the approach is found to be more efficient. In the case study, the design of the helicopter automatic flight control system was realized by applying model-based design processes with integration of tools. Requirement management, system architecture management and model-based systems engineering processes are explained and applied of the case study. Finally, model-based systems engineering approach is proven to be effective compared with the traditional systems engineering methods for complex systems in aviation and defence industries.

KEYWORDS

Model-Based Systems Engineering, Automatic Flight Control System, SysML.

1. INTRODUCTION

In order to understand Model-based systems Engineering, it is necessary to know the definition and scope of the systems engineering. The definition of systems engineering is defined as follows in the references.

“Systems engineering is an interdisciplinary approach and means to enable the realization of successful systems.” [1]

“Systems engineering is a discipline that concentrates on the design and application of the whole (system) as distinct from the parts. It involves looking at a problem in its entirety, considering all the facets and all the variables and relating the social to the technical aspect.” [2]

Considering these reference definitions, within the scope of this case study, the definition of systems engineering is made as follows.

“Systems engineering is a multidisciplinary and common mind approach that ensures successful realization of systems.”

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 01-19, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111101

The definition of model-based systems engineering is defined as follows in the references.
"Model-based systems engineering (MBSE) is the formalized application of modelling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases." [3]
Considering these reference definitions, within the scope of this case study, the definition of model-based systems engineering is made as follows.

"Model-based systems engineering is an approach to successfully realize systems driven by a model, with a consistent set of views that reflect multiple perspectives of the system."

The traditional systems engineering definition has been made to the systems engineering activities carried out before the model-based systems engineering approach. Traditional systems engineering has three main problems, such as being inadequate in defining complex systems, communication between stakeholders, and common language and interpretation among different design teams. In the case study, model-based systems engineering processes are applied and as a result, main problems are eliminated. Model-based systems engineering approach has multiple advantages over traditional systems engineering.

- Automatic generation of most of system documents by using the developed models.
- Since the models can be measured, it is easy to control and manage in complex systems.
- Consistency for all information in the system architecture thanks to the models.
- Ensuring traceability in the life cycle stages of the system with using SysML for modelling and maintaining tool integration.
- Easier to access information since a certain systematic is applied while the model is being established.
- More understandable communication establishment thanks to the representation of requirements as a model and the use of a common language for this model.
- Improving communication as a result of the establishment of common terminology and concepts between all stakeholders and design teams of a system.

It is important for companies that model-based systems engineering benefits are directly related to cost, time or resource savings. Adapting the model-based systems engineering approach to reflect the company's working principles is the most critical point for the efficiency of this process.

2. DESIGN METHOD

In the INCOSE System Engineering Handbook document that there are 6 different methods of model-based systems engineering. [1] These methods are INCOSE Object-Oriented Systems Engineering Method (OOSEM), IBM Rational Telelogic Harmony-SE, IBM Rational Unified Process for Systems Engineering (RUP-SE), Vitech MBSE Methodology, JPL State Analysis (SA) and Dori Object – Process Methodology (OPM).

The methods that mentioned above have been examined and a suitable method has been determined for the flight control system. The method created is shown in Figure 1.

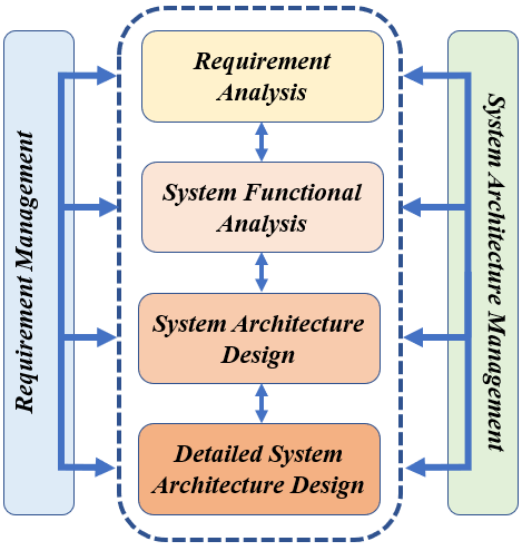


Figure 1. Model-Based Systems Engineering (MBSE) process

Model-based System Engineering processes; requirements analysis, system functional analysis, system architecture design and detailed system architecture design. Requirement and system architecture management are required throughout MBSE processes. By this means, process traceability and an iterative design are provided. The method followed from the customer requirements that are the input of the MBSE process to the system requirements and the system architecture that are the outputs of the process are shown in Figure 2.

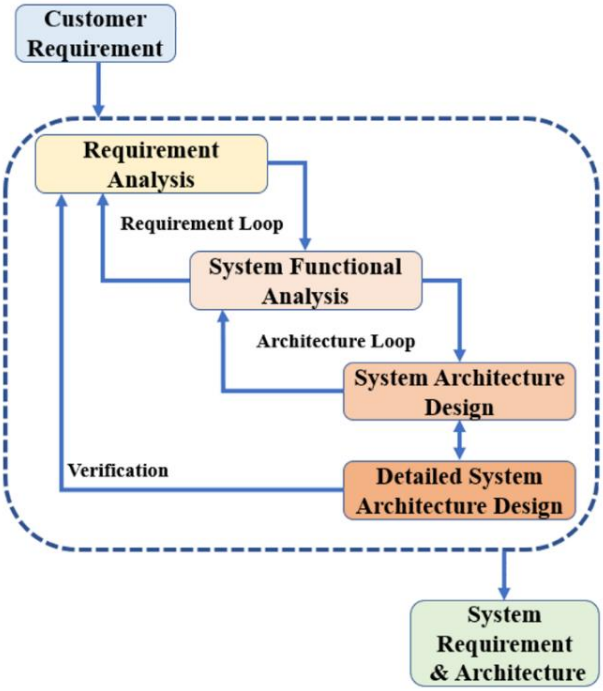


Figure 2. Model-Based Systems Engineering (MBSE) process with input and outputs [4]

In the case study of helicopter automatic flight control system, Model-based System Engineering process was carried out with reference to the ARP4754A document and the relevant sections of the DO-178C / 331 standard document listed below.

- ARP-4754A Section 4.5 Allocation of System Requirements to Items
- ARP-4754A Section 5.3 Requirements Capture
- ARP-4754A Section 5.4 Requirements Validation
- DO-178C/DO-331 Section 2.1 System Requirements Allocation to Software
- DO-178C Table A-2 Software Development Process
- DO-178C Table A-3 Verification of Outputs of Software Requirement Process

3. DESIGN

Helicopter automatic flight control system architecture design was realized by using SysML with the Model-based systems engineering approach. The design process was carried out in accordance with the method described above.

3.1. Requirement Management

Requirement management is an iterative process that continues throughout model-based systems engineering processes of the case study. Requirement management covers the following processes:

- Definition of requirements
- Validation of requirements
- Traceability and verification of requirements
- Transfer and synchronization of requirements.

In the requirement management, managing the requirements with a single software ensures that each stage is carried out more efficiently. In this case study, DOORS software was selected for requirement management processes. The relationship between the requirements in the DOORS and the model elements in the system architecture which is modelled with SysML was created by using IBM Rational Rhapsody.

3.1.1. Definition of Requirements

Within the scope of the case study three set of requirements were created by using DOORS:

- Contractual requirements that defining the behaviours that are targeted to occur in the system and received from costumer.
- System requirements that defining all functions and properties of system.
- Software requirements that taken as reference when designing flight control computer and implementing the software.

Requirement sets are defined in a hierarchy as in Figure 3. Thus, the levels at which the requirements are created, and which standards are used as the source when deriving the requirement sets are shown in Figure 3.

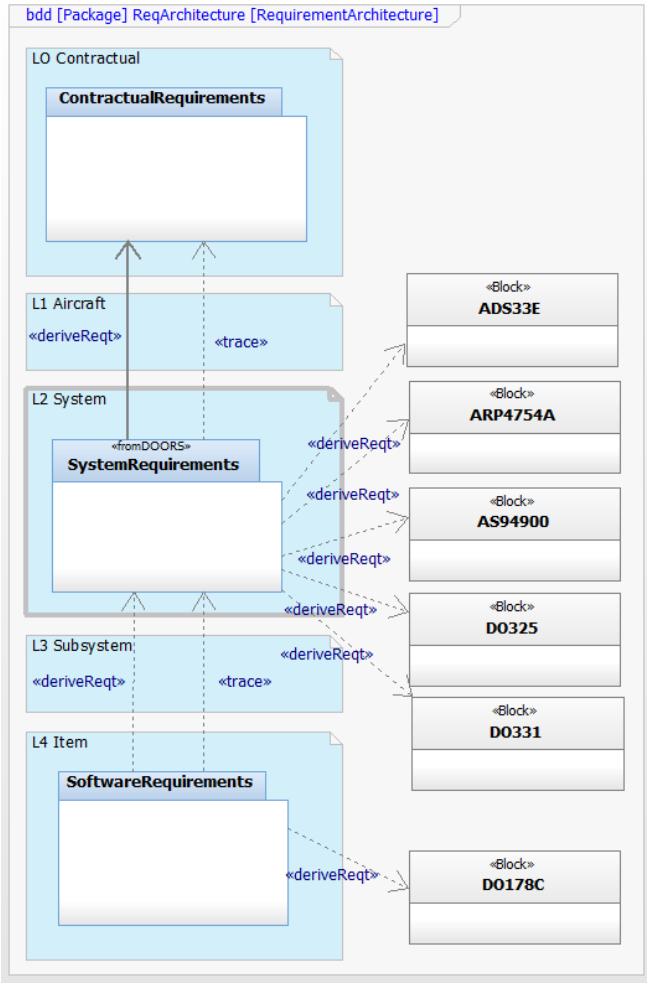
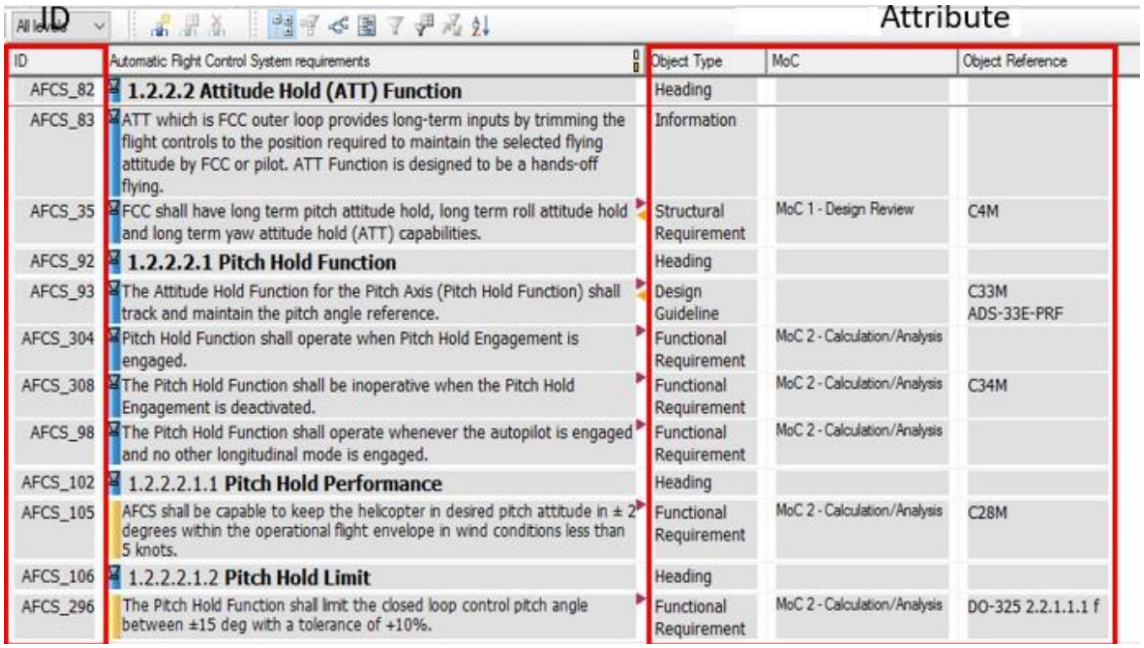


Figure 3. Requirement hierarchy

Unique ID assignment is made to each requirement in the requirement set. In addition, attributes that define requirements specifically are created for requirement sets. Object type means of complies (MoC) and requirement source / reference attributes were defined for system requirements.

- Object type refers to type of the requirements according to its content. The created object types are Information, Heading, Design Guideline, Structural Requirements and Functional Requirements.
- Means of compliance (MoC), expresses with which method to validate the requirements. The created MoC are Compliance Statement, Design Review, Calculation/Analysis, Safety Assessment, Laboratory Tests, Ground Tests, Flight Tests, Design Inspection/Audit, Simulation and Equipment Qualification.
- Object Reference refers to the source of the created requirements. The created object references are Engineering Judgment, Contractual Requirements and Standards.

An example of the ID and attributes defined in the requirements is as in Figure 4.



ID	Automatic Flight Control System requirements	Object Type	MoC	Object Reference
AFCS_82	**1.2.2.2 Attitude Hold (ATT) Function**	Heading		
AFCS_83	ATT which is FCC outer loop provides long-term inputs by trimming the flight controls to the position required to maintain the selected flying attitude by FCC or pilot. ATT Function is designed to be a hands-off flying.	Information		
AFCS_35	FCC shall have long term pitch attitude hold, long term roll attitude hold and long term yaw attitude hold (ATT) capabilities.	Structural Requirement	MoC 1 - Design Review	C4M
AFCS_92	**1.2.2.2.1 Pitch Hold Function**	Heading		
AFCS_93	The Attitude Hold Function for the Pitch Axis (Pitch Hold Function) shall track and maintain the pitch angle reference.	Design Guideline		C33M ADS-33E-PRF
AFCS_304	Pitch Hold Function shall operate when Pitch Hold Engagement is engaged.	Functional Requirement	MoC 2 - Calculation/Analysis	
AFCS_308	The Pitch Hold Function shall be inoperative when the Pitch Hold Engagement is deactivated.	Functional Requirement	MoC 2 - Calculation/Analysis	C34M
AFCS_98	The Pitch Hold Function shall operate whenever the autopilot is engaged and no other longitudinal mode is engaged.	Functional Requirement	MoC 2 - Calculation/Analysis	
AFCS_102	1.2.2.2.1.1 **Pitch Hold Performance**	Heading		
AFCS_105	AFCS shall be capable to keep the helicopter in desired pitch attitude in ± 2 degrees within the operational flight envelope in wind conditions less than 5 knots.	Functional Requirement	MoC 2 - Calculation/Analysis	C28M
AFCS_106	1.2.2.2.1.2 **Pitch Hold Limit**	Heading		
AFCS_296	The Pitch Hold Function shall limit the closed loop control pitch angle between ±15 deg with a tolerance of +10%.	Functional Requirement	MoC 2 - Calculation/Analysis	DO-325 2.2.1.1.1 f

Figure 4. Requirements in DOORS with attribute columns

3.1.2. Validation of Requirements

It indicates that the requirements are complete and correct. Validation process is usually done using a checklist of requirements. Requirements are updated by considering the missing and inaccurate statements resulting from the checklist and analysis.

Table 1. Example of requirement validation checks [7]

No	Correctness Checklist
1	Is it identifiable as a requirement?
2	Is the requirement redundant?
3	Does the requirement conflict with others?
4	Is it physically possible to meet the requirements?
5	Is the requirement set better suited to be combined into a single requirement?

3.1.3. Validation of Requirements

Traceability in requirements defines the whole life process of requirements. The life process of requirements starts from where its history and source are based and continues to new requirements that will be created throughout the development period. The requirement set with more general expressions is defined as the highest level, and the requirement set with all the details to design a system is defined as the lowest level. Traceability between requirements occurs when a lower level requirement meets a higher-level requirement. In this case study, traceability has been provided between the lowest level software requirement set and the highest-level customer requirement set with the connections. Traceability of the requirements is very important for verifying the requirements. Verification of requirements are defined as demonstrating that the system is designed correctly according to customer requirements as a result of implementation of the requirements. The requirement validation process begins after the design is finished and checks that the design has been made in accordance with the requirements.

There are several methods (MoC) for requirement verification. Some of the requirement validation methods are shown in Table 2.

Table 2. Means of compliances

MoC Code	MoC Description	Associated Compliance Documents	Definition
MoC 1	Design Review	Descriptions Drawings	Compliance is proven by the design review minutes, system description documents, drawings, etc.
MoC 2	Calculation and Analysis	Substantiation reports	Compliance is proven by an analysis activity and report, such as static and fatigue strength analysis, load analysis, platform performance analysis, off-line simulation modelling analysis etc
MoC 3	Safety Assessment	Safety analysis	Compliance is proven by reference to the safety documentation defined in Safety Program Plan.
MoC 4	Laboratory tests	Test programs Test reports	Compliance is proven by tests done on i.e. a specific rig test, subsystem bench test or system integration test activity

Before the verification of the requirements, test scenarios are created according the requirements. The models developed at the design stage are tested to verify the requirements. If the system features in requirements are satisfied completely in the test results, requirements are considered verified.

3.1.4. Transfer and Synchronization of Requirements

By transfer and synchronization between the IBM Rational Rhapsody that is created models of requirements and "DOORS" that is managed of the requirements were provided to continuous integration between requirements and models. As shown in Figure 5, integration is provided by using IBM Rational Rhapsody Gateway add on.

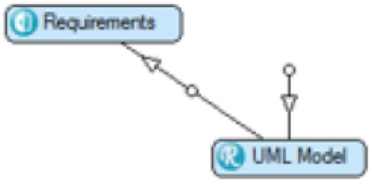


Figure 5. Requirements and model connection in IBM Rational Rhapsody Gateway

3.2. System Architecture Management

System architecture management is carried out with SysML which is a visual / graphic based architectural modelling language used in systems engineering applications. SysML has a grammar and vocabulary just like any of the natural languages we speak in this World (ex. English, Japanese etc.) [5]. Models are created to develop system architectures with SysML.

SysML models are examined under three main titles structural, behavioural and requirement. Various diagrams are used to create SysML models. SysML diagrams are shown in Figure 6.

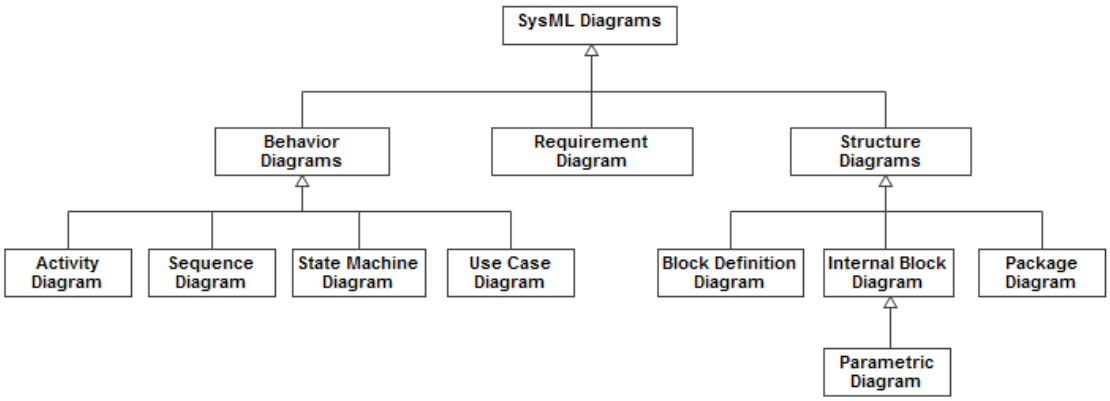


Figure 6. SysML taxonomy

The structural expression of a model answers the question: What is the system? Structural models are used to

- define the system,
- define system components,
- define system features,
- define system constraints,
- define the system model organization,
- determine their behaviour,
- define the relationships between system elements.

The behavioural expression of a model answers the question: How is the system behaves? Behavioural models are used to

- define the behaviour of the system,
- define use case of the system,
- define functions of system,
- define activities of system,
- define sequence of behaviour,
- define operations within the system elements.

Within the context of the case study, a hierarchy was created using SysML that contains the packages related to the its contents. The hierarchy shown in Figure 7 is the model organization of the system and was created using packages.

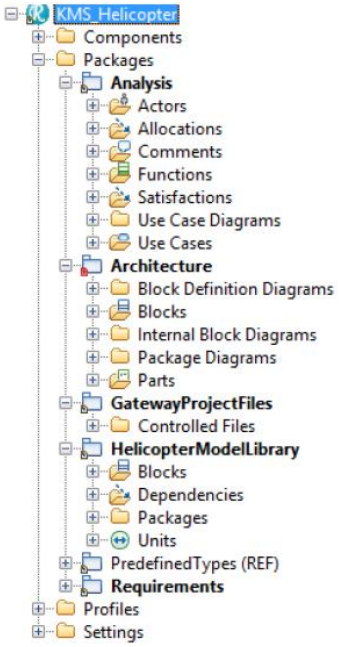


Figure 7. Case study model organization

System architecture management is provided by this model organization. Model organization was created with 6 different packages:

- The "Analysis" package consists of behavioural models and requirement analysis including Use Case Diagrams, Activity Diagrams, Sequence Diagrams.
- The "Architecture" package consists of structural models containing Block Definition Diagrams, Internal Block Diagrams and Package Diagrams.
- The “GatewayProjectFiles” package, consists of IBM Rational Rhapsody Gateway project files that provide communication between DOORS software used in requirement management and IBM Rational Rhapsody software where the system architecture is realized, and which contain various relationships between each other.
- The “HelicopterModelLibrary” package is a library containing the model elements, relationships, units and sub-packages used in the study.
- The "PredefinedTypes" package consists of models containing stereotypes representing the features to be used in the case study. It is defined automatically when the SysML project is created.
- The "Requirements" package includes models of requirements created within the scope of the case study and requirements found in the DOORS software.

3.3. Model-Based Systems Engineering Processes

Model-based systems Engineering (MBSE) is an approach used to reveal the needs that involve different perspectives of stakeholders, which one of the problems of systems engineering, and to analyse these requirements with models and make them more detailed and understandable. Thus, in complex systems like a helicopter, the entire process from customer requirements to system requirements and system architecture can be explained with this approach. In this process, requirements analysis, functional analysis, system architecture design and detailed system architecture design phases are carried out respectively.

3.3.1. Requirement Analysis

The requirements analysis process is the first phase of the model-based systems engineering process. The input of the requirements analysis process is the customer requirements, and the output is the use case models of the system. The requirements analysis process includes the design steps listed below:

- Examining customer requirements and determining required behaviours (use case)
- Derivation of preliminary system requirements for the use case determined with reference to customer requirements and standards
- Linking the derived system requirements to customer requirements.

Models are used when expressing targeted behaviours (use case) in the model-based systems engineering process. In SysML, the use case that is created with using phrases and actors of the system are expressed with the Use Case Diagram. After classification of customer requirements, use cases and actors are built in use case diagrams shown in Figure 8 to link the related requirements. It is intended to cover all customer requirements during the use case definition process. In addition to the actors and system boundary have been defined.

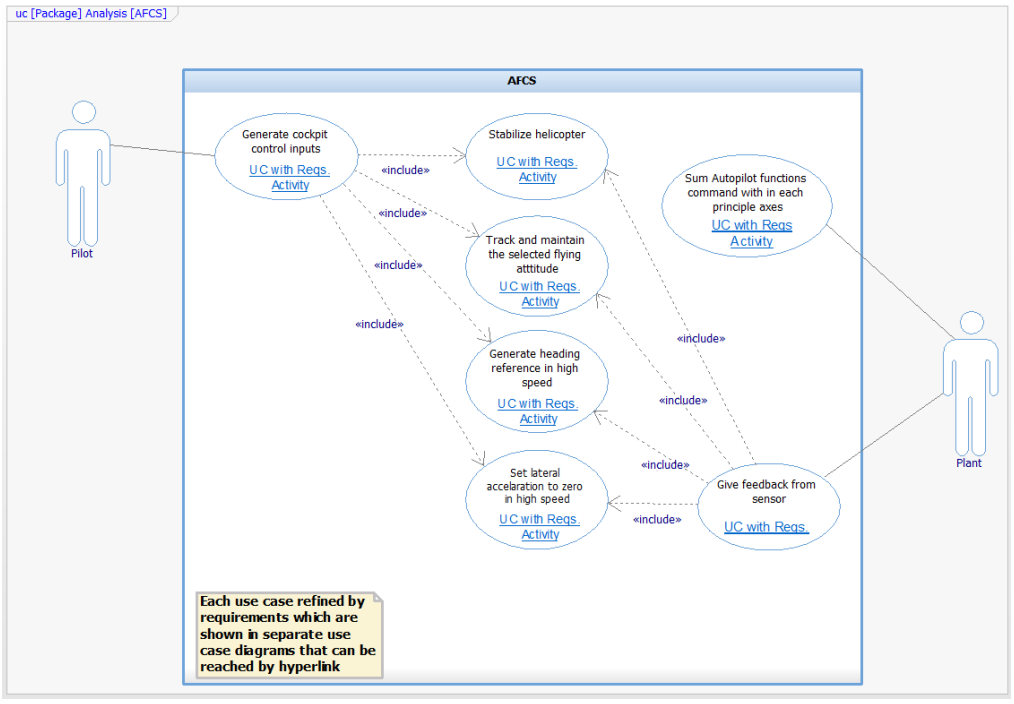


Figure 8. Use Case Diagram example from case study

After creating the success and establishing connections, preliminary system requirements started to be produced. The system requirements derived for “stabilized helicopter” use case and the “refine” connection between use case and system requirements in the Use Case Diagrams are linked as shown in Figure 9. Thus, system requirements have been created for the relevant use case.

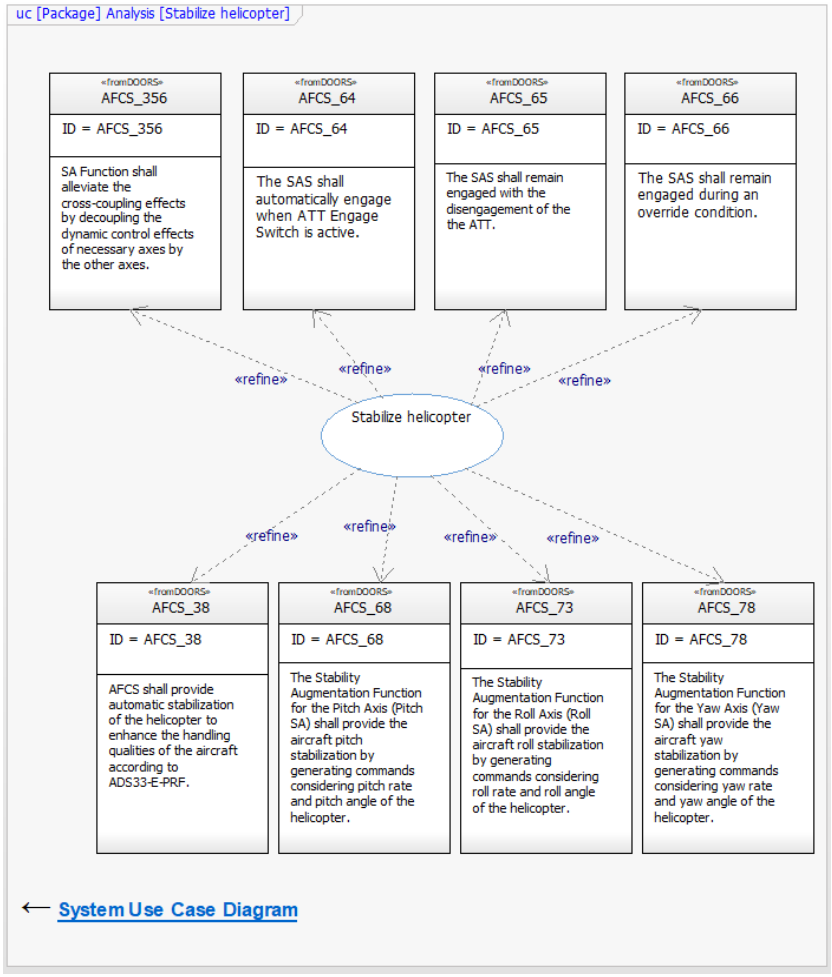


Figure 9. Use Case Diagram example with refine dependency

3.3.2. System Functional Analysis

The functional analysis process is the second phase of the Model-based System Engineering process. Functional analysis is defined as a systematic process for defining and associating the functions that a system must perform in order to be successful. The functional analysis process is carried out for the following steps.

- To define all the functions that the system must fulfil to meet the requirements in a graphical model.
- Allocation of detail requirements created as a result of detailing system requirements
- Defining sub-functions required for each function by making functional decomposition
- Explain what to do and how to do it before implementing the requirements.

The steps in the functional analysis process are shown in the Figure 10. [6]

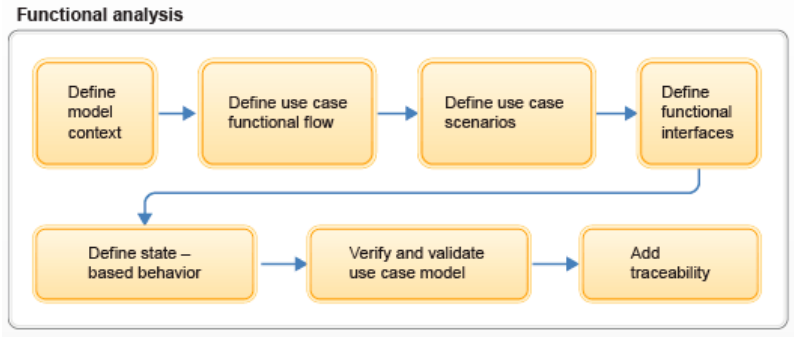


Figure 10. Functional analysis process

In the functional analysis process, which is one of the model-based systems engineering processes, the definition of the model content is determined by the use case. The creation of the detailed use case functional flow is provided by Activity Diagrams. While creating activity diagrams, actions are determined firstly, and control flow is obtained by taking into account the order of realization of these actions.

In the process of defining the scenarios of the use case, it is determined how a system can perform its use cases and whether there are any conflicts or conflicts between the lower level functions (actions) while performing these behaviours.

In the process of defining functional interfaces, the basic interactions between the system and the environment and the interconnections of the behaviours of the system components are defined. The inputs containing the data received from the outside of the actions and the outputs containing the data given out are determined.

Activity Diagrams created for the realization of the use cases that are desired to be in the system during the verification and validation of the use case model are verified by animations.

In the process of ensuring traceability, which is the final stage of functional analysis, it is shown that all requirements are covered by connecting requirements with Use case diagram components. The connection relationship is provided by “satisfy”.

The Activity Diagram shows the dynamic aspects of a system and the action-to-action control flow. It defines the basic interactions between the system and the environment, or the interconnections of the behaviour of the components. An Activity Diagram allows you to accurately transfer the most complex behavioural goals by creating different scenarios with various types of action. The "SAS" Activity Diagram created for the "stabilized helicopter" use case is as shown in Figure 11 with the data flow.

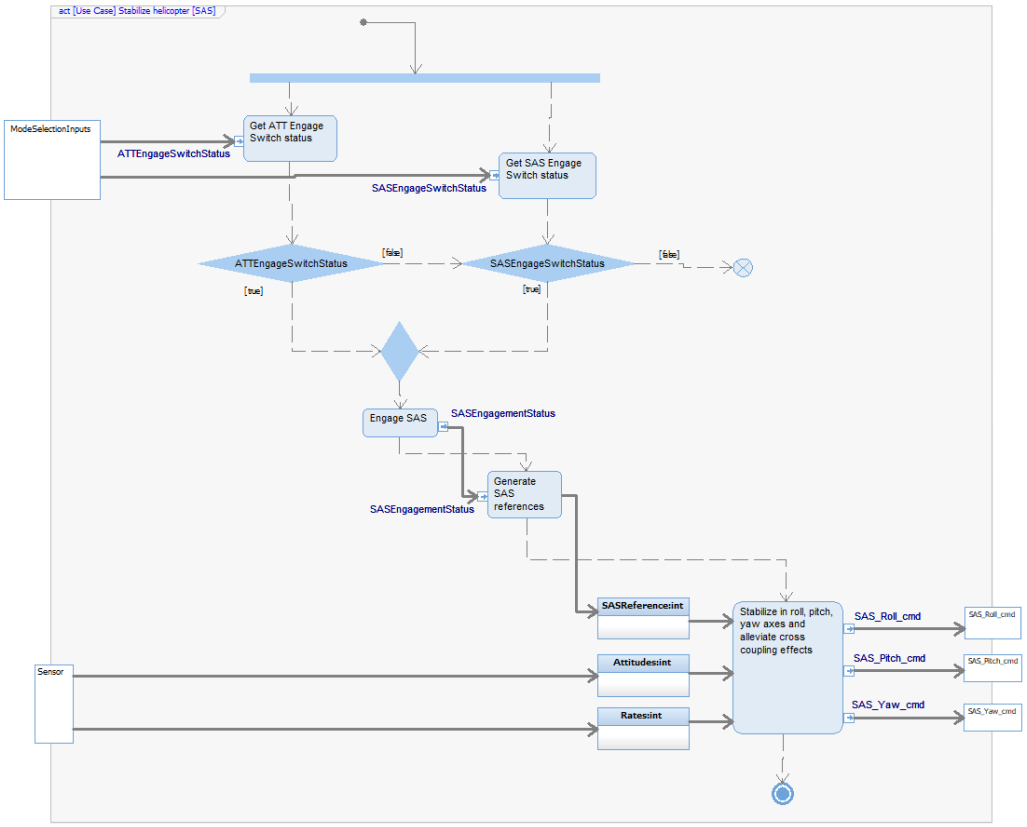


Figure 11. Activity Diagram example from case study

As a result of the creation of Activity Diagrams, the big picture of the behaviour of the helicopter automatic flight control system is revealed. The output of the functional analysis process is considered to be the creation of the functional architecture of the system and its definition of the functionality of the system. According to the ARP4754A document, the output of this process is defined as the determination of the scenarios and actions required for the realization of the use case of the system and the resulting functional requirements.[7]

Functional requirements define the functional infrastructure of the system, specify what the system will do in detail, express the necessary characteristics of the system and the constraints in the system solution. By obtaining functional requirements, the system requirements resulting from the requirement analysis are revised. Some of the functional requirements that are the output of the functional analysis process are as shown in Figure 12.

ID	Automatic Flight Control System requirements	Object Type
AFCS_18	SAS Engage Switch shall be a manual ON/OFF switch to establish engagement of SA Functions.	Functional Requirement
AFCS_348	The SAS Engage Switch shall remain its status when the Trim Release Button is pressed or released.	Functional Requirement
AFCS_251	The output commands of Autopilot Functions shall be summed separately for each principal control axis.	Functional Requirement
AFCS_70	Except where otherwise specified, a damping ratio of at least 0.3 critical shall be provided for nonstructural AFCF controlled mode responses. Specified damping requirements apply only to the response characteristics for perturbations an order of magnitude greater than the allowable residual oscillation.	Functional Requirement
AFCS_292	The Pitch SA Function shall limit the closed loop control pitch angle between ±15 deg with a tolerance of +10%.	Functional Requirement

Figure 12. Functional requirements example from case study on DOORS

3.3.3. System Architecture Design

The system architecture design process is the third phase of the Model-based systems engineering process. System architecture is defined as the conceptual model that defines the structure, behaviour and formality of the system.[8] In the system architecture design process, functional requirements are classified, a structural model component specific to each class is created, and functions are allocated to structural model components. Structural architectural and structural requirements obtain as a result of this process. While performing the system architecture design process in the case study, the path as follows:

- Defining basic system functions
- Classification of functions and creation of functional architecture
- Creation of structural components from functional architecture
- Allocation of system level operations to structural model components as shown in Figure
- Creation of structural architecture
- Obtaining structural requirements

The system architecture design process focuses on the development of a structural architecture that can perform the necessary functions within the limits of the estimated performance constraints. Structural models created in the system architecture design process,

- show which parts of the system will consist,
- show what the relationships between the parts will be,
- define the details / features of the internal structure of the parts,
- create the structural architecture of the system in a hierarchically.

Block Definition Diagram and Internal Block Diagram are created with SysML to define a structural architecture. In this case study, the structural architecture of the system was created hierarchically with different Block Definition Diagrams. Within the scope of this article, the design of the “SAS” system architecture was handled step by step by taking the "Stabilized helicopter" use case and the "SAS Activity Diagram" created during the functional analysis process.

Block	Allocation	Action
SAFunction	SAFunction	generateSASCmd
SASEngagement	SASEngagement	engageSAS
SASEngagement	SASEngagement	getSASEngageSwitchStatus
SASEngageSwitch	SASEngageSwitch	getSASEngageSwitchStatus
SASEngageSwitch	SASEngageSwitch	checkSASEngageSwitchStatus
SASReference	SASReference	generateSASReferences

Figure 13. Block and action allocation table

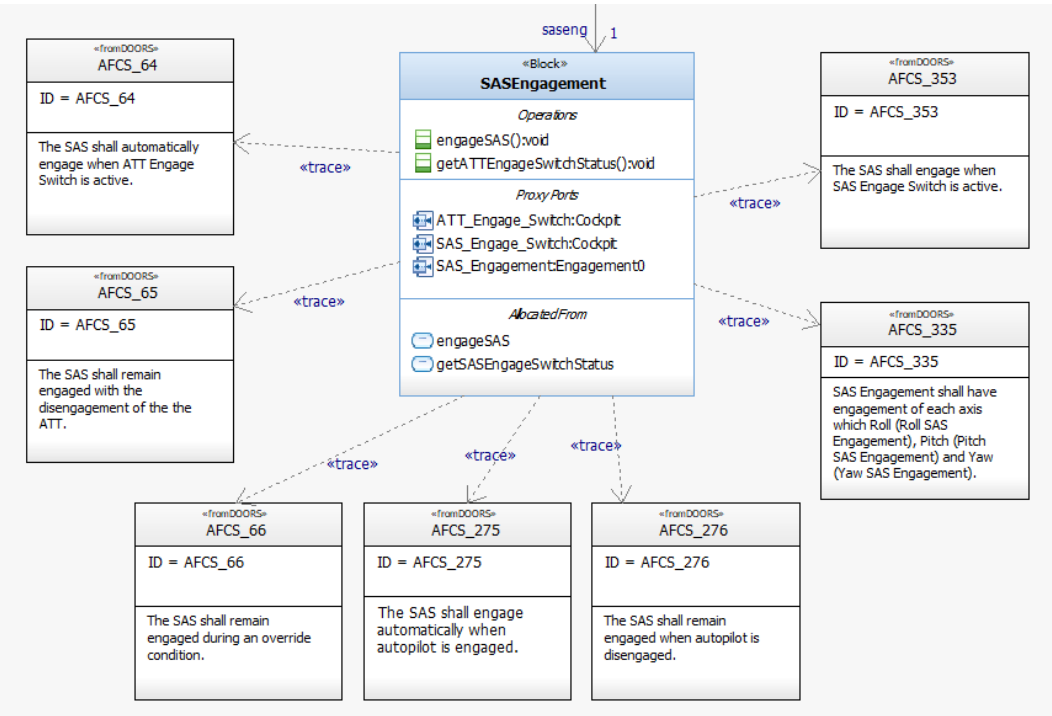


Figure 14. SAS Block definition diagram

It provides a visual representation to manage architectural system complexity and create a communication and coordination mechanism between components. The output of the system architecture process is conceptual models that define the structure, behaviour and formality of the system. These models are designed with Block Definition Diagrams. As a result of the creation of Block Definition Diagrams, the structural architecture and structural requirements of the helicopter automatic flight control system were revealed. With the obtain of structural requirements, the system requirements that obtained as a result of the needs analysis were revised.

Some of the structural requirements that are the output of the system architecture design process are as shown in Figure 15.

ID	Automatic Flight Control System requirements	Object Type
AFCS_2	AFCS shall consist of Cockpit Control Inputs, Flight Control Computer and Sensors models.	Structural Requirement
AFCS_6	Cockpit Control Inputs shall consist of Flight Control Inputs and Mode Selection Inputs.	Structural Requirement
AFCS_14	Mode Selection Inputs shall consist of switches/buttons (etc.) for each autopilot modes engagement.	Structural Requirement
AFCS_33	FCC shall provides helicopter flight control system that includes Autopilot Functions and Autopilot Logics.	Structural Requirement
AFCS_37	Autopilot Functions shall have Stability Augmentation (SA), Attitude Hold (ATT), Roll Heading Hold, Side Slip Functions.	Structural Requirement
AFCS_34	FCC shall have short term pitch, short term roll and short term yaw stability augmentation (SA) in all flight regimes.	Structural Requirement
AFCS_335	SAS Engagement shall have engagement of each axis which Roll (Roll SAS Engagement), Pitch (Pitch SAS Engagement) and Yaw (Yaw SAS Engagement).	Structural Requirement

Figure 15. Structural requirements example from case study on DOORS

3.3.4. Detailed System Architecture Design

The final stage of the process of Model-based systems engineering is the detailing of the system architecture. The detailing of the system architecture aims to explain in which order the structural architectural components of the system operate in accordance with the scenarios and to show the communication between the components. The system architecture developed using SysML is detailed with Sequence Diagrams. The process of obtaining Sequence Diagram in SysML is as shown in Figure 16. [9]

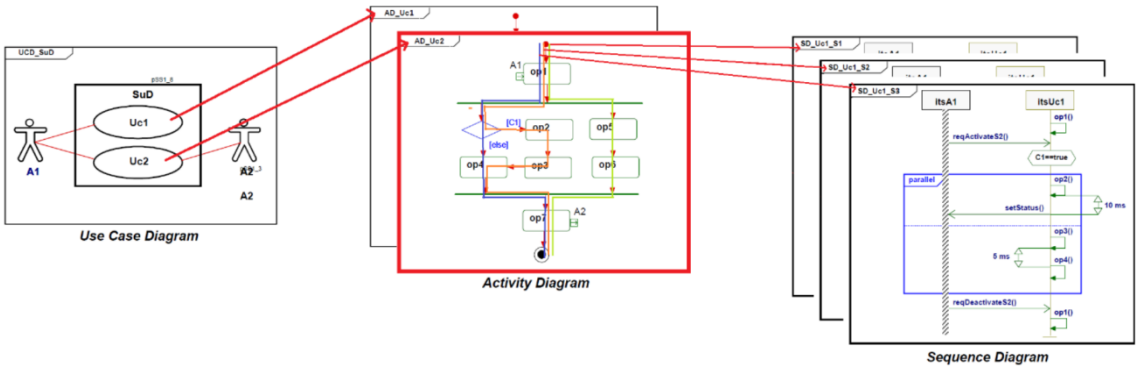


Figure 16. Process of the obtaining Sequence Diagram

When creating Sequence Diagram, a scenario is selected firstly from Activity diagram. The blocks in which the actions that are active in the selected scenario are allocated are added to the Sequence Diagram as a "lifeline" model component. Communication between the "Lifeline" model components is provided by messages. The detailing process of the system architecture was carried out in all the Activity Diagrams that the output of the system functional analysis in the case study. As an example of the system architecture detailing process, the helicopter automatic flight control subsystem “SAS” is detailed with the Sequence Diagram as shown in Figure 17.

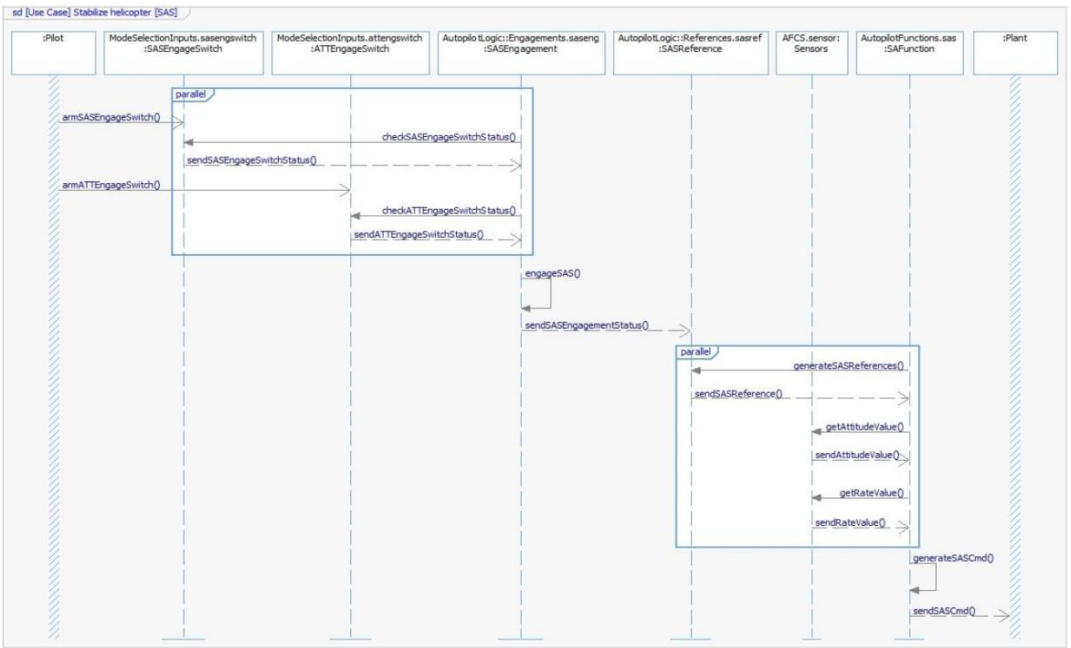


Figure 17. Sequence Diagram example from case study

During the system detailing process, the messages transmitted between the blocks in Sequence Diagrams are examined and the interfaces of the subsystems are created. The interfaces are shown in Internal Block Diagrams in SysML. The interface has been defined for all blocks created in the system. The helicopter and AFCS system interface to be used in the design is shown in Figure 18.

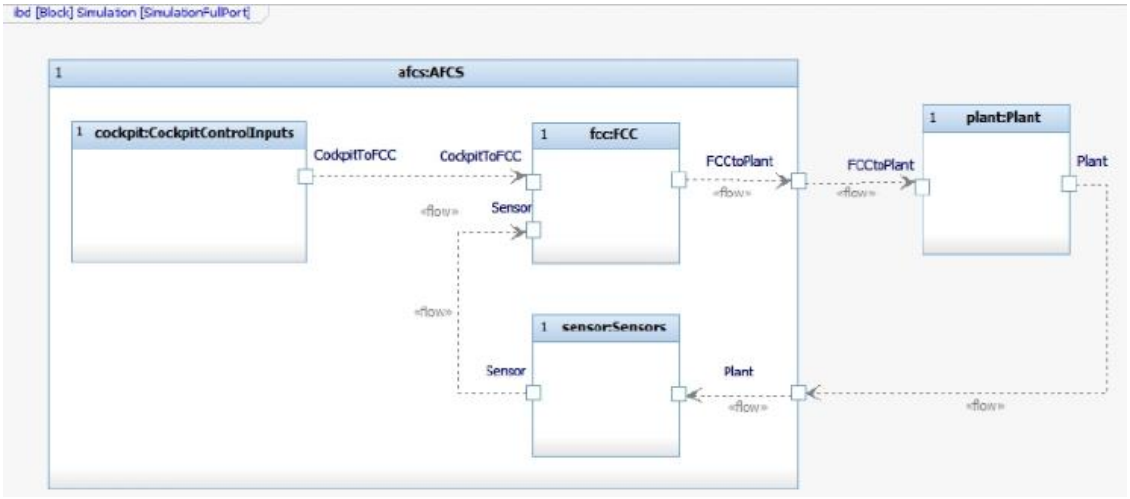


Figure 18. Internal Block Diagram example from case study

Interface blocks of helicopter automatic flight control system is shown Figure 19.

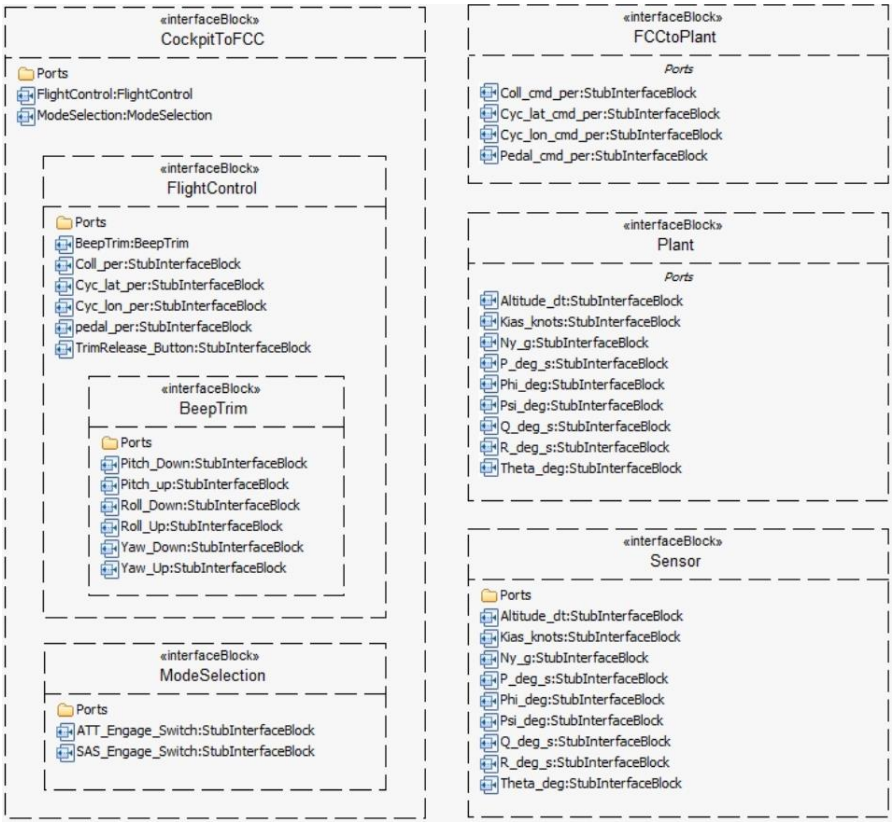


Figure 19. Interface block of AFCS case study

4. CONCLUSION

The model-based systems engineering process covers the requirements and system architecture stages of model-based design processes. Accordingly, requirements management, system architecture management and model-based systems engineering design processes have been developed.

Within the scope of the requirements management study, the requirements were defined in the DOORS software, a checklist was created for the validation of the requirements, the requirement was traceable, the requirement validation methods were defined, and the transfer methods were developed to use the requirements in different software.

Within the scope of the system architecture management study, the model organization for the helicopter automatic flight control system was realized in IBM Rational Rhapsody software with using SysML.

The following were found in the model-based systems engineering design processes.

- As a first stage the requirement analysis study, use case were revealed by reference to the customer requirements and the requirements were associated with the use cases.
- As a second stage the system functional analysis study, functional requirements of the system were revealed by developing functional architecture and functional models.
- Within the scope of the system architecture design study, structural requirements of the system were revealed by developing structural architecture and structural models.
- Within the scope of the detailed system architecture design study, the system's operating scenarios and system interfaces have been created.

With the model-based systems engineering approach and application of this study, a solution was found to the main problems of traditional system engineering. Model-based systems engineering approach is more systematic than traditional systems engineering but requires more preparation before implementation. As a result, a case study has shown that it is a more efficient design process for management and traceability.

5. FUTURE WORKS & LIMITATION

Similar to the work done in this article in the future, it can be applied in all aircraft design processes. More detailed testing and verification can be done using an advanced simulation infrastructure program. Traceability can be achieved by providing integration between programs where designs in different disciplines are realized and systems engineering designs.

As a limitation of the study, according to the methodology applied in this study, the requirements and system architecture stages of the model-based design stages are carried out for the automatic flight control system.

ACKNOWLEDGMENT

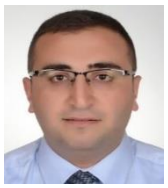
The material is based upon work supported by Turkish Aerospace Modelling and Simulation department. The authors would like to thank modelling and simulation co-workers for them supports.

REFERENCES

[1] INCOSE, Systems Engineering Handbook, INCOSE, 2004.
[2] S. Team, Systems Engineering Manual, FAA, 2014.
[3] Incose, Systems Engineering Vision 2020, Incose, 2007.
[4] Karagoz, Esma & Reilley, Kevin & Mavris, Dimitri. (2019). Model-Based Approach to the Requirements Analysis for a Conceptual Aircraft Sizing and Synthesis Problem. 10.2514/6.2019-0498.
[5] S. Friedenthal, A. Moore, and R. Steiner.OMG Systems Modelling Language Tutorial, 2009.
[6] IBM, "IBM Knowladge Center," IBM, [Online]. Available: https://www.ibm.com/support/knowledgecenter/SSB2MU_8.3.0/com.ibm.rhp.sysml.doc/topics/rhp_c_functional_analysis.html. [Accessed 5 September 2020].
[7] SAE, "ARP4754 - Guidelines for Development of Civil Aircraft and Systems," SAE, 2010.
[8] S. P. J. Holt, SysML for Systems Engineering 2nd Edition, 2013.
[9] H. Hoffmann, System Engineering Best Practices with the Rational Solution for Systems and Software Engineering, IBM, 2009.

AUTHORS

Haluk Altay



He is a graduate of Yıldız Technical University Mechatronics Engineering addition a student of M.Sc Istanbul Technical Universty Mechatronics Engineering. He has been involved in academic research for the past two years and worked several projects for the past three on modelling, flight mechanics and controls. He has experienced in Model Based Systems Engineering, Flight Mechanics and Dynamics, Aircraft Design, System Identification at Turkish Aerospace.

Muhammed Furkan Solmazgül

Furkan Solmazgül has been involved in model-based systems engineering projects since 2018. He is currently working as a design engineer at Turkish Aerospace. He graduated from Istanbul Commerce University in Mechatronics Engineering.

SECURE PROTOCOL FOR FOUR D2D SCENARIOS

Hoda Nematy

[1]Malek-Ashtar University of Technology, Shabanlou,
Babaee Hwy, Lavizan, Tehran, Iran.

ABSTRACT

In traditional cellular infrastructure, cellular devices communicate with each other directly even when they are close together. This strategy causes massive traffic to the cellular network therefore D2D communication has introduced to overcome this issue, bring more bandwidth and also higher rates to the cellular network. One of the major challenges for D2D Communication is to have one single secure protocol that can adapt in four D2D scenarios defined in references. These scenarios are Direct D2D and relaying D2D communication with and without cellular infrastructure. In this paper, we propose a Secure D2D protocol based on ARIADNE with TESLA. Also we use LTE-A AKA protocol for authentication and key agreement procedure between Source and Destination. Next, we adapt this scenario to be applicable in without cellular infrastructure ones. This protocol could be used in direct D2D also. Based on the results, our proposed protocol has a few computation overhead compare to recent works and have less communication overhead than SODE with preserve many security properties such as Authentication, Authorization, Confidentiality, Integrity, Secure Key Agreement, Secure Routing Transmission…. We check Authentication, Confidentiality, Reachability and Secure Key Agreement of the proposed protocol with ProVerif verification tools.

KEYWORDS

5th generation, Four D2D scenarios, LTE-A AKA protocol, secure D2D protocol, ProVerif.

1. INTRODUCTION

D2D is a new form of communication for reducing cellular traffic and increasing the efficiency of the cellular network. This form of communication has introduced for 4th cellular communication and certainly has a big role in the 5th generation. D2D communication is a technique for direct transmission between a Source and a Destination. This technique provides a few interactions between cellular phones and the central nodes (i.e. eNodeB). The aim of D2D communication is to use D2D for close distances and use cellular communication only for far enough distances [1]. D2D First used in [2] for data transmissions between nodes. Some other researches [1]–[3] use D2D for cellular communication. Based on recent researches security is an open problem in D2D communication [4].There are several security challenges for D2D communication including Authentication, Authorization, confidentiality, integrity… and a secure protocol has to address them. Our proposed protocols use ARIADNE with TESLA [5] and LTE-A key distribution system. It designed for all four communication scenarios. Four D2D scenarios including, Direct D2D with cellular infrastructure, Direct D2D without cellular infrastructure, relaying D2D with cellular infrastructure and relaying D2D without cellular infrastructure show in Figure 1. It has also been transmitted a message in the network opportunistically by adding the encrypted message to the routing packet, this is for the mobile nature of D2D devices. When users are mobile in D2D communication, they may change their location after each routing process and no

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 21-33, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111102

longer participate in sending and receiving messages, therefore the routing procedure needs to be done again. But in our proposed protocol, by adding the encrypted message field to the routing package, no need to redo the routing operation and users have to participate in D2D as long as sending and receiving one packet process time.

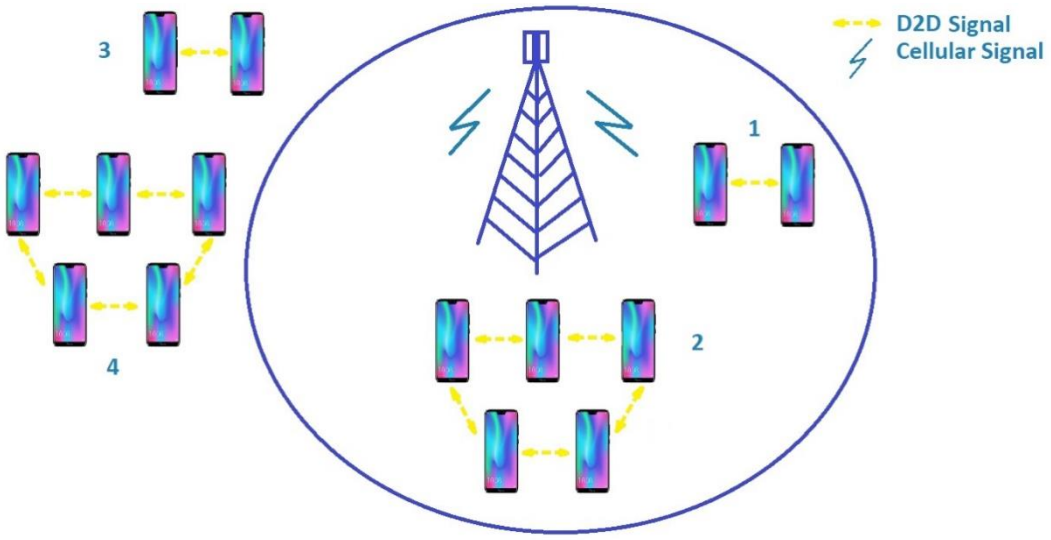


Figure 1. Four D2D Scenarios

The cellular networks may become out of reach in natural disasters, terrorist attacks, … In this scenario (out of coverage) the proposed protocol can override the network key agreement mode and use pre-shared keys. The other two ways that may be used for key agreement procedures are using the PUF circuiton D2D devices or using the Diffie-Hellman key agreement protocol. The rest of the paper is as follows. The related works come in section 2. Four D2D secure protocols with details and schematic will come in section 3 including Direct D2D Secure Protocol(DD2D), Relaying D2D Secure Protocol(RD2D), Direct D2D Secure Protocol without Cellular Infrastructure (DD2DW), and Relaying D2D Secure Protocol without Cellular Infrastructure (RD2DW). In section 4 the secure protocols will be analysed in three ways, Computation overhead, communication overhead, and security properties. In the former section, the security properties of secure protocols will discuss and the properties of Confidentiality, Reliability, one-way and two-way Authentication and Secure Key Agreement in two phases will proof with the ProVerif formal verification tool. In section 5 limitation and future works will present. Finally, the conclusion of the paper will present.

2. RELATED WORKS

The problem situation in [6] is based on a scenario in which one user covered by deactivated eNodeB wants to connect to the cellular network. In this scenario, a user in healthy eNodeB helps for communication and sharing secret keys. In this protocol two cryptic fields for each user have to be sent from each eNodeB to neighbour eNodeBs before the incident happens and every eNodeB should send these fields, to its users. In this protocol, so many communication overheads exist, because there is no information about which user may request communication and which user from the healthy network would respond to this request. Moreover, a user of healthy eNodeB may fall in the DOS attack by receiving too many requests from a malicious user. T. Ballan et al [9] use a Physically Unclonable Functions (PUF) to generate the secret key for each device. This circuit generates a unique value based on the unique character of each D2D devices, then use this unique value with the public key of another device and Elliptic Curve Cryptography to generate a

shared secret key. This sharing key is used as an input value of the Salsa20 / 20 stream cryptographic function and create a final message with the XOR operation of Salsa20/20 output and initial message. This method is prone to man-in-the-middle attacks when the attacker placed betwe en the receiver and the transmitter and sends his public key to the parties. Also, this method requires a PUF circuit that exists in both devices. L. Wang et al [10] present a distributed group key sharing scenario based on computational Diffie-Hellman (CDH) key sharing protocol in the absence of cellular infrastructure. This protocol does not provide a security solution based on the presence of an attacker within the network. Each time a user adds or eliminates from the group, a new session key should be created. P. Gope protocol [7] verifies the identity of D2D devices inside the network coverage by a middle layer called the fog layer. This middle layer connects to the core network and can authentication a device and also share a secret key with it. In another hand, the device can also verify the information received by the fog layer without disclosing its identity information to this layer. This method has been suggested to reduce the latency and to increase the mobility of end-users and could be used when a user is out of network coverage. A secure key exchange method between two D2D devices without network interference proposed in [8]. This protocol requires physical proximity of two devices before communication and for any communication physical proximity requires. In the case of reusing a key, the security of communication will be severely compromised. It is also possible to reveal the key if one of the devices is infected with malware. In [11] a secure protocol for secure communication between eNodeB and GW proposed. A summary of the security solutions of references shows in table 1.

Table 1. Security solutions in D2D communication

	Authentication	**Authorization**	**Confidentiality**	**Integrity**	**Secure routing transmission**	**Secure key agreement**	**Non-repudiation**
SOD [6]	-	-	+	-	+	+	-
LAAP [7]	+	+	-	-	-	+	+
Sec-D2D [8]	+	-	+	+	-	+	-
SDR [9]	-	-	+	-	-	+	-
CRA[10]	-	-	+	+	+	+	-

3. FOUR SECURE PROTOCOLS

We have four different protocols but the basis is the same. A Source wants to start a D2D communication to the Destination. In scenarios number 1 and 2, the Source and Destination are in each others neighboring and could receive information directly. But, in scenarios 3 and 4, the Source and Destination are not in each other neighbourhood and need the cooperation of other devices to transmit and receive information. In scenarios 1 and 3, all the devices including Source and Destination are in the cellular coverage therefore, we use the cellular advantage to distribute keys. However, for the intermediate nodes (i.e. relays), we use the TESLA broadcast authentication protocol for lessening cellular signalling traffic. In these scenarios, the Source which wants to establish a D2D communication to a specified destination sends a D2D request

including Source and Destination identity in a secure cellular channel to the MME. MME checks the validity of the message and authenticate the Source and Destination, and also checks if the destination is in the proximity of the Source or not. If all the situations above meet, MME builds a D2D session key and sends it to the Source in a secure cellular channel. Then the Source starts D2D communication towards Destination.

In ARIADNE, the packaging field includes S, D, id, and t. for Source, Destination, the ID of the message and time respectively. In this protocol, we also add the encrypted message along with the nonce. Furthermore, we use one key for evaluation of MACs instead of using two keys because the Source and destination have each other keys and one key is enough. We use the key chain TESLA protocol for intermediate users and assume that there is a system in the network where the initial values of the user's key chain are broadcast to the entire network, so every cellular device can authenticate received TESLA key. when users are in the coverage of the cellular network, this can be done by cellular network control messages. In the absence of cellular network coverage, we assume that users use the previous initial values when the cellular network was available. Our protocol in four scenarios is as follows.

3.1. Direct D2D Secure Protocol (DD2D)

In this protocol, two D2D devices are in each other vicinity and Source initiates a D2D communication by requesting the core network (MME) to establish a D2D. The pseudo code of the DD2D protocol is in pseudo code 1.Parameters used in pseudo code describes in table 2.

Pseudo code 1. Direct D2D (DD2D) Protocol

```
Start
Source:       Sends message (Request, IMSI, S, D) to MME in cellular channel
MME:          Authenticates Source and Destination
              If S & D is valid
                    If D is close enough to S
                          K= New key
                          Add [S , D] to D2D list
                          Sends K to Source
                    End if
              End if
Source:       N= New Nonce
              K'=Enc_K(N)
              C=Enc_K(m)
              H_0=MAC_K(Request, C, N, S, D, id, t)
              Source sends message (Request, C, N, S, D, id, t, H_0) to Destination in D2D channel
Destination:  If id is unique & t>=t_exp
                    Destination sends message (Request, IMSI, S, D) to MME in cellular channel
              End if
MME:          Authenticates Source and Destination
              If S & D is valid
                    If [S , D] are in D2D list
                          Sends K to Destination
                    End if
              End if
Destination:  H'_0= MAC_K(Request, C, N, S, D, id, t)
              If H'_0=H_0
                    K'= EncK(N)
                    m=Enc_K'(C)
                    M_D= MAC_K(Reply, S, D, t)
                    Destination sends message (Reply, S, D, t, M_D) to Source in D2D channel
              End if
End
```

Table 2: Parameter description

Parameter	Description
K	Secure D2D session key
$MAC_K(M)$	Message Authentication Code with the message (M) and the key (K)
$H_n()$	n^{th} Hash function in the series
$Enc_K()$	Symmetric Encryption with key K
$Dec_K()$	Symmetric Decryption with key K

3.2. Relaying D2D Secure Protocol (RD2D)

This protocol starts like DD2D by requesting a MME to establish a D2D communication from the Source. But in this scenario, the Source and the Destination are not in each others neighboring and relaying nodes should participate to transfer information. The pseudo code of the RD2D protocol is in pseudo code 2.

Pseudo code 2. Relaying D2D (RD2D) Protocol

```
Start
Source:          Sends message (Request, IMSI, S, D) to MME in cellular channel
MME:             Authenticates Source and Destination
                 If S & D is valid
                     If D is close enough to S
                         K= New key
                         Add [S , D] to D2D list
                         Send K to Source
                     End if
                 End if
Source :         N= New Nonce
                 K'=EncK(N)
                C=EncK'(m)
                H0=MAC_K(Request, C, N, S, D, id, t)
                Source sends message (Request, C, N, S, D, id, t, H0) towards Destination in D2D channel
A:               If id is unique & t>=t_exp
                     H_1=H(A, H_0)
                     M_A= MAC_KA1(Request, C, N, S, D, id, t, H_1, A)
                     A sends message (Request, C, N, S, D, id, t, H_1, A, M_A) towards Destination in D2D channel
                 End if
B:               If id is unique & t>=t_exp
                     H_2=H(B, H_1)
                     M_B= MAC_KB1(Request, C, N, S, D, id, t, H_2, A, B, M_A)
                     B sends message (Request, C, N, S, D, id, t, H_2, A, B, M_A, M_B) towards Destination in D2D channel
                 End if
C:               If id is unique & t>=t_exp
                     H_3=H(C, H_2)
                     M_C= MAC_KC1(Request, C, N, S, D, id, t, H_3, A, B, C, M_A, M_B)
                     C sends message (Request, C, N, S, D, id, t, H_2, A, B, M_A, M_B, M_C) towards Destination in D2D channel
                 End if
Destination:     If id is unique & t>=t_exp
                     Destination sends message (Request, IMSI, S, D) to MME in cellular channel
                 End if
MME:             Authenticates Source and Destination
                 If S & D is valid
                     If [S , D] are in D2D list
                         Send K to Destination
                     End if
                 End if
Destination:     H'_3=H(C, H(B, H(A, MAC_K(Request, C, N, S, D, id, t))))
                 If H'_3=H_3
                     K'= Enc_K(N)
                     m=Enc_K'(C)
                     M_D= MAC_K(Reply, S, D, t, A, B, C, M_A, M_B, M_C )
                     Destination sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D) towards Source in D2D channel
                 End if
C:               C adds KCt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt) towards Source in D2D channel
B:               B adds KBt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt, KBt) towards Source in D2D channel
A:               A adds KAt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt, KBt, KAt) towards Source in D2D Channel

end
```

3.3. Direct D2D Secure Protocol without Cellular Infrastructure (DD2DW)

This protocol is similar to the DD2D Protocol. However, cellular infrastructure does not exist in this protocol. To preserve confidentiality property, both Source and Destination have to use a key that sets before communication. We suppose each device already exchanged the key in a way such as key agreement procedures in [9], [10]. In the disaster situation, we suppose losing confidentiality is less important than losing vital communication. Moreover, in the situation that each if no other pre-distribution keys exist and no other procedures could be used devices can use their TESLA key. In this scenario the Destination could not validate the H_0 value before receiving the TESLA key of the source, but it can decrypt the message. So, in the case of emergency situation its better to first decrypt the package and if the TESLA key arrives and the package fails to validate then the Destination withdraws the packet. The protocol pseudo code is in the pseudo code 3.

Pseudo code 3. Direct D2D Protocol Without Cellular Infrastructure (DD2DW)

```
Start
Source:        C=Enc_K(m)
               H_0=MAC_K(Request, C, N, S, D, id, t)
               Source sends message (Request, C, N, S, D, id, t, H_0) to
               Destination in D2D channel
Destination:   If id is unique & t>=t_exp
                   H'_0= MAC_K(Request, C, N, S, D, id, t)
                   If H'_0=H_0
                       m=Enc_K(C)
                       M_D= MAC_K(Reply, S, D, t)
                       Destination sends message (Reply, S, D, t, M_D) to
                       Source in D2D channel
                   End if
               End if
End
```

3.4. Relaying D2D Secure Protocol without Cellular Infrastructure (RD2DW)

This protocol is a combination of RD2D and DD2DW, the Source and Destination are not in each other's vicinity so relaying nodes should participate in communication and also the cellular infrastructure is not available. We suppose Source and Destination already exchanged keys in a way such as explained in DD2DW. The protocol pseudo code is in pseudo code 4.

Pseudo code 4. Relaying D2D Secure Protocol without Cellular Infrastructure (RD2DW)

Start
Source: $C=Enc_K$ (m)
$H0=MAC_K$(Request, C, N, S, D, id, t)
Source sends message (Request, C, N, S, D, id, t, H0) towards Destination in D2D channel
A: If id is unique & $t>=t_{exp}$
$H_1=H(A, H_0)$
$M_A= MAC_{KAt}$(Request, C, N, S, D, id, t, H_1, A)
A sends message (Request, C, N, S, D, id, t, H_1, A, M_A) towards Destination in D2D channel
End if
B: If id is unique & $t>=t_{exp}$
$H_2=H(B, H_1)$
$M_B= MAC_{KBt}$(Request, C, N, S, D, id, t, H_2, A, B, M_A)
B sends message (Request, C, N, S, D, id, t, H_2, A, B, M_A, M_B) towards Destination in D2D channel
End if
C: If id is unique & $t>=t_{exp}$
$H_3=H(C, H_2)$
$M_C= MAC_{KCt}$(Request, C, N, S, D, id, t, H_3, A, B, C, M_A, M_B)
C sends message (Request, C, N, S, D, id, t, H_2, A, B, M_A, M_B, M_C) towards Destination in D2D channel
End if
Destination: If id is unique & $t>=t_{exp}$
$H'_3=H(C, H(B, H(A, MAC_K$(Request, C, N, S, D, id, t))))
If $H'_3=H_3$
$m=Enc_K(C)$
$M_D= MAC_K$(Reply, S, D, t, A, B, C, M_A, M_B, M_C)
Destination sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D) towards Source in D2D channel
End if
End if
C: C adds KCt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt) towards Source in D2D channel
B: B adds KBt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt, KBt) towards Source in D2D channel
A: A adds KAt and sends message (Reply, S, D, t, A, B, C, M_A, M_B, M_C M_D, KCt, KBt, KAt) towards Source in D2D Channel

end

4. ANALYSIS OF THE PROPOSED PROTOCOLS

The amount of operations based on the role and the packet size of each node is in table 3. In this table Enc is for encryption, Dec is for decryption, H is for hash value, Ks is for key size, and n is for the number of nodes including Source and Destination. We assume symmetric encryption with the output of 256 bits and also a hash function with the size of 256 bits, 4 bits for request, ti, I, N and 8 bits for Source and Destination identities. Based on the number of nodes participating in D2D, the replay packet will have a different size. If we assume the maximum number of nodes is 20, the maximum packet size of Destination in the replay packet is 629 bytes and also the maximum packet size of intermediate nodes in request and replay packet respectively are 662 bytes and 629ks bytes.

Table 2: Operations and packet size in proposed protocols

Device	**operations**	**Packet size**
The source in direct D2D	Enc+H	544 bit
The source in relaying D2D	2Enc+H	544 bit
Destination in direct D2D	Dec+H	286 bit
Destination in relaying D2D	Enc+Dec+nH	28+(n-2)8+(n-1)256 bit
Intermediate node in the request	2H	28+(n-1)8+n256 bit
Intermediate node in the reply	-	12+8n+(n-1)256+(n-2)Ks

4.1. Computation Overhead

In the proposed protocols, we use a symmetric function for encryption and decryption of the message and one for the key evaluation parts. Also we use a cryptographic hash function for each transmission. So, there are two symmetric encryptions/decryptions, one cryptographic hash function evaluation for source and destination, and one cryptographic hash function evaluation for each relaying device. The computation cost comes in table 4 describes the proposed protocol compared to other protocols. Enc and Dec are for Encryption and Decryption, n is for the number of devices, H is a hash function, Mul is for multiplication, EO is for exponential operation, PA is for pairing, Div is for division and PO is for point multiplication.

Table 3: Computation cost of protocols

protocol	Computation cost
SDGA [12]	$3(2n-1)PA + 5nEO + (4n-1)H + 2(2n-1)Mul$
PPAKA [13]	$2(2n-1)EO + (n^2+3n-4)H + (2n^2-3n+1)Mul$
GRAAD [14]	$2nPA + 7(3n-2)H + nEnc + nDec + 3(n-1)PO + 8(n-1)EO + 2(n-1)Mul$
LRSA [15]	$6nPO + (13n-7)H + (3n-1)Mul + 2Div$
SeDS [16]	$2PA + (5n-2)EO + Dec + (2n+1)H + 4(n-1)\ PO + 2(n-1)Enc$
DD2D	$3Enc + 3H + Dec$
RD2D	$3Enc + (2n+1)H + Dec$
DD2DW	$Enc + 3H + Dec$
RD2DW	$Enc + (2n-1)H + Dec$

4.2. Communication Overhead

In RD2D and RD2DW, the protocol has 2n packet transmission for each relay device (one for Request and one for Reply). So, the communication overhead of the proposed protocol is as equation 1.

$$CommunicationOverhead = \frac{T' \times M \times (2n+2)}{T} \quad (1)$$

T' is the number of timeslots that D2D requests happen, T is the total number of timeslots, M is the number of D2D requests at each timeslot ,and n is the number of devices. We compare the communication cost of RD2D with SODE [6] because RD2D has the biggest communication overhead among the other three proposed protocols. In SODE, two cryptic fields for each device has to be sent from each eNodeBs to each eNodeB'sneighbours. Also, two cryptic fields for each neighbours have to be sent to all the devices belongs to eNodeB. Another communication parts in SODE are from D2D request and D2D reply. These two communication are for key agreement between two devices in the network. Communication overhead of RD2D and SODE based on increasing the number of time slots when the number of eNodeBs are 2 and 7 are in figures2 and 3 respectively. The communication overhead increases as the number of nodes (n) increased. When the number of eNodeBs increase to 7, the communication overhead of SODE increases for about 3 times, but in RD2D the number of eNodeBs has no effect on the communication overhead. In another comparison, we check the change of the number of T' in communication overhead when M=1 and M=5 in figures4 and 5 respectively. The communication overhead increases as T' increased and when M increases to 5 both protocols have more communication overhead. It means as the number of D2D requests increase the communication overhead

increases as well. In figure 4 and 5 RD2D has less communication overhead than SODE and the slob of SODE is much more than RD2D.

Table 4. Parameters used in communication overhead simulation

Parameter	value
n	10
T	20
T'	10
M	1 & 5

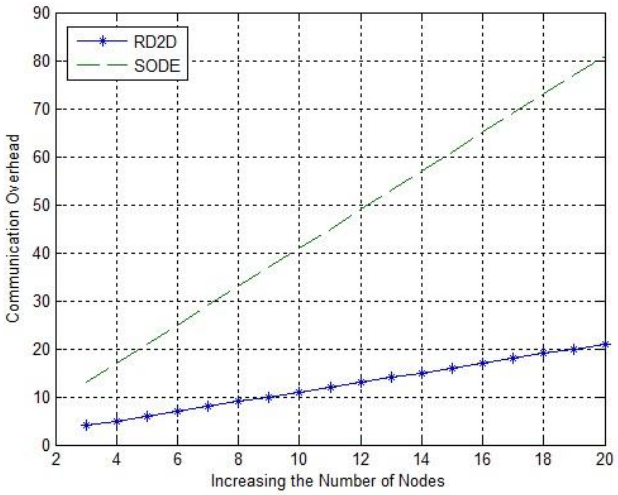


Figure 2. The Communication Overhead Vs the Number of Nodes when B=2

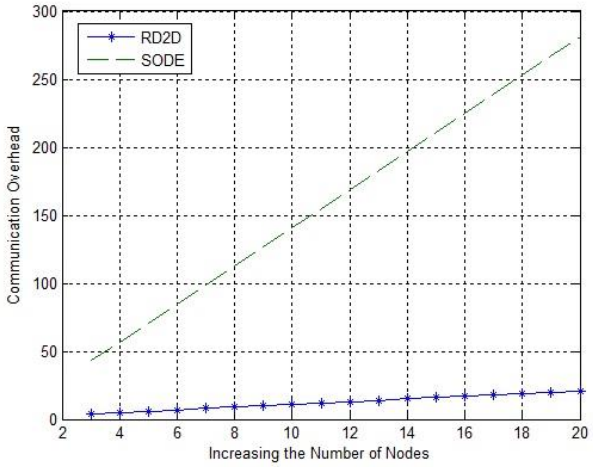


Figure 3. The Communication Overhead Vs the Number of Timeslots when B=7

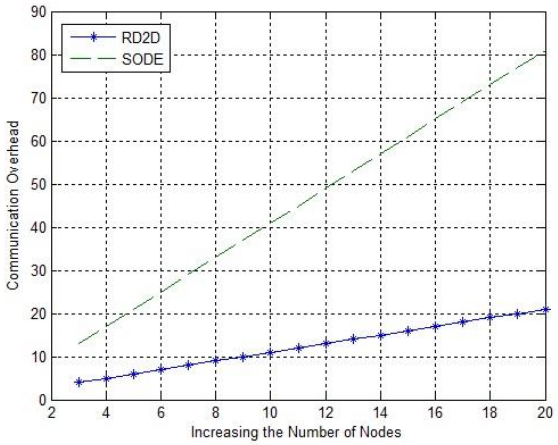


Figure 4. The Communication Overhead Vs the Number of Nodes when M=1

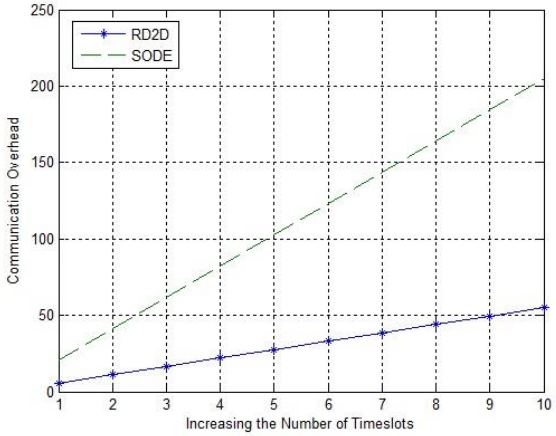


Figure 5. The Communication Overhead Vs the Number of Nodes when M=5

4.3. Security Properties of the Protocol

In this part, we show the security properties of our protocols. Our proposed protocols have Authentication, Authorization, Confidentiality, Integrity, Non-repudiation, Secure routing transmission, Secure key agreement, and reachability. We will show two more security properties Secure key agreement and reachability in the ProVerif Section and discuss the rest in this part.

1. Authentication and Authorization: This property is based on the cellular authentication and authorization process in cellular coverage scenarios (DD2D and RD2D). In two other scenarios (DD2DW and RD2DW), authentication and authorization are based on the privacy of secret keys on each side. If both sides (Source and Destination) could decrypt the packet and evaluate the message, it means both sides are authorized sides. For this assumption, we suppose that no one reveals the key and the key saved in both devices securely.
2. Confidentiality: this property is gained by the encryption and decryption of the message based on the secret key received from the MME. MME is the trusted server which would not reveal the key K to anybody but authorized Source and Destination. In DD2DW and RD2DW, the confidentiality of the message is based on the secrecy of the keys and key distribution system they used in the absence of cellular infrastructure.

3. Integrity: this property caught by the hash values. If the destination evaluates the hash chain values and they are different from what was inside the packet, it means the integrity of the packet losses and it should ignore the received packet. This property could be checked by the Source too, the field MD in reply packet does this part.
4. Non-repudiation: this property can be set by the packet id value in the request message which should be fresh. Also, t value should not be too far in the past.
5. Secure routing transmission: This property is only for RD2D and RD2DW because these two protocols have routing part. Our proposed protocols are based on ARIADNE protocol, it prevents tampering with the attackers or comprised nodes and it also resists to many Denial-of-Service attacks.

4.4. ProVerif Verification of RD2D Protocol

ProVerif is a formal tool for verifying cryptographic protocols [17]. Input language of ProVerif supports channels with the "Dolev-Yao" ability attacker. This attacker model is very strong and has full control over the channel. We use ProVerif for verifying confidentiality, reachability and secure key agreement of RD2D because it comprises three other protocols. Security properties that we use come in table 6.

Table 6. Security properties of the protocol used in ProVerif

Security Property		**ProVerif**
Confidentiality		query attacker(m).
Reachability		query event(mmeReachable()). query event(hssReachable()). query event(SourceReachable()). query event(DestinationReachable()).
Authentication	One-way authentication	event acceptsServerClientA(bitstring,key). event acceptsServerClientB(bitstring,key). event acceptsServerClientC(bitstring,key). event acceptsServerDestination(bitstring,key).
	One-to-one authentication*	event termDestination(bitstring,key).
Secure Key agreement	Running key	event SourceRunning(key). event mmeRunning(key). event DestinationRunning(key). event ClientARunning(bitstring,key). event ClientBRunning(bitstring,key). event ClientCRunning(bitstring,key).
	Key agreement	event SourceCommit(key). event mmeCommit(key). event DestinationCommit(key).

When one side of the communication checks authenticity it calls One-way authentication i.e. when Source authenticates relaying devices. However, in one-to-one authentication two sides of communication should authenticate each other i.e. Source and Destination. So we use one-to-one authentication for Source and Destination and one-way authentication for relaying devices. We check the Secure key agreement procedure in two phases, running key and key agreement. In the phase of running key, a device uses a key and in the phase of key agreement, the other device

agrees on the key used before. ProVerif verifies all the security properties of RD2D. Figure6, shows protocol verification in ProVerif.

ProVerif text output:

```
Starting query not event(SourceReachable)
goal reachable: end(SourceReachable)
RESULT not event(SourceReachable) is false.
Starting query not event(DestinationReachable)
goal reachable: end(DestinationReachable)
RESULT not event(DestinationReachable) is false.
-- Query event(SourceCommit(k_133)) ==> event(mmeRunning(k_133))
Completing...
200 rules inserted. The rule base contains 185 rules. 9 rules in the queue.
Starting query event(SourceCommit(k_133)) ==> event(mmeRunning(k_133))
goal reachable: begin(mmeRunning(kdf(n_128[imsi_127 = imsiS[!1 = @sid_35779],!1 = @sid_35780],k[!1 = @sid_35779]))) ->
end(SourceCommit(kdf(n_128[imsi_127 = imsiS[!1 = @sid_35779],!1 = @sid_35780],k[!1 = @sid_35779])))
RESULT event(SourceCommit(k_133)) ==> event(mmeRunning(k_133)) is true.
-- Query event(mmeCommit(k_134)) ==> event(SourceRunning(k_134))
Completing...
200 rules inserted. The rule base contains 185 rules. 9 rules in the queue.
Starting query event(mmeCommit(k_134)) ==> event(SourceRunning(k_134))
RESULT event(mmeCommit(k_134)) ==> event(SourceRunning(k_134)) is true.
-- Query inj-event(SourceCommit(k_135)) ==> inj-event(mmeRunning(k_135))
Completing...
```

Figure 6: ProVerif Verification of RD2D Protocol

5. LIMITATIONS AND FUTURE WORKS

There are a few researches in authentication and key agreement procedure in cellular networks and makes it hard to find resources. The problem of key distribution and key agreement procedure in disaster situations or terrorist attacks is still a challenge to be respond.

Using routing algorithms for finding intermediate nodes and combine the secure protocols and routing algorithms together would be a good improvement to this research. Moreover, a way of getting feedback from the D2D communications would be suggested in order to restrict malicious nodes and improve the communication quality. Finally, we suggest using a bonus method to increase the cooperation of intermediate nodes in the D2D communication.

6. CONCLUSIONS

We proposed four D2D secure protocols for four different scenarios (DD2D, RD2D, DD2DW, and RD2DW). This is the first time a protocol has the capability to adapt to four scenarios which are essential to D2D networks. These Protocols are based on ARIADNE with TESLA. We used LTE-A AKA protocol for Authentication and key agreement for the Source and Destination in RD2D and DD2D. Also, we used TESLA, broadcast authentication protocol, for key utilization in intermediate nodes. This protocol does not need pre-shared keys for these nodes. Based on the results, our proposed protocols have less computation overhead among recent works. RD2D has less communication overhead compare to SODE protocol and it has more communication overhead among three other proposed protocols, so the other proposed protocols have less communication overhead than SODE, too. Finally, we showed our protocol security features and proofs Confidentiality, Reachability, Authentication, Secure Key agreement with ProVerif formal verification tools. Our proposed protocols have Authentication and Authorization, Confidentiality, Integrity, Non-repudiation, Secure routing transmission, Reachability, and Secure Key agreement with low communication and computation overhead.

REFERENCES

[1] N. Kato, "On device-to-device (D2D) communication [Editor's note]," *IEEE Netw.*, vol. 30, no. 3, p. 2, 2016.

[2] Y.-D. Lin and Y.-C. Hsu, "Multihop cellular: A new architecture for wireless communications," in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, 2000, vol. 3, pp. 1273–1282.

[3] D. Wu, L. Zhou, Y. Cai, R. Q. Hu, and Y. Qian, "The role of mobility for D2D communications in LTE-Advanced networks: energy vs. bandwidth efficiency," *IEEE Wirel. Commun.*, vol. 21, no. 2, pp. 66–71, 2014.

[4] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Phys. Commun.*, vol. 18, pp. 64–84, 2016.

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wirel. networks*, vol. 11, no. 1–2, pp. 21–38, 2005.

[6] S. K. Tetarave and S. Tripathy, "Secure Opportunistic Data Exchange Using Smart Devices in 5G/LTE-A Networks," in *International Conference on Security & Privacy*, 2019, pp. 3–16.

[7] P. Gope, "LAAP: Lightweight Anonymous Authentication Protocol for D2D-Aided Fog Computing Paradigm," *Comput. Secur.*, 2019.

[8] M. Cao *et al.*, "Sec-D2D: A Secure and Lightweight D2D Communication System With Multiple Sensors," *IEEE Access*, vol. 7, pp. 33759–33770, 2019.

[9] T. Balan, A. Balan, and F. Sandu, "SDR Implementation of a D2D Security Cryptographic Mechanism," *IEEE Access*, vol. 7, pp. 38847–38855, 2019.

[10] L. Wang, Y. Tian, D. Zhang, and Y. Lu, "Constant-round authenticated and dynamic group key agreement protocol for D2D group communications," *Inf. Sci. (Ny).*, vol. 503, pp. 61–71, 2019.

[11] P. P. Tayade and P. Vijayakumar, "Enhancement of Security and Confidentiality for D2D Communication in LTE-Advanced Network Using Optimised Protocol," in *Wireless Communication Networks and Internet of Things*, Springer, 2019, pp. 131–139.

[12] H. Tan, Y. Song, S. Xuan, S. Pan, and I. Chung, "Secure D2D group authentication employing smartphone sensor behavior analysis," *Symmetry (Basel).*, vol. 11, no. 8, p. 969, 2019.

[13] M. Wang and Z. Yan, "Privacy-preserving authentication and key agreement protocols for D2D group communications," *IEEE Trans. Ind. Informatics*, vol. 14, no. 8, pp. 3637–3647, 2017.

[14] R.-H. Hsu, J. Lee, T. Q. S. Quek, and J.-C. Chen, "GRAAD: Group anonymous and accountable D2D communication in mobile networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 2, pp. 449–464, 2017.

[15] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 3, pp. 662–675, 2016.

[16] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, "SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2659–2672, 2015.

[17] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre, "ProVerif 2.00: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial," *Version from*, pp. 5–16, 2018.

AUTHORS

Hoda Nematy is an Electrical Engineer, having graduated from the Malek-Ashtar University of Technology with a M.S degree in Cryptography and Safe Communication. Currently, she is working as the R&D team manager in the Pars Pooya Control Binalood Co.

ENHANCING SECURITY IN INTERNET OF THINGS ENVIRONMENT BY DEVELOPING AN AUTHENTICATION MECHANISM USING COAP PROTOCOL

Samah Mohammed S ALhusayni and Wael Ali Alosaimi, Ph.D.

Taif University, Saudi Arabia

ABSTRACT

Internet of Things (IoT) has a huge attention recently due to its new emergence, benefits, and contribution to improving the quality of human lives. Securing IoT poses an open area of research, as it is the base of allowing people to use the technology and embrace this development in their daily activities. Authentication is one of the influencing security element of Information Assurance (IA), which includes confidentiality, integrity, and availability, non repudiation, and authentication. Therefore, there is a need to enhance security in the current authentication mechanisms. In this report, some of the authentication mechanisms proposed in recent years have been presented and reviewed. Specifically, the study focuses on enhancement of security in CoAP protocol due to its relevance to the characteristics of IoT devices and its need to enhance its security by using the symmetric key with biometric features in the authentication. This study will help in providing secure authentication technology for IoT data, device, and users.

KEYWORDS

Authentication , authorization, key agreement, anonymity, traceability, Security, Cybersecurity, Secure by Design, Next Generation Internet, Smart City, wireless sensor networks, 5G network, the Internet of Things, CoAP, symmetric key and biometric.

1. INTRODUCTION

This research introduces research background of authentication mechanism in Internet of Things (IoT). It explains the concept of IoT, and how networks and computers have evolved until IoT appeared and merged with blockchain and artificial intelligence, homes, cars, smart cities and more than that. An example of smart cities is the technical city of NEOM, which illustrates the Kingdom's role in adopting technical projects and its leadership in this field, which requires awareness of members are of the importance of this stage and their role in it.

1.1. Overview of IoTs

Internet of thing (IOT) means a network which joined many things via internet[3] which help to achieve the end users goals [4]. The Internet of Things is a combination of technologies that work to connect many things over wired and wireless networks which handle by people, machines, or both[3] These things are connected to a platform that is manage within certain rules, analyze, process and store data, detect security threats, respond to any thing[5]. The level of competency

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 35-54, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111103

is measured according to the level of achievement of the tasks[5]. IOT system will be good as it can true response in any alteration there[6, 7].

Communication technology has developed very greatly in this era, where it started with a device that is no longer used now such as the telegraph, then the phone, and then the computer appeared that created another world as it began to solve complex mathematical operations and codes and was very large in size[3].Then, it developed and shrunk its size and increased its speed then appear of the personal computer which serves business offices and people through word processing programs, tables, and the like, and then to laptops, tablets, and smart devices with various applications where the combination of the Internet and WWW is important of IoT[3].

Internet also developed little by little, so the Internet of things was formed, starting from small closed networks to integrating more than one network, due to the emergence of microcontrollers with low cost and complexity ,and adequate processing power, so appeared educational websites, videos, forums and blogs .The Internet of things was not limited to commercial projects and extended to the Internet of things to consumers, and companies contributed provided smart home tools such as Google Apple and Siemens. The Internet of things developed to Hundreds of platforms and thousands of applications appeared, including the industrial Internet of things to automate many industrial then IoT evolved from a large infrastructure to the Next Generation Internet (NGI) that integrates with Internet systems for things such as augmented and virtual reality, machine learning, artificial intelligence, and blockchain to obtain professional tools[3]. The Internet and advanced wireless networks have a significant role to play in the widespread use of mobile devices that play a major role in consumer access and power over the different devices and services of the Internet of Things across Wi-Fi networks and mobile networks[8]. Such as fifth generation networks that are an active choice for IoT implementations like smart house, smart cities , smart healthcare, smart grids, etc.[9]. such as the city of Neom in Saudi Arabia, which depends on artificial intelligence and provides development and investment solutions to become a famed center in the region and there is a great trend for other smart cities and most services have been automated to become electronic. This was an example in a country as well as many countries, which means many users and applications and big data.

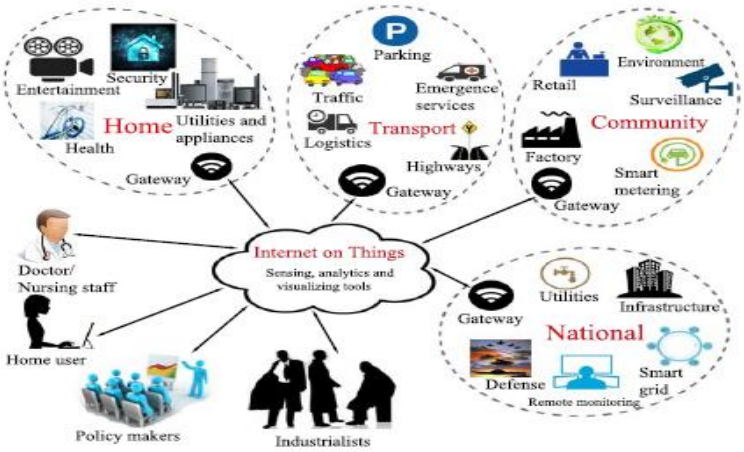


Figure1. IoT network architecture[1]

The above figure represents a summary of the structure of the network in IoT which has many applications transportation, smart homes and cities, community and industrial services, as well as

multiple users enter the system via the Internet through a portal in which the user is authenticated, which is the first stage and an essential part of the safety of the Internet of things.

Thus, within this development and the large number of users, it has become a target for adversary and owners of illegal targets and hackers, which required states and decision-makers to put in place laws and legislation that protect everyone and deter everyone who takes an irregular way to achieve his goals. Among the scholars and researchers are preparing studies for various possible security attacks, gaps that are a pathway to them, motives and points related to the subject, and providing security solutions that keep pace with this development and help in raising the level of security, responding to attacks, overcoming problems, and recovery.

1.2. Overview of IoTs

The spread of Internet of things networks in different milieus and for various purposes represents a security challenge that requires securing networks from any attack. IoT-linked protection problems are becoming more and more concerning due to the ubiquity of IoT and use at sensitive implementation, where intensify the effects at every security breaches to the degree that they are life-threatening [10]. The report [11] indicated that 20% of the institutions were attacked once at least, and exploited to be through which to attack [12, 13]. From this standpoint, and by looking at the graph in the picture 2, which shows that there is an increase of nearly a third of the number of devices for the year 2025, which means an increase in the probability of attacks significantly. The security specifications of the IoT rely greatly at the amount of providing services; the necessity to secrecy, integrity and authentication relies specifically about the security requirements at the IoT network app [10]. In special, authentication is known to be a critical prerequisite for IoT [14].

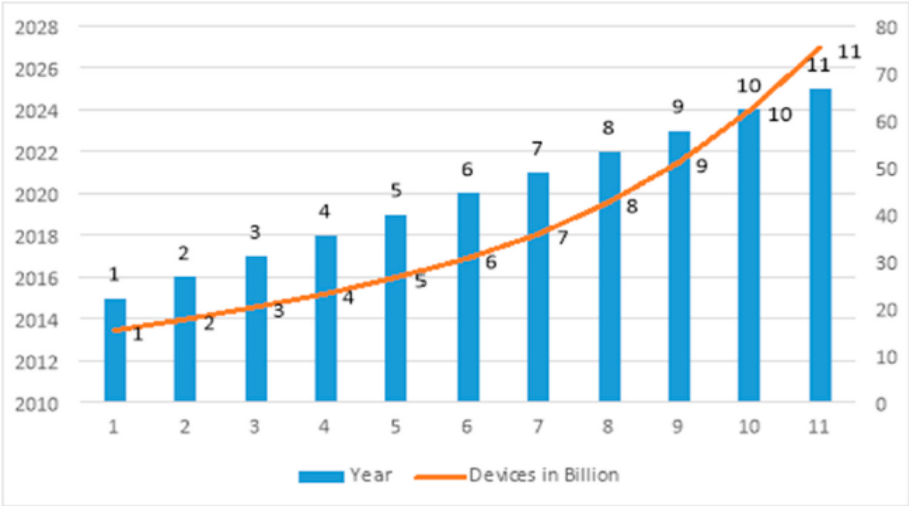


Figure 2. Awaited devices in the Internet of Things by 2025[2]

1.2.1. Elements of Authentication

According to what is in [10], a set of points related to authentication and its relationship to the Internet of Things can be presented as following:

-Identity: data submitted by an entity to another in order to trust itself and one or a mixture of hash, symmetric or asymmetric encryption methods may be used for identity-based authentication schemes.

– Bodily: biometric features depending on a person's physical features, like fingerprinting, hand geometry, retina scanning.

– Behavior: biometric depends on social behavioral features, e.g. keystroke dynamics, walk analysis, speech ID.

1.2.2. Using Tokens

-Token-based Authentication: validates the user or computer on the basis of an identity key generated by the server.
-Non-Token-based authentication: requires the use of user id and password tokens any moment the content needs to be shared.

1.2.3. Authentication Method

-A-way authentication: just one entity can validate the other, but the other will not be validated.
-Two-way authentication: the two organizations authorize one to another.
-Three-way authentication: essential authority verifies the two entities and allows them to validate each other.

1.2.4. Architecture of Authentication

Distributed direct authentication between the entities to the correspondence.

A central server or a trusted third party to spread and maintain authentication certificates.

1.2.5. IoT layer

The layers how where an authentication mechanism is implemented.

-Perception Layer: Liable to storing and dealing out the data obtained via the entities on the IoT network.
-Network layer: liable to obtaining and manipulating the obtained information of the perception layer.
-Application layer: liable of collecting information of the second layer and then availability service demanded of the customer.

1.2.6. Hardware-based

The authentication method may involve the physical properties of the devices or devices to be used.

-Implied hardware-based: applies hardware physical features to improve authentication, like Physical Unclonable Method (PUF) or Valid Random Number Generator (TRNG).
-Outright hardware-based: Several authentication methods were dependent at the utilization from the Trusted Platform Modules (TPM), a device which holds and manages the codes applied in device authentication.

1.3. Problem Statement

The development of the Internet of Things technology and the people's dependence on it in many matters of their lives requires securing it against any attack and revealing its vulnerabilities and

immunizing them. The first step of securing any technology is by conducting an effective authentication technique. Therefore, this study will review the existing authentication techniques in IoT environment in order to propose a harder authentication technique.

2. LITERATURE REVIEWS

This section includes a summary to the current authentication mechanisms inside IoT environment. Specifically, CoAP protocol components, characteristics, and mechanism is presented

2.1. Existing Authentication Mechanisms

Table (1) summarizes existing authentication mechanisms in terms of their aims and approach.

Table 1. Previous Authentication Mechanisms

Research Title	Year	Aim	Research Approach
Authentication of IoT Device and IoT Server Using Secure Vaults[15]	2018	Solve problem of Single password-based authentication mechanisms which put IOT vulnerable of many attack	Provides a reciprocal authentication method consists of multi-key or passwords where named the shared secure between the IoT server and the IoTclient as secure vault. After each successful session among the server and the IoT equipment, the collection of passwords is modified.
Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks[1]	2018	Design of a new secure remote user authentication scheme	Design user authenticated key management protocol UAKMP which based on three variables are smart consumer card password, and private biometrics. Compared to other existing systems, UAKMP is more stable, supports the nodes addition process, and even the key and biometrics change process internally without the GWN's mediation.
Multi-level Trust based Intelligence Schema for Securing of Internet of Things (IoT) Against Security Threats Using Cryptographic Authentication[16]	2020	Reduction of gray hole attacks using check node information with detection rate of 94.5percent against gray hole attack	Depend on AODV routing protocol and is offered below the MTISS-IoT. The suggested solution is based on cryptography authentication and consists of four steps, like checking node trust in the IoT, path monitoring, detection of gray whole attacks, and the removal of malicious attacks in MTISS-IoT.
A Novel Lightweight Block Cipher-Based Mutual Authentication Protocol for Constrained Environments[17]	2020	Developed LBCbAP a modern encryption protocol based on lightweight block ciphers agnist hidden exposure and desynchronization attack.	A latest stable protocol established on lightweight block ciphers, LBCbAP, backed via formulated or not formulated security evidence, was introduced. In this protocol we use a block cipher CRAFT as the central primitive security that illustrates its security against different forms of threats, including hidden exposure and desynchronization threats.

Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments[18]	2020	Suggests an easy and reliable authentication scheme for WSNs in IoT systems based on temporal credentials and dynamic IDs.	It follows the standards for the authentication system's basic architecture specifications and enhances security efficacy in real-world IoT settings. In comparison with the other systems, the performance review showed high reliability and better performance for the method.
Smart card-based secure authentication protocol in multi-server IoT environment[19]	2017	Suggested a smart card-based authentication protocol and tested it using AVISPA by visualizing a structured validate scenario	It authenticates each entity via letting people to use a smart card transferred via invalidation server to go through the verification process and access to an IoT-connected server and the authentication protocol is used in different applications such as key exchanges, using smart card, and more.
BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology[20]	2020	Suggestion a Machine to Machine Authentication Protocol for Smart City Apps leveraging 5 G Technologies (BIDAPSCA5 G) built on the Blockchain Internet of Things (IoT).	The registration process of connected devices is carried out via secret blockchain accessible only by authorized individuals. Shared authentication was conducted without RAC, Gate-Way-Node (GWN) intervention to minimize the cost of processing location-based authenticate process, blockchain-based repeal.Step and IoTD registration, device-level IoTD confidentiality property.
A secure authentication scheme for IoT application in smart home[21]	2020	Presented a secure addressing and authentication (SCSAA) framework based on a smart card by changing the existing IPv6 method to minimize security issues in the IoT.	By issuing a special 64-bit Interface Identifier (IID) to smart phones or programs and authenticating them securely in the IoT system, it presents a strong way of addressing and using the hidden session key to block unauthorized access to the network. It is tested by model ROR and the method AVISPA.
A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment[22]	2019	In order to solve security issues such as session key leakage, impersonation and replay attacks, a stable and flexible three-factor authentication solution for IoT in the cloud computing world	This authentication protocol can stand multiple attacks and provide protected mutual authentication between user Ui, cloud server Sj, and server CS control using BAN logic analysis and protection using hidden and biometric parameters using only bitwise exclusive or (XOR) and hashing functions to make it more powerful than the schemes of Pelaez et al.
Secure Authentication Protocol for 5G Enabled IoT Network[23].	2018	Supply an appliance layer authentication protocol to minimize all attacks emanating as of the public access network. and examine the security protocol by An advanced security monitoring platform Scyther	Introduce an effective protection protocol in the Application layer, among client-Equipment and Mobility Management Feature (AMF) that is taking charge of the ration of resources after the verification of Network Slice Collection Association Details (NSSAI) of 5G network. Where the request for user passwords and services is secretly shared, thereby maintaining anonymity and the protocol is immune

			to numerous attacks that which arise from secrecy, honesty and availability.
A three-factor anonymous user authentication scheme for Internet of Things environments[24]	2020	suggest an upgraded three-factor user authentication mechanism to overcome security problems which find in Dhillon and Kalra schema	Indicate a three-factor anonymous user authentication method for IoT environments that follow a specific four stages: registration, login and authentication, changing of password, and user revocation stage, and use the random oracle model, BAN logic, and ProVerif tool to conduct informal and structured security assessments. The findings of the study suggest that the proposed system is protected from different documented attacks and meets all protection criteria and is compliant with relatively low-cost IoT systems.
Dynamic Authentication Key Agreement Scheme for Effective Path Selection in I IoT Systems[25]	2020	Provides a new solution that uses an active authentication key agreement system in which only legitimate users can access data in the IIoT setting from IoT sensor nodes.	For key validation and protected data transmission, the Dynamic Authentication Key Agreement System (DAKAS) and the Efficient Route Selection and Access Control Logic System (EPSSCLS) are used. It is support add of new nodes after the state of before-process of deployment in the network, the process of the complex node IoT sensing system and the transmission route are revoked in the event of any intrusion detection or stolen and leaked information by an opponent. Using the true or random (ROR) model and AVISPAA, structured security checking is carried out.
Smart Contract-Based Cross-Domain Authentication and Key Agreement System for Heterogeneous Wireless Networks[26]	2020	Formulate a cross-domain authentication and key approval scheme setup on a blockchain smart knot.	Cross-domain authentication and key agreement protocol are configured. The smart contracts are used to handle the shared keys of the nodes, and the device parameters are checked by contract demand. Customers can pick momentary authentication specifications based on the roaming domain system specifications to complete the encryption and authentication arrangement, and users are private in the operation. The protocol does not have complex encryption and certificate authentication processes, that reduced overhead of computing and connectivity.
On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks[27]	2020	Provides a stable and effective authentication protocol depending on 3-factor authentication using biometric data and employs the honey	suggest an effective protocol to defend against brute force and theft smartcard attacks which uses only hashing algorithm, except public key Elliptical Curve Cryptography and Conduct informal vulnerability scanning,

		list technique and provide protection even though two of the three factors are hacked.	model-based Real-Or-Random (ROR) and logic-based Burrows Abadi Needham (BAN) official security evaluation, and conduct formal verification employing (AVISPA) simulation tools.
A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things[8]	2020	Introduce system design by proposing the incorporation of WSNs and 5 G into IoT. Centered on the crypto analysis of Adavoudi-Jolfaei et al.'s scheme and device architecture, we present a privacy-based elliptical curve encryption (ECC) Keeping the WSN verification, authorizing, and mutual authentication framework in 5G incorporated IoT.	They studied the three-factor authentication and control access scheme of Adavoudi-Jolfaei et al. and highlighted its vulnerabilities, and then implemented a device implementation appropriate for WSNs in 5G-integrated IoT. On the basis of thestructural design, An ECC-based three-factor verification, authorizing, and mutual authentication framework was proposed.
A Security Approach for CoAP-based Internet of Things Resource Discovery[28].	2020	Provides a protection strategy employing TACACS+ to security improving of the CoAP which Assists entrance check , identity verification and auditing	A protection solution to the CoAP technique utilized explore resources in the IoT field. The protection strategy is focused on the Utilization of the TACACS+ protocol to enhance the security of the CoAP.

The table above shows a recent set of authentication techniques in the Internet of Things. This secure authentication of IoT objects is done in several ways

Using two factors such as[15] which use AES encryption and HMAC and have more saving power compared with ECC algorithm. In[18]based on temporal credentials and dynamic IDs which depend on MAC to secure translate of data. In [20] using ECC and SHA-1 algorithm to mutual authentication between tow IOT devices. In [25] using the Dynamic Authentication Key Agreement System (DAKAS) and the Efficient Route Selection and Access Control Logic System (EPSSCLS)for key validation and protected data transmission. In [26] cross-domain authentication and key agreement protocol are configured and the smart contracts are used to handle the shared keys of the nodes.

Or three factors as in[1] proposed UAKMP which based on three variables are smart consumer, card password, and private biometrics. In [22]using hidden and biometric parameters, only bitwise exclusive or (XOR) and hashing functions. In [24] indicate a three-factor anonymous user authentication method for IoT environments that follow a specific four stages: registration, login and authentication, changing of password, and user revocation stage. In[27]using biometric data and employs the honey list technique and provide protection even though two of the three factors are hacked. In [8]introduced a three verification, authorizing, and mutual authentication framework built through ECC.

By using these technologies, many attacks are countered and security goals achieved like in [16]detection rate of 94.5 percent against gray hole attack. In [17] approach secure agnist hidden exposure and desynchronization attack. In [19] protected from identity plagiarism and exposure of key. In [21] using strong way with hidden session key to block unauthorized access to the network. In [22]solve security issues such as session key leakage, impersonation and replay attacks. In [23]maintaining anonymity and the protocol is immune to numerous attacks that which arise from secrecy, honesty and availability. In [27]defend against brute force and theft smartcard attacks. In [28]separator security amidst users depend on the permissions available to them to ensure authentication, authorization, management of access and auditing services.

2.2. Constrained Application Protocol (CoAP) protocol

Constrained Application Protocol (CoAP) has a constant byte header of only 4 bytes, but constrained assets are used[29]. The cost-saving availability of RESTful resources in Low-Power Lossy Networks (LLNs) combined with limited sophistication in form head of protocol , message decoding, asynchronous transfer framework and built-in asset exploration renders it an optimal option for IoT deployers. So for These characteristic aspects make CoAP an optimal substitute for current IoT devices like MQTT and XMPP[29]. CoAP is therefore implemented in a variety of products, like transportation logistics, housing automation, intelligent cities and shipment monitoring[29].

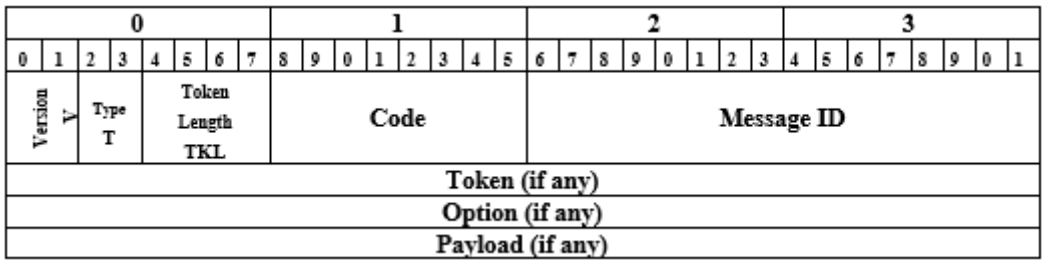


Figure 3. CoAP packet with 4 bytes.

CoAP is a constraint state that caused a terrible package transfer and a large overhead, such as a limited hub with small RAM or Processor power, and is a request/response technique [30]. It is designed by the Internet Engineering Task Force (IETF) by an idea of device to device applications and platform automation to minimize overhead, optimize packet transference and increase work simplicity by using the main HTTP application [31]. The main characteristic of CoAP is an integrity and reliability [32], as it supports unicast and multicast demands by leveraging User Datagram Protocol (UDP), and gives the ability to exchange asynchronous messages [30]. It is able to interoperate with HTTP because it introduces an internet transfer protocol dependent on the Representational State Transfer (REST) above the HTTP features [33]. But because CoAP is dependent on REST, the CoAP-REST proxy provide a direct transference of these protocols. CoAP/HTTP assists CoAP users to connect HTTP server assets using a reverse proxy that converts the HTTP state key to the CoAP response code [34]. CoAP helps devices with mini power, connection, and computing capacity systems to use RESTful activities [35]. CoAP is proposed by scholars, owing to its light properties, to be used in a variety of fields from applied of smart cities to the commercial WSNs [36].

CoAP is a simple device layer request/response protocols for both synchronized and unsynchronized answers[35]. CoAP has the below data packets and answer forms: provable, needs an acknowledgment inside the ACK or with an independent message. Non-confirmable (no

need for ACK), restart (verified receipt of a text that could not be executed) and acknowledgment (proven receipt of have a provable message), Piggy-backed answer (receiver answer is piggybacked to ACK) and independent answer (receiver answer in a text other than ACK after some moment)[35]. As HTTP, CoAP utilizes GET, PUT, POST and DELETE methods for generating, restoring, modifying and removing processes[35].

The researcher in[35] mentioned the elements of CoAP and its distinguishing properties as follows:

2.2.1. Components of CoAP protocol

1. Last node Determined by IP and UDP port number. The last node is the target or origin of the CoAP packet.
2. Dispatcher who creates message.
3. Receiver message.
4. Consumer who put an order rather than a message
5. Server the recipient last node of the demand and the source node of the reply.
6. Source server: A service is generated or exists on this server.
7. Intermediate: is a last node that can perform as a host and a consumer to a source server.

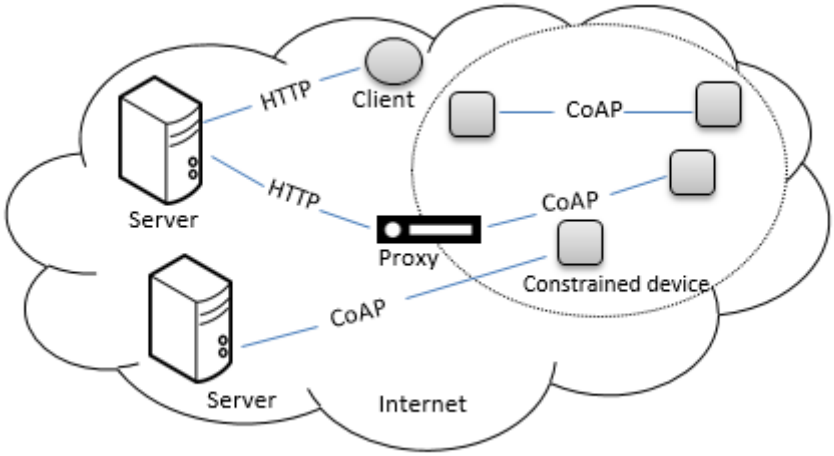


Figure 4. CoAP transaction

Figure 4 explained CoAP interaction between elements with more cases of them.

2.2.2. CoAP protocol characteristics

1. Assets monitoring: on-request subscriptions utilizing publish/subscribe system for tracking online services
2. Move of the block resources: without refresh the entire data in order to transmitter data and receive. This minimize cost communications.
3. Asset exploration: URI patterns are utilized which utilize website domains in the CoRE link format to allow the exploration of resources for consumer.
4. Dealing directly with HTTP: CoAP is simple communicate with HTTP according to the standard REST structure that contributes to flexible interaction.
5. Most programming languages like C, C #, Javascript, erlang, Ruby contain CoAP libraries as well as for iOS and Android.
6. CoAP has smaller processor and Capacity consuming and is easy to use[35].

2.2.3. Drawback of CoAP

The CoAP protocol does not include trusted standards for secure structures and its messages are secured on top of the UDP in the Datagram Transport Layer Security (DTLS)[37] that was not initially designed for resource-limited devices so it is not suitable for a CoAP agent[36]. Like , in executing a handshake procedure, DTLS requires six travel messaging that raise workload information exchange and consume restricted power from machines[36].

A number of scholars have undertaken DTLS research to protect the protocol, but substantial work remains to understand how securing CoAP is controlled and applied[38, 39] with maintaining large efficiency after having the requisite security for transmissions[36].

CoAP protocol is defined as large inertness, terrible packet transmission, and its inability to be used on a complicated category of data[30].

2.2.4. Security for CoAP protocol

The DTLS protocol is running over UDP and gives for encrypted CoAP exchanges [33]. Supports validation, auto key management, secrecy, encryption technologies and data integrity but DTLS not support multicasting like CoAP [33] and we know all that CoAP protocol is one of routing application layer witch related with authentication directly. CoAP protection is a significant factor owing to the unavailability of trustable specifications to protect the CoAP structure[36]. DTLS offers security services, including anonymity, honesty, authentication and non-rejection facilities using the essentials of the AES/CCM[38]. According to[36] DTLS handles key protection aspects such as authentication, anonymity, password retention, and message integrity in four forms:

1- No Sec Type: where it expects that the protection function will be enforced with other protocol layer, and therefore data will be transferred without security.
2-PreSharedKey Type: which machines that are permitted to applied itself system with a singular symmetric key which allows to connect with other machine?
3-RawPublicKey Type: is known to be important for the working of the CoAP and usually adopts the machines that needed authentication, and utilizes the asymmetric password for each machine to identify and communicate with these machines.
4-Certificates Type: is known to be an authentication method for machines that execute CoAP via an X.509 certificate.

2.2.4.1. Challenges of using DLTS

It needs four transmission and return transmissions, three of which are for DTLS and one for COAP, which supports multiple transmissions and which distinguishes the Internet of Things while not supported by DTLS this one of disadvantages of using DTLS [40].

The DTLS interaction protocols may (yet including the ungoverned cookie) lead to an aggressive assault on battery-operated system resources. As a response, nodes may miss their position in the connection and interrupt the whole network.

Although DTLS will secure from replay attack through the bit image frame, packets must be received initially via nodes, translated, and often transmitted. The probability of this threat may cause the network to overflow without scanning proxies as 6LoWPAN Border Router (6LBR).

Separation of handshake packets also has a problem Too the hashing is important to execute everything to validate handshake packets Messages that indicate a big buffer to several nodes are necessary and in each situation this does not applied

Security in DTLS does not do well with CoAP so all messages need to be resend if one is lost also when all packets in-flight transmission transfers in a UDP packet, much assets needed big buffers for managing.

2.2.4.2. Object Security for Constrained RESTful Environments

OSCORE is a new universal solution which offers cover-to-cover protection for CoAP transactions on the application layer [41]. OSCORE is a good choice to security in CoAP protocol than DTLS. Where the presence of the DTLS layer requires step-by-step security between both the transfers between the server and the proxy and also the enforcement of protection between the agent and the client [41]. While OSCORE provides secure two-way Contact among the client and the server is secured by using a proxy [41]. The security solution allows proxies to perform their functions as forwarding and scheduling CoAP queries connected to servers. OSCORE's effectiveness at protecting and decoding messages is superior to DTLS using HMAC and authenticated encryption associated data AEAD [41]. OSCORE reaches this outcome through a very better execution of the AES encryption [41]. OSCORE consumes greater RAM than CoAP but DTLS consumes greater than OSCORE [41]. Its outcomes in a per-exchange power usage of around 8–28 percent greater than that of CoAP [41]. This means that OSCORE is most power saving than CoAP, which outcomes in a power demand of around 17–59 per cent increaser than COAP [41]. OSCORE execution shows simple improved efficiency than TinyDTLS in respect of overload network messaging, RAM utilization, transmission round-trip time and effort consumption. Thus, offering security enhancements to OSCORE without extra efficiency dragging [41]. OSCORE accomplishes that result using a highly robust execution of the AES CCM 128 methodology [41].

3. RESEARCH METHODOLOGY

The proposed security solution aims to authenticate IoT users using symmetric key with biometric features. Biometric is a strong mechanism to authenticate user because it is a unique code which is hard to be hacked. Biometric features have a high demand due to its true effect in software and precision in performance[42].Symmetric key via AES-128-CCM bits is a suitable state for security with a natural IoT constrained devices when implementing CoAP protocol. The presented solution adopts these two methods to create a secure authentication mechanism between the server and the client. So that the agent verifies the client's authenticity and then begins the process of transmissions and processing of requests via original CoAP method.

3.1. Registration step

The scenario of this solution will be as the following. Assume there is a server and a client who has biometric features according to requirements of the application, as well as a symmetric key known between them. When the client wants to connect IoT devices, he sends request for the server to initiate a connection. The server requests the biometric and the shared key from the client. The customer takes the biometric image and then enters the shared key. The biometric is encrypted with the shared key until it reaches the destination. The key is decrypted then when the shared key is true, the biometric is verified and biometric stored there (for the first time). By the end of the process, object authentication and data exchange are done.

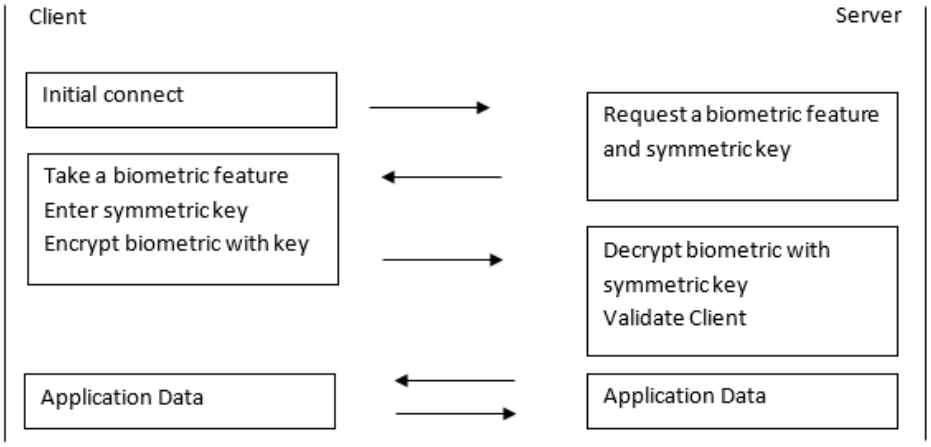


Figure 5.Senario of the Proposed Solution

3.2. Second step

Suppose that when the client wanted to connect again, the client did not need a request to start a connection and had previously contacted the server. He will send his request loaded with the encrypted biometric with the shared key to the server, which in turn receives the request and finds it loaded with the authentication part, so he verifies the validity of the biometric that stored in first step by decrypting the shared key. The validity of the key means decryption, it will verify the validity of the biometric and authenticate the client. These steps are explained in Figure 6.

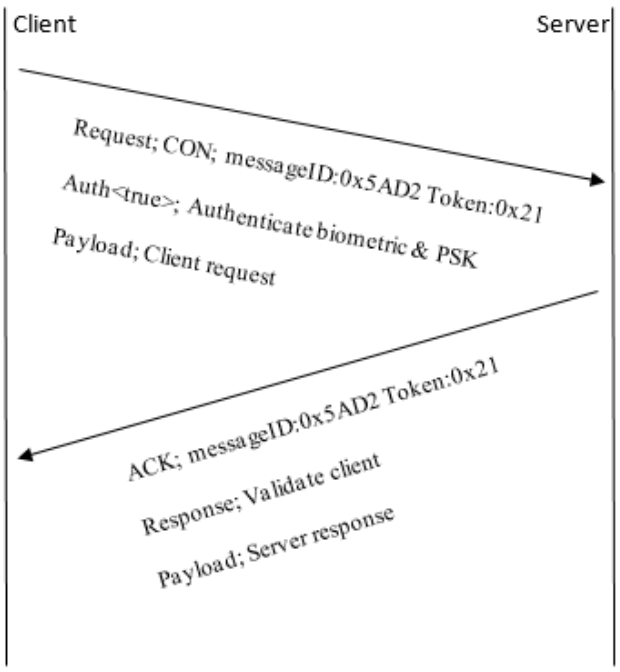


Figure 6. Authentication handshake

3.3. Transfer Data

As for what is related to the other party, which is the limited resource devices that cannot deal with encryption such as a biometric and complicated matters, the transfers between it and the server will be dependent on simple CoAP transfers because we have secured the server by securing all his clients. Thus the validity of such an assumption will provide energy and optimal use of resources in a safe environment.

4. REQUIREMENT ANALYSIS

Programming with pythonlanguage to produce the possibility of implementing the proposed solution. The application provides an authentication service to IoT clients. It uses COAP loT protocol, which depends on encrypting the client biometric by a symmetric key AES CCM 128 and validating the client in the server side by decrypting the symmetric key byfollowing these steps. The client sign up in the proposed application by registering his biometric and the symmetric key. The client biometric will be encrypted by a symmetric key. Then, the encrypted biometric will be sent to the server, which will decrypt the symmetric key and store the biometric. When the client login to the application in the next times, the server will validate the client by decrypting symmetric key and comparing his biometric with the stored biometric. If the decrypted biometric is the same as the stored biometric, then the client is authenticated. So, the server will grant him access to all connected devices. As a result, the client have access to the app (Camera) and any other control services (ON, OFF, TALK, and RECORD).

5. IMPLEMENTATION

The implementation of the suggested solution is based on python language, which can be run in any supported environment like anaconda, pycharm and so on. There are two main objectives that were relied on when implementing the program. The first is that the program works based on the CoAP protocol. Second, the verification data, which is the fingerprint, is encrypted with the symmetric key encryption algorithm, which is AES CCM 128.

The program was created to receive all fingerprints. In the client side, it is assumed a set of fingerprint images that added to the database so that the client can choose his fingerprint, which is encrypted with the encryption algorithm by calling it and then sending the encrypted fingerprint to the server. The server receives the encrypted image on the authentication block and decrypts it and tries to match the receiver fingerprint with the correct user. Upon verification, a message appears in the name of the user as a proof of validity of verification. This means that the server will allow the client to connect to the services that are available to him. Here, it is assumed that the service connected to the server is a camera device that shows the option to take a picture. A default picture was placed because it can accomplish the goal of the program as an evidence and using a real camera will consume long time and cost. These resources are not available at the present time.

5.1. Screenshot of the Program

1- The main interface of the program that appears when the client's code is executed where he can access by entering his biometric or exit program.

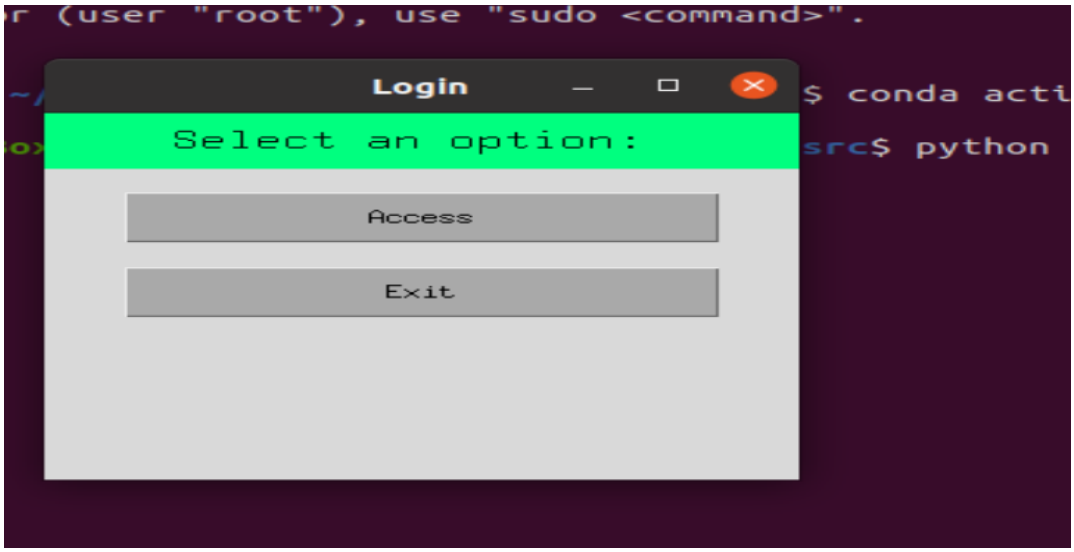


Figure 7. The main interface

2- The second screen, the client chooses his fingerprint from the set of fingerprints defined in his database, as it appears in the screen where the image is selected and then encoded with the encryption algorithm and sent to the server.

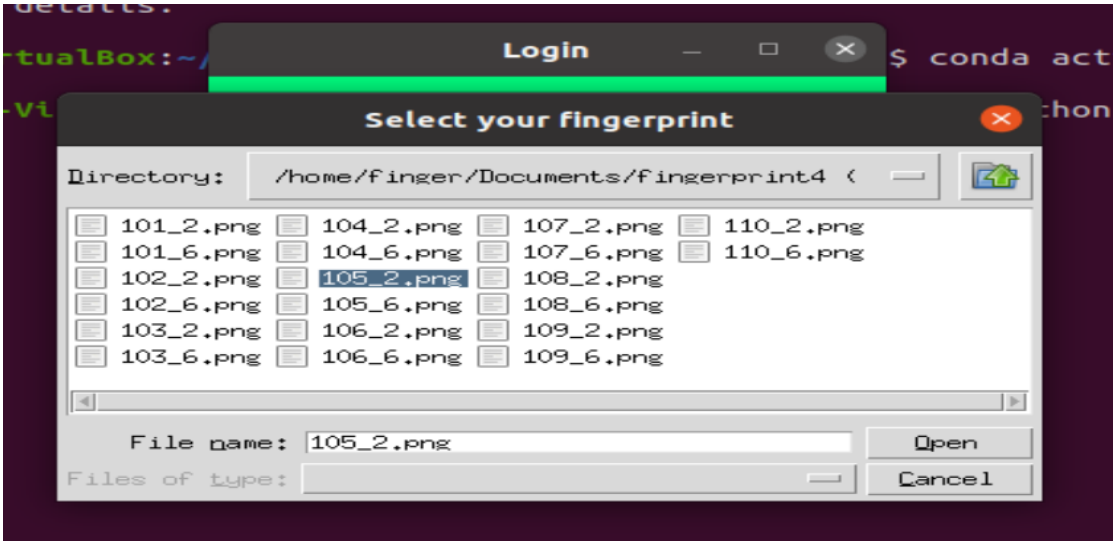


Figure 8. Second screen

3- The third screen shows the image of the received and enhanced fingerprint of the server, where it was transferred from the client side to the server via the CoAP protocol and the server decrypts the fingerprint which appear in photo as new unique message received.

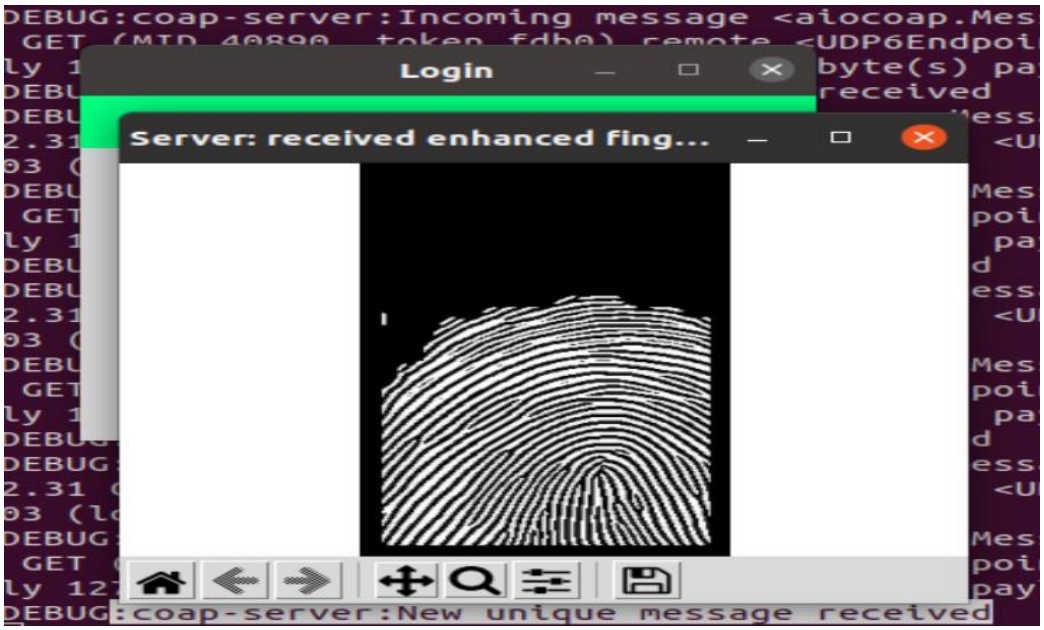


Figure 9. Third screen

4- The fourth screen shows the server verification of the client matching the received fingerprint with the correct user.

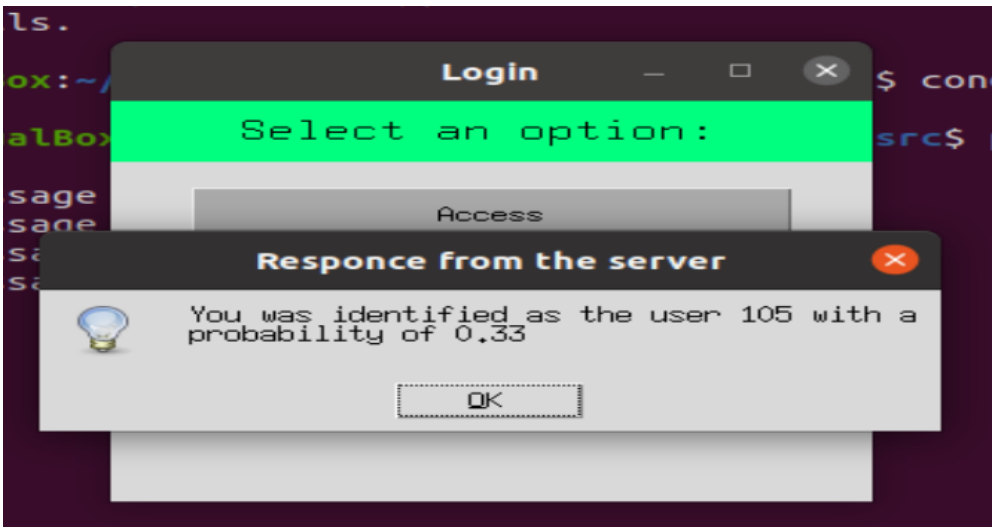


Figure 10. Fourth screen

5- The fifth screen displays linking the client to one of the server-related services, which is the camera, and allows him to take a picture.

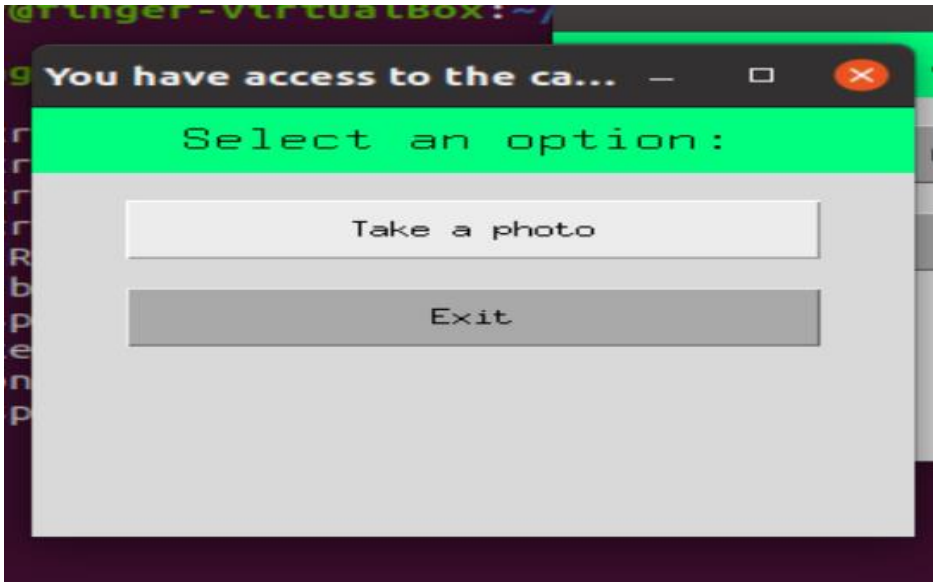


Figure 11. Fifth screen

6- The sixth screen shows the default image for the camera capture.

Figure 12. Sixth screen

5.2. Analysis of the Enhanced COAP Protocol

In this project, an authentication mechanism is applied via CoAP protocol to improve its security by using fingerprint biometric encrypted with symmetric key AES CCM. Hence, biometric feature is considered as a strong security mechanism and symmetric key AES CCM 128 is suitable for constrained devices. It is proved that the proposed solution has overcome some of the defects of the CoAP protocol, which are mentioned earlier, as its reliance on safety on DTLS is not suitable for restricted devices and costs more time. This leads to energy consumption and thus affects its effectiveness. The proposed solution is distinguished from OSCORE in that it relies on

a robust verification process, which is fingerprint, and therefore it can be said that the project have provided a good solution in this regard.

6. CONCLUSION

This project focused on enhancing security in Internet of things (IoT) by developing an authentication mechanism depending on the available features of CoAP protocol, which is the famous protocol in IoT. The study started with presenting an overview of the emergence of the Internet of things and the importance of being the focus of the study. Then, it provided a brief of authentication and its role in IoTs as the first line of defense. After that, the report summarized a list of researches to some of the authentication mechanisms in the Internet of things at the recent last years. CoAP protocol has been chosen to be the study focus because it is designed specifically for the Internet of things and its restricted devices. Python language is applied to execute the proposed security solution for authentication using a symmetric key with biometric features. The implementation proves that the proposed method enhanced security of IoT users by improving CoAP protocol performance and support CoAP library with created authentication method.

7. FUTURE WORK

As a future work, this study lays the foundation stone for the expansion of the more implementation of the authentication methods based on CoAP protocol. The proposed solution can be improved by including all kinds of biometric features, such as the iris, facial recognition and retina. In addition, the extent of its effectiveness and security when it is actually implemented in the Internet of things environment and linked to more than one device and evaluated in terms of its efficiency in enhancing security of IoT users.

ACKNOWLEDGEMENTS

I would like to thank God for his generosity in providing me the ability to perform this work. I am so grateful to my family for their love and continuous support, to my friends for their motivation, my supervisor (Dr. Wael) for his guidance and encouragement. I also sincere to express my thanks to Taif University for providing a great opportunity that allow me to accomplish my scientific goals. Especially, that coincides with the aspirations of the vision of our King the Custodian of the Two Holy Mosques.

REFERENCES

[1] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269-282, 2017.

[2] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures," *Computers*, vol. 9, no. 2, p. 44, 2020.

[3] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: Evolution and technologies from a security perspective," *Sustainable Cities and Society*, vol. 54, p. 101728, 2020.

[4] S. S. Daniele Miorandi, Francesco De Pellegrini, and Imrich and Chlamtac., " Internet of Things: Vision, applications and researchchallenges," *Ad Hoc Networks 10, 7 (2012), 1497 { 1516.*, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870512000674.

[5] Google, "Technical overview of Internet of Things," update 2020/9/9. [Online]. Available: https://cloud.google.com/solutions/iot-overview.

[6] J. Manyika *et al.*, "Unlocking the Potential of the Internet of Things," *McKinsey Global Institute*, 2015.
[7] M. Botterman, "for the European Commission Information Society and Media Directorate General," in *Networked Enterprise & RFID Unit–D4, Internet of Things: An Early Reality of the Future Internet, Report of the Internet of Things Workshop, Prague, Czech Republic*, 2009.
[8] S. Shin and T. Kwon, "A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things," *IEEE Access*, vol. 8, pp. 67555-67571, 2020.
[9] G. Choudhary, J. Kim, and V. Sharma, "Security of 5G-mobile backhaul networks: A survey," *arXiv preprint arXiv:1906.11427*, 2019.
[10] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) Authentication schemes," *Sensors*, vol. 19, no. 5, p. 1141, 2019.
[11] D. Maresch and J. Gartner, "Make disruptive technological change happen-The case of additive manufacturing," *Technological Forecasting and Social Change*, vol. 155, p. 119216, 2020.
[12] M. E. Ahmed and H. Kim, "DDoS attack mitigation in Internet of Things using software defined networking," in *2017 IEEE third international conference on big data computing service and applications (BigDataService)*, 2017: IEEE, pp. 271-276.
[13] C. Beek *et al.*, "Mcafee labs threats report," *McAfee, Santa Clara, CA, USA, Tech. Rep*, 2017.
[14] L. Atzori, A. Iera, and G. Morabito, "" The internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787-2805," 2010.
[15] T. Shah and S. Venkatesan, "Authentication of IoT device and IoT server using secure vaults," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018: IEEE, pp. 819-824.
[16] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah, and R. Fotohi, "Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication," *The Journal of Supercomputing*, pp. 1-26, 2020.
[17] C. Trinh *et al.*, "A Novel Lightweight Block Cipher-Based Mutual Authentication Protocol for Constrained Environments," *IEEE Access*, vol. 8, pp. 165536-165550, 2020.
[18] C.-T. Chen, C.-C. Lee, and I.-C. Lin, "Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments," *PloS one*, vol. 15, no. 4, p. e0232277, 2020.
[19] W.-i. Bae and J. Kwak, "Smart card-based secure authentication protocol in multi-server IoT environment," *Multimedia Tools and Applications*, vol. 79, no. 23, pp. 15793-15811, 2020.
[20] M. Vivekanandan and V. Sastry, "BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology," *Peer-to-Peer Networking and Applications*, pp. 1-17, 2020.
[21] P. Kumar and L. Chouhan, "A secure authentication scheme for IoT application in smart home," *Peer-to-Peer Networking and Applications*, pp. 1-19, 2020.
[22] S. Yu, K. Park, and Y. Park, "A secure lightweight three-factor authentication scheme for IoT in cloud computing environment," *Sensors*, vol. 19, no. 16, p. 3598, 2019.
[23] S. Sharma *et al.*, "Secure protocol for 5g enabled iot network," in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, 2018: IEEE, pp. 621-626.
[24] H. Lee, D. Kang, J. Ryu authentication, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for Internet of Things environments," *Journal of Information Security and Applications*, vol. 52, p. 102494, 2020.
[25] M. H. A. Venkatesh M Ka, Sukumar Sc, Dr Geetha Rd*, "Dynamic Authentication Key Agreement Scheme for Effective Path Selection in I IoT Systems," *VDGOOD Journal of Computer Science Engineering*, 2020.
[26] G. Li, Y. Wang, B. Zhang, and S. Lu, "Smart Contract-Based Cross-Domain Authentication and Key Agreement System for Heterogeneous Wireless Networks," *Mobile Information Systems*, vol. 2020, 2020.
[27] J. Lee, S. Yu, M. Kim, Y. Park, and A. K. Das, "On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks," *IEEE Access*, vol. 8, pp. 107046-107062, 2020.
[28] K. Khalil, K. Elgazzar, A. Abdelgawad, and M. Bayoumi, "A security approach for CoAP-based internet of things resource discovery," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020: IEEE, pp. 1-6.

[29] M. A. Jan, F. Khan, M. Alam, and M. Usman, "A payload-based mutual authentication scheme for Internet of Things," *Future Generation Computer Systems,* vol. 92, pp. 1028-1039, 2019.
[30] K. Pothuganti, "Overview on Application Layer routing Protocols for the Internet of Things," *International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering,* vol. 7, no. 11, 2018.
[31] H. Kitano, "Artificial intelligence to win the nobel prize and beyond: Creating the engine for scientific discovery," *AI magazine,* vol. 37, no. 1, pp. 39-49, 2016.
[32] V. D. Soni, "Prediction of Geniunity of News using advanced Machine Learning and Natural Language processing Algorithms," *International Journal of Innovative Research in Science Engineering and Technology,* vol. 7, no. 5, pp. 6349-6354, 2018.
[33] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials,* vol. 17, no. 4, pp. 2347-2376, 2015.
[34] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," *Transaction on IoT and Cloud computing,* vol. 3, no. 1, pp. 11-17, 2015.
[35] S. Verma and M. A. Rastogi, "IOT Application Layer Protocols: A Survey," *Journal of Xi'an University of Architecture & Technology,* vol. XII, no. VIII, 2020.
[36] F. A. Alhaidari and E. J. Alqahtani, "Securing Communication between Fog Computing and IoT Using Constrained Application Protocol (CoAP): A Survey," *Journal of Communications,* vol. 15, no. 1, 2020.
[37] E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," 2012.
[38] J. Vishwesh and M. Rajashekar, "Internet of Things (IoT): Security analysis & security protocol CoAP," *International Journal of Recent Trends in Engineering and Research,* vol. 3, no. 3, pp. 417-425, 2017.
[39] M. Zolanvari and R. Jain, "IoT security: a survey," in *Recent Advances in Networking (Data Center Virtualization, SDN, Big Data, Internet of Things)*: Nova Sci, 2015, pp. 1-15.
[40] T. A. Alghamdi, A. Lasebae, and M. Aiash, "Security analysis of the constrained application protocol in the Internet of Things," in *Second International Conference on Future Generation Communication Technologies (FGCT 2013),* 2013: IEEE, pp. 163-168.
[41] M. Gunnarsson, J. Brorsson, F. Palombini, L. Seitz, and M. Tiloca, "Evaluating the Performance of the OSCORE Security Protocol in Constrained IoT Environments," *Internet of Things,* p. 100333, 2020.
[42] M. M. A. Ebtesam H Alharbi, "BIOMETRIC AUTHENTICATION SYSTEMS TOWARDS SECURE AND PRIVACY IDENTIFICATION: A REVIEW," *Electronic Interdisciplinary Miscellaneous Journal (EIMJ)* no. 23 4/2020, 2020.
[43] A. Team, "HLPSL Tutorial: A Beginner's Guide to Modelling and Analysing Internet Security Protocols, 2006," ed.
[44] R. A. Abouhogail, "A Comparative Analysis of Tools for Testing the Security Protocols," 2019.
[45] T. Genet, "A short span+ avispa tutorial," IRISA, 2015.

PRODUCT QUALITY EVALUATION METHOD (PQEM): A COMPREHENSIVE APPROACH FOR THE SOFTWARE PRODUCT LIFE CYCLE

Mariana Falco[1] and Gabriela Robiolo[2]

[1]LIDTUA/CONICET, Engineering School, Universidad Austral,
Pilar, Buenos Aires, Argentina
[2]LIDTUA, Engineering School, Universidad Austral,
Pilar, Buenos Aires, Argentina

ABSTRACT

Project managers, product owners, and quality assurance leaders need to visualize and understand the entire picture of the development process as well as comprehend the product quality level, in a synthetic and intuitive way in order to facilitate the decision of accepting or rejecting each iteration within the software life cycle. This idea is extremely important nowadays, due to the fact that time is a key resource and it should be managed wisely to obtain a feasible quality level for each software deliverable. This article presents a novel solution called Product Quality Evaluation Method (PQEM) to evaluate a set of quality characteristics for each iteration of a software product. PQEM is based on the Goal-Question-Metric approach, the standard ISO/IEC 25010, and the extension made of testing coverage in order to obtain the quality coverage of each quality characteristic. The outcome of PQEM is a single value representing the quality per each iteration of a product, as an aggregated measure. Even though a value it is not the regular idea of measuring quality, we believe that it can be useful to use this value to understand easily the quality level of each iteration. An illustrative example of the method was carried out with a web and mobile application, within the healthcare environment.

KEYWORDS

Quality Characteristics, Product Quality Measurement, Coverage, Quality Attributes.

1. INTRODUCTION

The quality of a system is extremely important, and software metrics became an essential part to understanding whether the quality of the software corresponds to what the stakeholders needs [1]. Those needs are characterized by the ISO/IEC 25010 as a set of quality characteristics and sub-characteristics [2]. Considering the diverse stakeholders participating in software projects such as developers, managers, and end users, quality needs to be evaluated at different levels of detail.

Based on the above, several quality measures or metrics have been proposed to achieve the evaluation and measurement, but the practical application of these metrics is challenged, on the one hand, by the need to combine different metrics as recommended by distinct quality-model methods such as Goal-Question-Metric [3] and Factor-Criteria-Metric [4]; and on the other hand, by the need to reach insights in the quality of the entire software product, based on the metric values obtained for software elements such as methods and classes.

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 55-71, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111104

Consequently, a meaningful quality assessment needs to blend the results of various methods to answer specific questions, combining for example cyclomatic complexity with test coverage [1]. As such, project managers and practitioners have different complications when they need to understand the product quality level, in a way that is easy, synthetic and intuitive to identify and extract the status related to each iteration within the software product. For example, when the project manager must make the decision to accept or reject the issues done within an iteration, evaluate the work of the developers, decide on a payment or negotiate a budget extension.

Based on these challenges, our first work was to define a method architecture evaluation method in order to analyse and measure the quality characteristics of a product architecture and its implementation [5]. Based on a deep analysis and feedback from colleagues, we developed a newer version of this method and we called it: Product Quality Evaluation Method (PQEM), which is a five-step method per iteration, whose main goal is to analyse, study, measure and assess the quality level of the different software iterations. PQEM produces a single value between 0 and 1 as the final outcome that represents the product quality level, which is basically the degree to which the software product covers/fulfils its quality attribute requirements [6].

The first step within PQEM is what we called the product setup, where the stakeholder defines the amount of expected iterations that constitutes the development process of the product, as well as the acceptance criteria for the expected quality level per iteration. PQEM is based on the Goal-Question-Metric approach [3] which is a main part of the method baseline, and through this approach is possible to define a set of goals (related to the quality characteristics), questions (our quality attribute requirements or QARs [6], and a set of quality measures or metrics, which allow to measure their fulfilment, are elicited for later aggregation. It is worth mentioning that the ISO/IEC 25010 [2] provided the set of quality characteristics and sub-characteristics as the main foundation to select what to measure according to the product domain and objectives.

The elicitation process is followed by: a) the measurement itself, b) the collection and synthesizing of the results that include the implementation of the extension of the testing coverage [7] as a quality coverage, and c) the final assessment of the product quality level obtained. Likewise, this process is repeated for each iteration within the product life-cycle; and this method can be applied to every development method that defines iterations, like agile methods; within academia and industry.

The present article is structured as follows: in Section II the related work will be addressed, while Section III will provide the description of the research method used. Section IV will describe and characterize each of the steps within the Product Quality Evaluation Method (PQEM). Section V will contain an illustrative application of the method, while Section VI will address the discussion and threats to validity. Finally, Section VII will describe the conclusions and future work.

2. RELATED WORK

Both the definition of the architecture of a product and the specification of quality characteristics and QARs are decisions that should not be taken lightly because they have a high impact on the state of the final product. Even though scenario-based architectural assessment techniques [8] are a well-established approach for performing structured evaluations of architectural designs, these techniques are not widely used in industry. A complete analysis was made in [5] with respect to the first iteration of the application presented here, and its comparison with other architecture-based methods.

E. Woods [9] created an architectural review method called Tiny Architectural Review Approach (TARA), which focuses on how well a particular architecture supports a set of key requirements,

opposite of what most scenario-based methods like ATAM [8] do. TARA allows for the situation where the system has already been implemented, but PQEM can be applied while the software is in development. PQEM five steps per iteration, while TARA is defined with seven steps. Considering the seven steps in a TARA session, one of the main differences with PQEM is that it does not include metrics to analyse the quality characteristics, but in Step 3 they analyse system's production metrics.

TARA approaches only test coverage after running all automated test available, while PQEM extends this concept to analyse the coverage of all quality characteristics per iteration of a product, defining several equations to compute these values. Unlike TARA, PQEM reach to findings and conclusions per each iteration through the TOC quality level, which is a number between 0 and 1; and this number is able to show how close the implementation was to the defined acceptance criteria.

Later on, some authors agreed that managing the cost-effective evolution of industrial software systems represents a challenge based on their complexity and long lifetimes. As such, Koziolek et al. [10] applied several state-of-the-art approaches, to combine them into a holistic lightweight method called MORPHOSIS, which facilitates sustainable software architectures. Consequently, their main focus is sustainability, while our main target is to achieve a proper level of quality that will have impact not only in the sustainability but in the set of quality characteristics included. This method includes three phases: evolution scenario analysis, architecture enforcement and architecture-level metrics tracking.

In the first phase, the authors conducted an evolution scenario analysis according to an extended version of the ALMA method [11], from which they were able to perform a combined top-down, bottom-up scenario elicitation. This is a difference with our work, because apart from not being scenario-based, the elicitation process is not based on ALMA instead the Goal-Question-Metric approach is implemented. The second phase allows to treat the dependencies between module layers, and finally, within the third phase they have found several architecture-level code metrics that measured different aspect of sustainability. The set of metrics measure the quality of modularization of a non-object-oriented software system, and the authors employ the notion of API as the basis for the metrics [12].

They have used Goal Structuring Notation to break down maintainability according to ISO/IEC 25010. As such, they have not focused on the entire set of quality characteristics defined by the ISO/IEC, like PQEM does in the elicitation process. Several authors mentioned that it is important to comprehend the consequences of the decisions on the various software engineering artefacts, like code, test cases, deployments, among others; when analysing the impact of a change request.

As a summary, within PQEM the elicitation is based on the GQM method, to specify the needs of stakeholders in the form of goals, questions, metrics and acceptance criteria for each question. None of the studies proposed any form of synthesis of the analysis, as such, we introduce the definition and calculation of coverage values for each selected quality characteristics, and for the entire product, which leads to the achievement of a multidimensional number as a summary value of the achieved quality level as final output. Finally, the focus of this method is oriented to the measurement of quality characteristics.

3. RESEARCH METHOD

Our research method is embedded within the design-science paradigm, which advocates the problem-solving perspective seeking to create innovations that define ideas, practices,

capabilities, and products through analysis, design, implementation, and management; in order to achieve efficiency and effectiveness [13]. These authors defined a set of guidelines to assist the community to understand the requirements and necessities for effective design-science research. Considering that the paradigm comprises problem conceptualization, solution design, and validation, Runeson et al. [14] stated that it fits as a frame for empirical software engineering research with the goal of providing theoretical knowledge for practical solutions related to real-world software engineering challenges.

3.1. Problem Relevance

Quality plays a major role for end-users, because it is a confirmation of all requirements were designed and developed according to their needs [15,16]. A meaningful quality assessment needs to combine the results of various methods to answer specific questions, joining for example cyclomatic complexity with test coverage [1]; and also, the assessment needs to be able to define a model, broken down into different quality characteristics and sub-characteristics.

Project managers and practitioners have different difficulties when they need to understand the product quality level from every iteration and from the full product, and this understanding can occur when the project manager must make the decision to accept or reject the issues or tasks done as a part of an iteration or even the entire release [17], evaluate the work of the developers, decide on a payment or negotiate a budget extension. PQEM allows to monitor the evolution of the quality level in the product life cycle.

3.2. Design as an Artifact

Based on the previous challenges, the present paper introduces Product Quality Evaluation Method (PQEM) which is a five-step method per iteration, which allows the managers and practitioners study, measure and understand the quality level of a software product. The final output is a numerical single value between 0 and 1, which represents the product quality level. This value is obtained through the quality coverage of each quality characteristic measured, and it can be thought of a multidimensional value due to the fact that the quality level synthesize the quality level achieved by each quality characteristic or sub-characteristic.

The multidimensional component of the PQEM method can be understood as the degree to which the software product covers the set of quality attributes requirements [6]. It is worth mentioning that this process is repeated after each iteration, and even though is currently being performed with a spreadsheet, a tool that facilitates the application and use of PQEM is being developed. Consequently, what is lacking in systematization as far as the method is concerned, it is being put together on to achieve automation from the tool.

3.3. Design Evaluation

The evaluation of the method is carried out through an illustrative example within the academia, by applying it to a mobile application. We will conduct a case study within an industrial setting, to obtain a complete validation on the usefulness and viability of the PQEM method.

3.4. Research Contributions

The main contributions of PQEM is five-fold:

i) we have built a product evaluation method that includes quality characteristics as defined by ISO/IEC 25010 [2];
ii) we have extended the use of testing coverage to define quality characteristics coverage, and product coverage;
iii) we have defined an aggregation measure that allows for a fine-grained analysis of the results;
iv) we have extended the acceptance criteria for functional and non-functional requirements;
v) we have synthesized the functional and non-functional requirements on a number that represents the quality level of a product.

3.5. Research Rigor

The method connects software quality evaluation and non-functional requirements, two areas of research that have a long history in contributing to each other's development. Also, the method is grounded on solid achievements from two disciplines, on the one hand, Goal-Question-Metric [3,17] has been empirically validated in many case studies, and demonstrated its worth in studies on requirements. On the other hand, the PQEM method has foundations on the ISO/IEC 25010 [2] standard which set the baseline of quality measurements and quality characteristics.

3.6. Design as a Search Process

We have defined the PQEM method, the validation has been done with small mobile and web applications, the design and development process of an automated tool based on PQEM has been started, we will seek to validate this tool with a case study on an industrial setting, and finally, we are defining an automated framework that will allow the practical implementation of PQEM, and it might also be used for the implementation of product quality measurement or quality model processes not restrictive to software. Each of these steps generates useful feedback to improve and optimize what has been proposed. Considering that source code metrics are essential and they allow us to set grounds about the quality characteristics measured by the metrics, the automated tool will be able to integrate different automated tools that measure quality attributes in order to obtain a full quality analysis of each software product analysed; for example: SonarQube [18].

3.7. Communication of Research

Technology-oriented audiences are provided with sufficient detail to enable them to be able to replicate each step of the PQEM method. Also, the management-oriented audiences are able to understand whether the organizational resources should be committed to using the method within their specific organizational context. Our main goal is to promote the free software project as well as case studies in the industry.

4. PRODUCT QUALITY EVALUATION METHOD (PQEM)

This section describes the PQEM steps which are the following: **S1)** product setup, **S2)** elicitation, **S3)** measurement, **S4)** results and **S5)** assessment, as shown in Figure 1. It is worth mentioning that the first step (called product setup) should be performed only once, but steps 2 to 5 should be repeated per each iteration for any software product. The latter would lead to a fully functional software product or application to be deployed to customers.

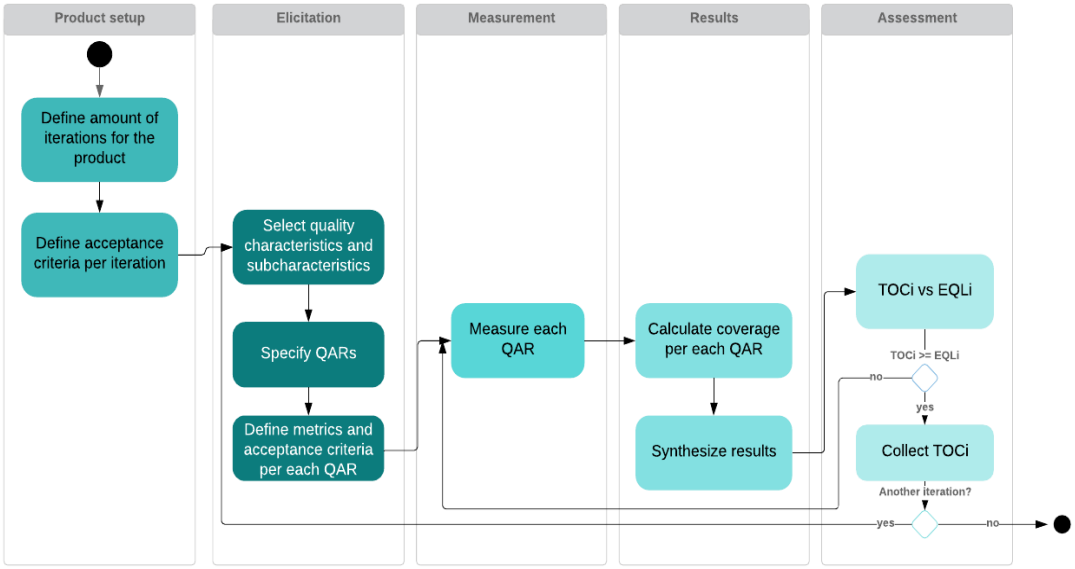


Figure 1. Describing PQEM through an activity diagram.

4.1. Step 1: Product Setup

The first step of PQEM includes the definition of the amount of iterations that the software product is expected to achieved, as well as the characterization and rationale of the acceptance criteria for the expected quality level per iteration EQL_i, which can be different and incremental from the first one to the last one [19]. The latter is a key point because the acceptance criteria advocates understanding how well the quality for each goal is achieved, allowing a glimpse of the entire product quality, within each iteration.

In this way, the acceptance criteria is defined by the stakeholders, and it is a positive number that can take any value between 0 and 1. For example, if you consider three iterations for a software product, then it can be defined an acceptance criteria of 0.70, 0.80, and 0.90, respectively per each of the three iterations. Based on the previous values, it is possible to see that in this example it is expected to achieve an improvement in quality as the product grows in functionality. Later on, it is feasible to comprehend that 1 is the best and strictest value of the acceptance criteria, which means that all quality attributes requirements have passed the measurement; while 0 equates to all QARs did not pass. Another point in consideration is that PQEM is a five-step method, but per iteration only four steps are repeated (from Step 2 to Step 5).

4.2. Step 2: Elicitation of Quality Attributes Requirements (QARs)

Nowadays, system engineering is crucial in the industry, and requirements engineering is an important stage of that overall process, where a proper process can generate not only efficiently but rapidly new products [20]. We have conducted this elicitation process through the Goal-Question-Metric approach [3], and so **Step 2.1** will approach the conceptual level with the definition of goals (considering the structure defined in [17], composed of purpose, issue, object, and viewpoint); **Step 2.2** will include the operational level with the specification of the questions by goal, and finally, **Step 2.3** will specify the quantitative level, defining the metrics by question. Note that Step 2 should be validated by the stakeholders.

4.2.1. Step 2.1: Select quality characteristics and sub-characteristics

ISO/IEC 25010:2011 [2] describes the quality model as the cornerstone of a product quality evaluation system, and this standard determines which quality characteristics will be taken into account when evaluating a software product. The product quality model comprises the following quality characteristics: Functional Suitability, Performance Efficiency, Compatibility, Usability, Reliability, Security, Maintainability, and Portability. As explained by Estdale & Georgiadou [21], the standard ISO/IEC 25010 provides a huge contribution to establish the delivery performance of different software processes. Regarding PQEM, all of the quality characteristics and their sub-characteristics can be selected by the stakeholders; and considering that each characteristic is mapped with a goal, it is defined by the purpose, issue, object and viewpoint per selected characteristic.

4.2.2. Step 2.2: Specify Quality Attributes Requirements (QARs)

Bass et al. [6] explained that the requirements of a system originate from different sources and forms, like functional, quality attributes and constants. Regarding Step 2.1, the QARs for each of the quality characteristics are now specified by the stakeholder and the development team. These QARs are the questions defined for each of the goals, and for example, in the context of Performance Efficiency a QAR can be defined as: *"How fast is the sensor notification in case of disconnection?"*, or for Interoperability: *"Does the system allows to capture and display data from wireless sensors?"* [22].

4.2.3. Step 2.3: Define Metrics and Acceptance Criteria per each Quality Attribute Requirement (QAR)

In this sub-step, the metrics are defined, and they will provide the necessary information to answer the questions defined in Step 2.2. By defining the limits and parameters of a user story or functionality, and determining when a story is complete and functioning as expected, it is possible to specify an acceptance criteria containing conditions that a software product must satisfy in order to be accepted by the stakeholder [23]. Acceptance criteria are also discussed when defining what requirements must be met in each incremental version of a software product [6]. In this context, we sought to extend these concepts for each of the quality measures in order to determine if this measured value was met or not, addressing not only functionalities, but also quality characteristics. As such, the acceptance criteria possess a unique importance due to the fact that through its definition it is possible to objectively know whether each QAR is present or not, as well as obtain the TOC value based on the QARs coverage, which can be disaggregated per quality characteristic. Each quality measure requires some acceptance criteria in order to be useful and complete.

4.3. Step 3: Measure and Test each Quality Attribute Requirement (QAR)

This step involves the measurement of each question, executing the defined quality measure, and describing whether the acceptance criteria was met (1 as passed) or not (0 as failed). In the case of Usability, the measurement binds the responses of the number of users who were part of the Usability test. The final value of each test question will be obtained from the application of Equation (6) and (7), which promote the unification of the total number of answers per respondent, for each of the defined questions; allowing later to compute the measurement.

4.4. Step 4: Collect and Synthesize Results

Regarding the evaluation method, we have based our equations on the concept of testing coverage to derive coverage for the different quality characteristics, and the total coverage of QARs per iteration. Based on the foregoing, Equations (1) to (5) describe the calculations needed to compute the quality level of a software product on each iteration.

$$OC_{qi} = p_{qi} / r_{qi} \quad (1)$$

$$EC_{qi} = rq_i / t_i \quad (2)$$

$$O_vCq_i = pq_i / T_i \quad (3)$$

$$TEC_i = \Sigma_{(1 \text{ to } n)} EC_{qi} \quad (4)$$

$$TOC_i = \Sigma_{(1 \text{ to } n)} O_vC_{qi} \quad (5)$$

where:

- *q* identified each quality characteristic,
- *i* identifies each iteration,
- *n* is the number of quality characteristics defined,
- OC_{qi} is the obtained coverage per quality characteristic for each iteration,
- p_{qi} is the number of passed QARs per quality characteristic for each iteration,
- r_{qi} is the number of QARs per quality characteristic for each iteration,
- EC_{qi} is the expected coverage per quality characteristic per iteration,
- T_i is the total number of QARs per iteration,
- OvC_{qi} is the overall coverage per quality characteristic per iteration,
- TEC_i is the total expected coverage per iteration (which its maximum value is 1),
- TOC_i is the total obtained coverage of QARs per iteration.

TOC_i is a multidimensional value, because it summarizes the obtained quality level of all quality characteristics and sub-characteristics. For each QAR corresponding to Usability, z answers will be obtained according to the number of participants that perform the Usability test. With respect to Usability, each QAR is analysed as follows:

A. It is necessary to unify the z answers from the Usability test that were different from 0 and 1 to become 0 or 1, for example those being a qualitative value like low, very low, medium or high can be unified defining a criterion that all those answers with low and very low will be considered as passed (1) and medium and high as failed (0).

B. Then, all of the values (0s and 1s) for each QAR are summarized, and it is obtained the number that represents the passed QARs.

C. Later on, the coverage per QAR is calculated with Equation (6), where *x* is each QAR.

$$UC_x = pa_x / re_x \quad (6)$$

Where:

- UC_x is the Usability coverage per QAR,
- pa_x is the number of passed answers per QAR,
- re_x is the number of respondents.

If the value obtained with Equation (6) is lower than 0.5 then it is considered as failed, passed otherwise, obtaining the value p_{qi} for Usability; as the sum of the passed values.

D) Finally, once p_{qi} is calculated, it is possible to compute the coverage for Usability itself with Equation (1) and (3); and carry on with the calculations in order to obtain the TOC_i value, through Equation (5).

4.5. Step 5: Assessment of the Product Quality Level

It is possible to perform the analysis of the quality level obtained by means of Equation (5), and the comparison with EQL_i defined by Step 3. In this line, there are two possibilities: following Fig. 1, if TOC_i is bigger or the same to the EQL_i value, then it is possible to collect the TOC_i value. If there is another iteration, the elicitation step will begin. If there is no other iteration, then the process stops. Now, if TOC_i is lower to the EQL_i value, then a new measurement is needed in order to achieve at least the EQL_i value.

4.5.1. Step 5.1: Collect Measurement

Once, the previously defined Equations per each iteration are computed, it is necessary to collect the results to understand the product quality level. As such, Equation (6) allows to construct Equation (7) which contains the list of TOC_i values obtained by iteration $i = (1, 2, ..., y)$. It is worth mentioning that when TOC_i is equal to or bigger of EQL_i (the expected quality level) the collection is carried out.

$$TOC_{product} = \{TOC_1, TOC_2, ..., TOC_y\} \quad (7)$$

4.5.2. Step 5.2: Decision and Control

Once all the measurements from Step 4 are done, the TOC*i* value obtained for the current iteration will be compared to the expected quality level (EQL*i*). On the one hand, if the TOC*i* value is lower than the defined EQL*i* value, then it is necessary to return to the measurement step, which requires solving the QARs that are not existing in development. In this step, if there is another measurement, and it end up being equal or exceed the EQL_i defined for that iteration, it is possible to continue with the next one. On the other hand, if the obtained TOC value is greater than the EQL_i value, then the next iteration may begin, going back to Step 2.1.

5. AN ILLUSTRATIVE APPLICATION OF PQEM

We will present an illustrative application of the PQEM method, in order to help non-technical staff to understand the steps and the related costs to conduct the measurement.

5.1. Step 5: Main Goal and Context

Our case study aims to address the implementation of the proposed evaluation method to a mobile and web application, which is the second iteration of a previous developed app, called HeartCare [5] whose main goal is to ensure that the recovery of cardiac patients can take place in an environment outside hospitals. HeartCare was analysed with the evaluation method, and obtained a quality level of 0.775. The architecture of this second iteration is based on the layered design principle, and takes into consideration the need to develop separate modules which can evolve independently.

One of these modules is responsible for managing the heart rate sensor. This device helps the patient monitor their heart condition while he or she is in rest position, or while performing a physical exercise, through a mobile device. The back was implemented with Spring, while the

web version is implemented with Angular and the mobile version with React native. The literature describes similar examples to the second iteration of HeartCare [24,25].

5.1.1. Step 1: Product Setup

With respect to the application, three iterations were defined [5]. And, according to the stakeholder, the first iteration called HeartCare were set with a 0.70 acceptance criteria, the second one with 0.70 as well, and the third one and final will have a 0.80 acceptance criteria, which is being currently developed.

5.1.2. Step 2: Elicitation of Quality Attributes Requirements (QARs)

The quality characteristics, questions, metrics and acceptance criteria as well as the results are stored in a structured artifact (spreadsheet), as shown in Table 1. The ID column allows to identify and quickly group each row by quality characteristic, followed by the QAR, the metric and the acceptance criteria. Finally, the Result column contains the result of the measurement made per row for all QARs (1 passed, 0 failed).

Table 1. Artifact to store data. Example for Fault-Tolerance.

ID	Quality characteristic	Question	Metric	Acceptance criteria	Result
13	Fault-tolerance	Are the amount of crashes under control?	Number of crashes	Number should be less than 10	Passed
14	Fault-tolerance	Are the amount of hangs under control?	Number of hangs	Number should be less than 10	Passed
15	Fault-tolerance	Are the amount of functionality incorrect responses under control?	Number of functionality incorrect responses	Number should be less than 15	Passed
16	Fault-tolerance	Are the amount of updates requiring restart under control?	Number of updates requiring restart under control	Number should be less than 4	Passed
17	Fault-tolerance	Are the amount of incompatibility errors under control?	Number of incompatibility errors	Number should be less than 4	Passed

5.1.2.1. Step 2.1: Select Quality Characteristics and Sub-Characteristics

Based on the needs of stakeholders, the following characteristics and sub-characteristics from ISO/IEC 25010 [2] have been selected: (a) Functional Suitability: Functional Completeness, Functional Correctness; (b) Performance Efficiency: Time Behaviour, Resource Utilization, Capacity; (c) Compatibility: Interoperability; (d) Usability; (e) Reliability: Availability, Recoverability, Fault-tolerance; (f) Security: Confidentiality, Integrity, Authenticity; (g) Maintainability: Modifiability, Testability; and (h) Portability. These QAs were selected considering the previous iteration of the application called HeartCare and the new requirements defined by the stakeholders, in the context of the second iteration of the app.

In this context, only one goal will be presented to achieve the traceability of the steps, but it is convenient to emphasize that the specific goals of all the quality characteristics have been specified. Instantiating the GQM approach, the goal for Reliability is analyse the delivered product and development process for the purpose of understanding, with respect to reliability and its causes, from the viewpoint of the project manager and user, in the context of the second iteration. It is important to mention that the following subsections will use Fault-Tolerance as the quality sub-characteristic to show each step of PQEM, which is part of Reliability.

5.1.2.2. Step 2.2: Specify Quality Attributes Requirements (QARs)

Considering the goal, one of the questions that arises for Fault-Tolerance is: *Are the amount of crashes under control?* as shown in Fig. 2. The full set of QARs by quality characteristic leads to obtain the list of aspects that need to be study in the software product.

5.1.2.3. Step 2.3: Define Metrics and Acceptance Criteria per each Quality Attribute Requirement (QAR)

Based on the previous QAR and following Fig. 2, it is necessary to define the metric and the acceptance criteria; consequently, it is possible to explicit the following metric: *Number of crashes*, and acceptance criteria: *Less than 10 crashes*.

5.1.3. Step 3: Measure and Test each Quality Attribute Requirement (QAR)

In order to fulfil the Result column in Fig. 2, an analysis was carried out to identify whether each QAR were part or not in the iteration under measure. For example, the row with ID 17 shown in Fig. 2 ask whether the amount of incompatibility errors is under control in the application. As such, some tests were carried out to count the incompatibility errors within the web version, the mobile version and the sensor. Only one compatibility error was found, and so this QAR was set as passed. This same procedure was performed for all the QARs.

5.1.4. Step 4: Collect and Synthesize Results

At this point, it is necessary to calculate the coverage for each of the defined quality characteristics. Following the example, Equation (1) allows calculating the coverage value for Fault-Tolerance which gives $OC_{q2} = p_{q2}/r_{q2} = 5/5 = 1$, being $i = 2$ as we are considering the second iteration of the application. It is worth mentioning that within Usability, each QAR was answered by ten respondents, who gave their perspective of the functioning and design of the web and mobile version of the second iteration of HeartCare.

Equation (6) and (7) allowed the unification of the Usability answers, obtaining a single value to represent the result per each Usability QAR. Once the results from Equation (6) and p_{qi} were obtained; Equations (1) to (4) were calculated for all of the characteristics, and therefore completing Table 2, obtaining by means of Equation (5) a TOC_2 value of 0.90.

Table 2. Summary of results from the application of PQEM to the second iteration of the web and mobile app.

Quality characteristic	r_{q2}	p_{q2}	OC_{q2}	EC_{q2}	O_vC_{q2}
Availability	12	10	0.83	0.005	0.04
Fault-Tolerance	5	5	1	0.02	0.02
Recoverability	7	5	0.71	0.03	0.02
Functional Suitability	59	56	0.95	0.23	0.22
Interoperability	6	4	0.67	0.02	0.02
Modifiability	59	59	1	0.23	0.23
Security	17	15	0.88	0.07	0.06
Usability	64	58	0.91	0.25	0.22
Portability	10	8	0.80	0.04	0.03
Total	**258**	**233**		**$TEC_2 = 1$**	**$TOC_2 = 0.90$**

5.1.5. Step 5: Assessment of the Product Quality Level

The assessment itself addresses the analysis of the value obtained by the Equation (5) based on the previous calculation of the coverage of all quality characteristics. In this case, an acceptance criteria was defined in 0.70; and following Table 2, the quality level TOC_i for the second iteration

was 0.90. As can be seen, the quality level TOC_i not only reached but also exceeded the defined acceptance criteria (0.70). As such, when compared with the TOC_i value obtained for the previous iteration, the application reached the acceptance criteria without an outstanding difference (only with 0.075) and with a bigger technical debt [26].

When analysing each of the quality characteristics shown in Table 2, it is possible to understand that none of them achieve a huge difference between the expected and the obtained coverage. But the small differences are those QARs that should be focused on the next iteration; and can be considered as the technical debt [21].

5.1.5.1. Step 5.1: Collect Measurement

Based on Equation (5), it is possible to obtain that Equation (7) gives the following result: $TOC_{product} = \{0.775; 0.90\}$.

5.1.5.2. Step 5.2: Decision and Control

In this context, and due to the fact that the TOC_i value was bigger than the EQL_i defined, then it is possible to continue to the next iteration.

6. DISCUSSION

Based on recent literature, some authors have presented different ways of studying a software product (mainly its architecture) and its quality attributes, reaching also to the measurement of quality measures. But the main issue nowadays, is that whether the practitioners are able to properly identify the quality level of each defined iteration from a software product. In this context, PQEM is a five-step method that can be used to measure the quality level of each iteration within the life cycle of a software product, understanding and giving a numerical value (TOC_i) to how well the set of quality characteristics are represented within the product. PQEM embedded ISO/IEC 25010 [2], the Goal-Question-Metric approach to perform the elicitation process, and the extension of the testing coverage for a set of quality characteristics.

The latter is another highlight, which allowed defining the coverage for each quality attribute in each iteration. These coverage values have been calculated in first place for TOC_1, the first iteration of the application, which gave a value of 0.775. The estimated value was set on 0.70, so it is possible to say that the quality level was achieved. Now, the TOC_2 value, that it was defined to be equal to or exceeds 0.70; and after applying PQEM it was obtained a coverage of 0.90, from which it can be understood that the iteration can still improve by about 10 percent, considered as technical debt [26].

From these values it is feasible to understand the evolution of the product, where the rise of the TOC value is due to a quality increase, by adding QARs and desegregating even more the chosen quality characteristics and sub-characteristics. The first iteration of the application measured 7 quality characteristics with 138 QARs in total, while the second iteration analysed and measured 10 quality characteristics with 258 QARs. There was a need to update all of the QARs due to some changes within the architecture from one iteration to the other, also we added Fault-Tolerance, Recoverability, and Portability in order to increase the quality. Subsequently, it is important to monitor the changes from one iteration to the other in order to produce a full quality analysis. It is worth mentioning that the measurement of the third iteration is currently in progress.

With respect to validity threats [27], within construct validity, it is necessary to ask whether the quality level really represents the quality of the product. In response, the quality level is an aggregated value based on the full set of QARs, where the selection of each QAR were validated with stakeholders, so we considered that is not necessary to validate the value obtained per se. PQEM presents the evaluation of a system in one number. By doing so, it assumes that all quality requirements are equally important. However, it may be the case (and in reality it is often so) that the violation of a single requirement may result in an unusable product.

This drawback will be contained in future work which includes the generalization of PQEM where it will contain the definition of a set of weights which will allow to pondering each quality characteristic. This generalization will be included on a software tool that represents the automated version of the PQEM method; and it will also provide an interface to connect to another existing quality measurement tools like SonarQube and Jenkins [28]. Likewise, not only will the importance of quality characteristics be included in addition to weights, also addressing the mandatory nature of certain characteristics in the software product under evaluation. Even though it might seem small the amount of selected quality characteristics, we believe that the community is well aware of the goodness and scientific reachability of the ISO/IEC 25010 [2].

Also, the initial definition of QARs as well as whether to include all of them or just a few may distort the evolution of the product quality level, due to the fact that the TOC value is obtained as the sum of the quality coverages of each quality characteristic. It must not be forgotten that the QARs are almost always related to the application domain. For example, the second iteration of the web and mobile application [5] being measured is embedded within the healthcare sector, while helping patients ensure their cardiac recovery. This relationship with the domain impact on the definition and selection of the QARs because some quality characteristics can be more important than others, regarding the viability of the product. In healthcare, if an integration to existing healthcare records is necessary, then the set of QARs for Interoperability might be larger than other non-health related application.

As part of internal validity, it is possible to say that all of those QARs belonging to Usability have a reduced subjectivity due to the number of people involved in the Usability test carried out. Also, subjectivity included in the evaluation of the QARs, when we decided to accept or reject them. But it is worth mentioning that all of them were defined in order for them to be easily verifiable, testable or measurable.

Later on, some parts of PQEM might seem to be extremely dependent on the stakeholders. In its current form without tool support, PQEM it is just a very abstract (albeit very systematic) process that only becomes concrete when it gets to metric aggregation at the end. These conditions will be improved by the creation of a catalogue that includes quality measures and questions in order to decrease the dependency of stakeholders, and increase the practical applicability of PQEM. The latter will be supported by the development of the automated version of the method.

Another question point is whether the number as such is representative for the stakeholders; on which it can be said that the value of that number arises from the entire previous breakdown for all quality characteristics, when synthesizing the breakdown. Therefore, if you need to understand that number it is possible to go through the different levels of aggregation to understand that number in depth.

With respect to external validity, it might seem that the validation of the method is performed on a relatively small case where the system might seem small and with no applicability to industrial practice. But, actually, the application possesses several actual characteristics such as concurrency, web and mobile version, use of sensors, healthcare domain, need for high

availability, among others. Also, mobile applications are becoming complex software systems that must be developed quickly and evolve continuously to fit new user requirements and execution contexts [29].

All of these characteristics realize the need to applied the method in order to analyse the quality level of the second iteration of HeartCare, due to the need of understanding how well was designed and implemented was the application. The future implementation of a software tool to make PQEM accessible as a web will allow to replicate the method more easily, and even increase the external validation.

6.1. Implications for Research and Practice

Regarding the implications of putting the PQEM method into practice, it is feasible to mention that PQEM itself takes time to apply due to the definition and specification of Steps 2 and 3. These steps require in-depth knowledge of the software product to be developed. Therefore, it is time and cost that it is required for its applicability. A product owner will need to understand this scope to map the resources, time and associated costs in order to achieve an effective implementation for each defined iteration; regardless of the type of project.

But considering that, by itself, any process of definition and measurement of quality requires the same considerations, it is therefore necessary to approach it as part of development and not as an aggregate. The quality must go hand in hand with the development of the iterations.

Considering the size of the projects and the teams, the illustrative case shows the feasibility of the application in a small project with two iterations (one prior to this article [5], and the second, the one described above) which was implemented with a team of five developers, a technical leader and a project manager. Therefore, in the example we showed that measurement with PQEM is feasible in small projects for small co-located teams when there is a need for the domain that justifies the addition of time and cost to applied the method. Likewise, the application of the method may not be necessary to justify the cost, if it is considered a complex product or domain or of which it is necessary to ensure a certain level of quality.

Inside an agile environment, the use of PQEM might require more documentation and analysis to the delivery cycle due to the fact that each iteration requires a quality measurement and evaluation. In case a new standard is needed for example the European DGDR standard for privacy [30], what is important to understand is that if it is possible to extract QARs, defining goals and requirements then it is possible to apply PQEM with a different standard; achieving adaptation and flexibility.

In this article, a method was introduced that facilitates the elicitation, measurement and monitoring of QARs, and therefore its application is justified when this represents a company policy, is a requirement of the complexity of the product or domain, or is has assumed to obtain a certain level of quality.

7. CONCLUSIONS

Software engineering principles and quality goals are necessary but not sufficient for the needs of today's marketplace; because exists the necessity of shorter and iterative cycle times, and completed with fewer resources. Establishing the proper metrics to monitor the software project is essential, as well as the requirement that project managers and leaders view the entire and big picture of the development process [27-31]. Therefore, project leaders and product owners need

to understand the level and quality of a software product, intuitively; which facilitates the decision to accept or reject a product.

In this context, the PQEM method [5] is introduced which assess the quality of a product by a single numeric value between 0 and 1. To calculate this value, it uses a GQM-motivated quality model that refines quality goals to quality attribute requirements (question along with a metric and acceptance criteria). The quality evaluation derived from the rate of passed quality attribute requirements.

Also, we presented an illustrative example from the health care sector to demonstrate its applicability. Knowing what to measure is a recurrent problem in a data-driven approaches, using GQM for identifying the quality attributes ensures that the assessment of the product is adapted to the organization applying the proposed method. To achieve the applicability, a quality model should not only be an assessment model but also a usable and intuitive guideline to increase quality [1]. It is possible to visualize the contribution of PQEM as it obviously helped an organization to refine and concretize their (often abstract) quality requirements down to hard, measurable criteria. Consequently, with PQEM the manager can know if the project has quality problems or if the quality level is below the expected; the same as the developer who can know what the points of failure are. As future work, the authors will develop an automated tool of PQEM, and a catalogue that include a set of suggested questions and metrics for the stakeholder to use.

ACKNOWLEDGEMENTS

This work is supported by a research grant from Engineering School, Universidad Austral, Argentina.

REFERENCES

[1] K. Mordal, N. Anquetil, J. Laval, A. Serebrenik, B. Vasilescu, and S. Ducasse. "Software quality metrics aggregation in industry." *Journal of Software:* Evolution and Process 25, no. 10, pp. 1117-1135, 2013.

[2] ISO/IEC 25010 (n.d), https://iso25000.com/index.php/en/iso-25000-standards/iso-25010, Last access: 1/7/2021.

[3] V. R. Basili, Software modeling and measurement: the Goal/Question/Metric paradigm. 1992.

[4] J. A. McCall, P. K. Richards, and G. F. Walters. Factors in software quality. Volume i. concepts and definitions of software quality. General Electronic co. Sunnyvale, CA, 1977.

[5] M. Falco, and G. Robiolo. "*A Unique Value that Synthesizes the Quality Level of a Product Architecture: Outcome of a Quality Attributes Requirements Evaluation Method*." In International Conference on Product-Focused Software Process Improvement, pp. 649-660. Springer, Cham, 2019.

[6] L. Bass, P. Clements, and R. Kazman. Software architecture in practice. Addison-Wesley Professional, 2003.

[7] J. J.Chilenski, and S. P. Miller. "*Applicability of modified condition/decision coverage to software testing*." Software Engineering Journal 9, no. 5 (1994): 193-200.

[8] R. Kazman, M. Klein, and P. Clements. ATAM: Method for architecture evaluation. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2000.

[9] E. Woods. "*Industrial architectural assessment using TARA*", Journal of Systems and Software 85, no. 9, pp. 2034-2047, 2012.

[10] H. Koziolek, D. Domis, T. Goldschmidt, P. Vorst, and R. J. Weiss. "MORPHOSIS: A lightweight method facilitating sustainable software architectures." In 2012 Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture, pp. 253-257. IEEE, 2012.

[11] P. Bengtsson, N. Lassing, J. Bosch, and H. van Vliet. "*Architecture-level modifiability analysis (ALMA)*", Journal of Systems and Software 69, no. 1-2, pp. 129-147, 2004.

[12] S. Sarkar, G. M. Rama, and Avinash C. Kak. "API-based and information-theoretic metrics for measuring the quality of software modularization." IEEE Transactions on Software Engineering 33, no. 1 (2006): 14-32.

[13] A. R. Hevner, S. T. March, J. Park, and S. Ram. "Design science in information systems research." MIS quarterly, pp. 75-105, 2004.

[14] P. Runeson, E. Engström, and M-A Storey. "*The design science paradigm as a frame for empirical software engineering."* In Contemporary empirical methods in software engineering, pp. 127-147. Springer, Cham, 2020.

[15] P. Jain, A. Sharma, and L. Ahuja. "*The Impact of Agile Software Development Process on the Quality of Software Product*." In 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 812-815. IEEE, 2018.

[16] H. R. Neri, and G. Horta Travassos. "*Measuresoftgram: a future vision of software product quality*." In Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, pp. 1-4. 2018.

[17] V. R. Caldiera, G. Basili, and H. Dieter Rombach. "The goal question metric approach." Encyclopedia of software engineering, pp. 528-532, 1994.

[18] A. S. Nuñez-Varela, H. G. Pérez-Gonzalez, F. E. Martínez-Perez, and C. Soubervielle-Montalvo. "Source code metrics: A systematic mapping study." Journal of Systems and Software 128, pp. 164-197, 2017.

[19] Segue Technologies, September 3, 2015, What Characteristics Make Good Agile Acceptance Criteria? https://www.seguetech.com/what-characteristics-make-good-agile-acceptance-criteria/. Last access: 1/7/2021.

[20] J. Dick, E. Hull, and K. Jackson. Requirements engineering. Springer, 2017.

[21] J. Estdale, and E. Georgiadou. "*Applying the ISO/IEC 25010 quality models to software product*." In European Conference on Software Process Improvement, pp. 492-503. Springer, Cham, 2018.

[22] S. Jiménez-Fernández, P. De Toledo, and F. Del Pozo. "*Usability and interoperability in wireless sensor networks for patient telemonitoring in chronic disease management*." IEEE Transactions on Biomedical Engineering 60, no. 12 (2013): 3331-3339.

[23] R. van Solingen, D.M. Rini, and E. W. Berghout. The Goal/Question/Metric Method: a practical guide for quality improvement of software development. McGraw-Hill, 1999.

[24] V. Gay, P. Leijdekkers, and E. Barin. "*A mobile rehabilitation application for the remote monitoring of cardiac patients after a heart attack or a coronary bypass surgery*." In Proceedings of the 2nd international conference on pervasive technologies related to assistive environments, pp. 1-7, 2009.

[25] P. Kakria, N. K. Tripathi, and P. Kitipawang. "*A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors."* International journal of telemedicine and applications, 2015.

[26] Z. Li, P. Avgeriou, and P. Liang. "*A systematic mapping study on technical debt and its management."* Journal of Systems and Software 101 (2015): 193-220.

[27] V. R. Basili, R. W. Selby, and D. H. Hutchens. "Experimentation in software engineering." IEEE Transactions on software engineering 7 (1986): 733-743.

[28] M. Falco, E. Scott, G. Robiolo, “Overview of an Automated Framework to Measure and Track the Quality Level of a Product”, In IEEE ARGENCON 2020, V Biennal Congress of IEEE Argentina Section.

[29] G. Hecht, R. Rouvoy, N. Moha, and L. Duchien. "Detecting antipatterns in android apps." In 2015 2nd ACM international conference on mobile software engineering and systems, pp. 148-149, IEEE, 2015.

[30] European Union, Regulartion 2016/679 of the European Parliament and of the Council. General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN, Last access: 1/7/2021.

[31] R. T. Futrell, L. I. Shafer, and D. F. Shafer. Quality software project management. Prentice Hall PTR, 2001.

AUTHORS

Mariana Falco. PhD in Engineering student. Information System Engineer. She is a teacher within the Engineer School at Universidad Austral (UA), where she also does her research on Software Engineering, Quality Measurement, and Quality Metrics. She collaborates with fellow colleagues on researches related to information technologies applied to different domains. She is part of the LIDTUA Lab (UA) as well as the Research & Development Lab (UA), as a researcher and project manager.

Gabriela Robiolo. PhD in Information Sciences. She is currently a full-time professor at Universidad Austral, within the Engineering School. She is a researcher on Software Engineering, and Quality Measurement, and also she collaborates with other researchers on related topics. She is part of the LIDTUA Lab (UA) as well as the Research & Development Lab (UA), as one of the principal researchers.

A GENERALIZED APPROACH TO DATA SUPPLY CHAIN MANAGEMENT – BALANCING DATA VALUE AND DATA DEBT

Roberto Maranca[1] and Michele Staiano[2]

[1]Data Excellence – Schneider Electrics, UK
[2]Department of Industrial Engineering – University of Napoli Federico II, Italy

ABSTRACT

The "data supply chains" (DSCs), which are connecting the point where physical information is digitized to the point where the data is consumed, are getting longer and more convoluted. Although plenty of frameworks have emerged in the recent past, none of them, in the authors' opinion, have so far provided a robust set of formalised "how to", that would connect a "well built" DSC to a higher likelihood to achieve the expected value. This paper aims at demonstrating: (i) a generalized model of the DSC in its constituent parts (source, target, process, controls), and (ii) a quantification methodology that would link the underlying current quality as well as the legacy "bad data" to the cost or effort of attaining the desired value. Such approach offers a practical and scalable model enabling to restructure at its foundation some practices of data management priming them for the digital challenges of the future.

KEYWORDS

Data Management, Data Supply Chain, Quality, Complexity, Value.

1. INTRODUCTION

In an increasingly digitised world "Data" is becoming crucial for solving the essential challenges that mankind faces in its way forward. The insight or knowledge that derives from the analysis of the digital representation of reality is more and more required in a world whose complexity and interdependencies grow exponentially.

The management of information has become a key constituency for enterprises, and over the years it has pressurized them into developing complete capability made of people, processes, tools and, obviously, data to operationalise its undertaking. The DSCs are clearly an integral part of the creation of value in human activities, in some cases the most important one, and yet the canonical approach to data in private or public enterprises, though innovating at speed with Data Science (sometimes with inflated expectations), is handling such chains in somewhat artisan fashion.

The principal objective for the exploitation of data is to monitor certain activities from a revenue, performance or compliance point of view, and to optimize the input parameters of such activities to pursue an enterprise's strategic objectives of growth, cost containment and risk management, and also more recently of social responsibilities. However, as the catalyst for the set-up of a data capability varied in time and kind from the more appealing (e.g., digital marketing) to the non-negotiable (e.g., supervisory reporting), the consequence is that within the same company, different areas matured their approach to data at different pace and following different models. In

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 73-79, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111105

this multi-speed and siloed approach to data, superimposed generations of technologies, processes and procedures have created convoluted (and surprisingly unchartered) internal avenues of distribution and consumption of data; in this scenario, the combined effect of continuous business changes (e.g. mergers, product development, regulations, leadership turnover) and the decreasing ability to respond to such changes with robust simplifications, owing to the increasingly complex enterprise setting, have been feeding each other creating a *chaotic environment*, in which the proverbial flapping of a butterfly's wings can generate unforeseen and very costly consequences. Facing a looming complexity tipping point of the ever more interdependent DSCs, one has just to look at the increased amount of "data breaches" or "data leaks" or "data flops" or "algorithmic failures" to quantify how close the above mentioned complexity tipping point is. Thus, while the data supply chains, DSCs, are getting longer and longer to fuel digital transformations that are coalescing larger and larger ecosystems of functions, intermediaries, partners, and of course third parties (i.e., customers, prospects, accounts), it has emerged a greater awareness of the need to know the what, the where, the who and the how of the enterprise's data, as a risk reduction factor for those unintended consequences. The "Enterprise Metadata Management" discipline – as the ability of collect, organize, relate and take advantage of a set of descriptors of the data used in the enterprise – has greatly increased its presence in the data stacks and has been overtime significantly extended by the raise of the Semantic of Data, already indispensable for the World Wide Web interoperability. However, the authors are hereby going to demonstrate that a further formalization of the DSCs, that connects the semantic approach to a generalised value base and a quantitative model, can provide the basis for the creation of a stronger causality between the assessment of the *quality* of the information *flowing* in a DSC and the predictable and reliable attainment of the intended value.

2. GENERALISED DATA SUPPLY CHAIN MODEL

The simplest model underpinning a data supply chain can be described as a single sequential path (see also Fig.1) that comprises:

- **i.** a **point of consumption C** where a set of information $\mathbf{D}_i$ – the data elements, $i = 1, \ldots, n$ – is output and *used* (consumed) by an *agent* $\mathbf{A}_j$, the *data consumers* $j = 1, \ldots, k$, to deliver a tangible or intangible value $\mathbf{V}_{ij}$
- **ii.** **a source S** where the set $\mathbf{D}_i$ is extracted with a process $\mathbf{P}_{ie}$ in conformity with a set of requirements $\mathbf{R}_{ij}$, such process is commonly known as *ETL*, Extract Transformation and Load
- **iii.** a quality process $\mathbf{P}_{iq}$ that produces a set of $\mathbf{Q}_{ij}$ measurements for $\mathbf{D}_i$, based on quality requirements imposed by $\mathbf{A}_j$
- **iv.** a visualization process $\mathbf{P}_{iv}$ that allows $\mathbf{A}_j$ to *consume* $\mathbf{D}_i$ and $\mathbf{Q}_{ij}$
- **v.** a set of tolerances $\mathbf{L}_{ij}$ for each $\mathbf{Q}_{ij}$ imposed by $\mathbf{A}_j$ on the basis of which $\mathbf{D}_i$ is accepted or rejected.

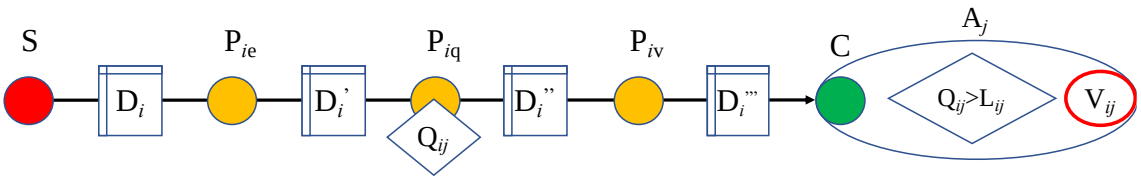


Figure 1. The simplest model for a DSC.

The flow of $\mathbf{D}_i$ is assumed to have a certain cadence **T**, which may vary from a *quasi-real time* – i.e., any time a new set $\mathbf{D}_i$ is available in **S** – to once a day (overnight batches) to *on demand* when $\mathbf{A}_j$ is making a request for the set.

When the flow is established for the first time, it is very likely that the $\mathbf{Q}_{ij}$ could be quite inferior to the level of acceptability, so an "uplift" of quality would be required. Thus, it is useful to express such uplift in a quantitative manner as an amount, $\mathbf{M}_{ij}$, proportional to the measured gap according to the formula $\mathbf{M}_{ij\_} = \mu(\mathbf{Q}_{ij} - \mathbf{L}_{ij})$, where μ is an "issue fixing cost" function. As the sum of all $\mathbf{M}_{ij}$ for all the data sets $\boldsymbol{D}_i$ will constitute the theoretical amount that an enterprise would need to pay to unlock for all the data consumers $\mathbf{A}_j$ the expected $\mathbf{V}_{ij}$ values, we would like to call this the enterprise's ***Data Debt***.

2.1. Simple Data Supply Chain Example

Let's demonstrate with a practical example inspired to a real business situation how the data debt comes into play. A Customer Relationship Management tool is capturing and managing sales opportunities; the enterprise at a time T_0 has got 1000 sales opportunities. An opportunity data set is transferred to Operational Data Store, and it is there consumed by a Sales Director to fine tune their pricing strategy. The pricing strategy has got the obvious intent to increase sales and revenue adjusting the list price for certain specific customers and it is thus based on an internal customer classification. There are 10 different customer classes defined by the enterprise and they are represented by a data element called *customer type,* which would therefore is expected to assume a value between 1 and 10. As the customer type is essential to the action that would derive value from data, it is useful to assign to it the status of *critical data element (CDE)* within the data set. So according to our model above we have (note that, being this simple DSC built against the needs of just one data consumer **A**, in the following we have dropped the second index for the sake of conciseness in the notation):

- $\mathbf{S} = \boldsymbol{CRM}$
- $\mathbf{C} = \boldsymbol{ODS}$
- $\mathbf{A} = \boldsymbol{Sales\ Director}$
- $\mathbf{V} = \boldsymbol{Opportunity(T_1) - Opportunity(T_0) > 0}$
- $\mathbf{D}_1 = \boldsymbol{customer\ type\ for\ each\ opportunity}$
- $\mathbf{P}_{1e} = \boldsymbol{Extracts\ Opportunity\ dataset\ from\ S}$
- $\mathbf{P}_{1q} = \boldsymbol{Execute\ the\ Q_1\ rule\ on\ all\ the\ customer\ types\ contained\ in\ D_1}$
- $\boldsymbol{q_1} = \boldsymbol{value\ output\ of\ the\ Q_1\ rule}$
- $\mathbf{P}_{1v} = \boldsymbol{Displays\ for\ A_1\ the\ list\ of\ customer\ types\ and\ the\ Q_1\ result}$
- $\mathbf{L}_1 = \boldsymbol{acceptance\ level\ is\ 1000}$

For the sake of simplicity, let consider that in this case **A** will be able to achieve its objective if the output value form the sole rule $\mathbf{Q}_1$ is able to satisfy the requisite $\mathbf{L}_1$:

$$\mathbf{Q}_1 \triangleq \{\boldsymbol{q}_1 = \textbf{Count of all records in } \mathbf{D}_1\textbf{: }\text{'customer type'} \in \textbf{[1,2,3,4,5,6,7,8,9,10]}\} \textbf{ is greater or equal to } \mathbf{L}_1$$

However, having checked the 1000 customer types in $\mathbf{D}_1$, it is found that only 800 are valid customer types, so $\mathbf{Q}_1 = 800$. It is important to note that in this case one is not checking whether the customer type is "accurate", i.e., it is exact customer type given the customer is referred to, but the rule only checks whether the customer type is valid, therefore the pricing A_1 will implement would be consistent with the pricing policies but not necessarily yielding the expected result if the customer had been mislabelled with the *wrong* customer type. In any case, for this

case, the Data Debt would be $\mathbf{M_1} = \mu(200)$ as 200 are the *issues* affecting the data set as per the rule $\mathbf{Q_1}$; since in the vast majority of cases the cost to fix a single issue can be expressed as a function of time spent by an employee to access and amend the single Customer Type. Let's say that per acquired experience and for the sake of the exercise, the enterprise expects the typical Data Steward to take 30mins to fix one customer type, with a typical hourly rate of 30€/hr, the function $\mu(\cdot)$ is reduced to constant coefficient m_1 that, for our example, yields:

$$\mathbf{M_1} = 200 \times m_1 = 200 \times (0.5\text{h} \times 30€/\text{h}) = 3000€$$

Thus, whatever expectation **A** had of the **value** generated by pricing an opportunity based on customer type, they should add 3000€ of data debt to their cost benefit analysis.

Although this is an extremely simplified case under almost "aseptic" laboratory conditions, the $\mathbf{M_1}$ still constitute a powerful quantification of a *cost* hurdle the DSC has to overcome to start positively to contribute to the bottom-line of the company. Furthermore, as finance and operation functions are getting more proficient in detailing their costs at activity level (as per activity-based costing, ABC), there is an ideal synergy in including data debt considerations in those frameworks.

3. CONNECTING DATA SUPPLY CHAIN COSTS AND VALUE CHAINS

On the other hand, the more the downstream value creation mechanism is known and the finer the $\mathbf{L_{ij}}$ requirements can be set to optimize the acceptable reduction of $\mathbf{V_i}$ in presence of a greater $\mathbf{M_i}$ carried over: in fact, once the model of a DSC has been defined and the different $\mathbf{M_{ij}}$ have been calculated, the logical next step is to optimize the efforts in data debt reduction to unlock value faster. To this end, let us slightly modify a chart commonly used in stock analysis, a cost/value chart, to look at the relationship between the cost to carry out the establishing of the DSC and improving its data standards, and the value seen from the perspective of the agent $\mathbf{A_j}$.

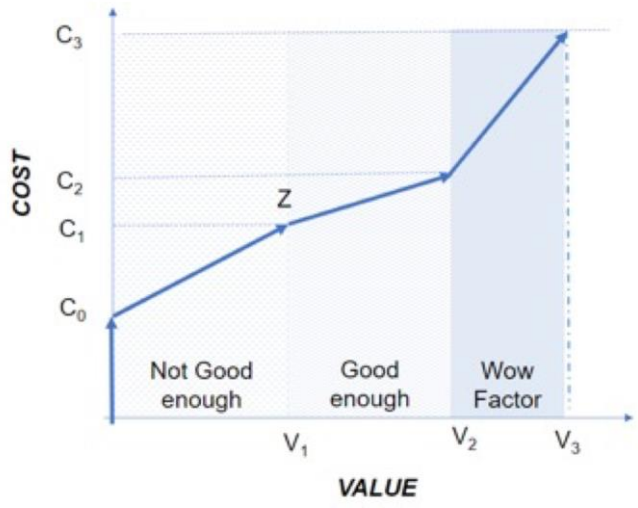


Figure 2. The modified stock chart.

A first initial cost will be required to set up the infrastructure, the process, and the organization to operate the DSC; let denote that cost C_0 and assume it constant for now (i.e., there are no running costs). Obviously, for the agent no value is available at this point in time ($V_0 = 0$), then we could assume that data is starting to flow in the DSC and, especially if working with agile

methodologies, very well suiting data, some initial value could be measured, in fact some call this phase "Proof of Value" (POV). In reality, and as per the model, until the point where all the *essential* $\boldsymbol{L_{ij}}$ are satisfied is reached, the DSC is not *good enough* to be *operational* – i.e., to be used in a live business environment to generate value. The point Z, which it is in effect the MVP (minimum viable product) for the DSC, it is identified now as the point where V_1 is achieved at a cost C_1, with C_1 the cost incurred to set up the DSC and to repay the data debt linked to the *minimum consumption requirements.*

What are then these minimum requirements? The expression of $\mathbf{Q_{ij}}$ rules is commonly done using a taxonomy of data quality dimensions as a reference (e.g., completeness, validity, etc.), however rather than picking one it is preferrable to further classify such dimensions in a value generating optic that could marry much more the agent **A**'s view of quality. So in line with the assumption that data should be more and more treated as a product, we could borrow an approach to quality based on customer satisfaction, and the Kano's model comes handy for simplifying the approach to define the minimum consumption requirement and selecting the $\mathbf{Q_{ij}}$ rules that are instrumental in reaching that point/level. Using the Kano definition *of must-be, one dimensional and attractive* the total cost C_1, proportional to the sum of data debts, $\Sigma\mathbf{M_{ij}}$, in the $\boldsymbol{D_i}$, can now be expressed as:

$$C_T = C_0 + C_1 + C_2 + C_3$$

But if we now assume that the three costs are in fact associated to the debt to repay for the fulfilment of must be quality level (= reaching the minimal fitness for consumption), the saturation of one-dimensional quality (= attaining the expected capability) and the achievement of an attractive level (= hitting unspoken needs about data so increasing its value), respectively, then in terms of data debt the formula could be written as:

$$C_T = C_0 + \sum_{i=1}^{n} (M_i^m + M_i^o + M_i^a)$$

which, in the case of MVP as the one where the must be rules about basic/critical requirements ought to be satisfied, becomes:

$$C_T = C_0 + \sum_{i=1}^{n} M_i^m$$

Remarkably the objective of achieving value at the lowest cost can be now visualized geometrically as the reduction of the angle that the segment ending in the point Z measures with the Value axis. The geometry is indeed highlighting a proportion between partial derivatives:

$$\partial C/\partial V \propto \partial C/\partial M$$

where a decrease of Data debt will produce to a proportional increase of the value:

$$dV \propto -dM$$

More pragmatically, from the formula above it is easy to gather that a lower C_1 is achieved with a higher maturity of the Data capabilities of the enterprise. Specifically, this entiles:

- **Lower set up costs (C_0)**:

    a. **Agile Architecture** achieves efficient and rapid instantiation of the DSC
    b. **Robust Delivery Methodology** increases firs time right outcome and minimize resource waste

   c. **Data Productization** creates reusable information products to quickly enable consumption

- **Reduced data debt ($\Sigma \mathbf{M}_i$)**:
   a. **Active Data Monitoring** capitalizes on previous data debt reduction exercise to keep the target achieved
   b. **Robust Change Control** provides sustainability, so that endogenous (e.g. org changes) or exogenous (e.g. acquisitions) changes are not adversely affecting the quality and integrity of the data

It is worth to highlight, and can be proven, that the additional efforts required to move from *must be* quality (the one related to a minimum viable product) to satisfy *one dimensional* needs are usually comparatively less costly than the former (as the less steep segment between V_1 and V_2 depicts) at least until they cross the line of the *unspoken* needs. In the proposed model these circumstances depend, accordingly to the Kano's theory of attractive quality, on the different quality dimensions that matter in a path toward data excellence. Once the V_2 point is reached by *saturating* the quality standards of the data set, additional unexpected value could only be supplied by increasing quality in a fashion not previously envisioned by the customer themselves, i.e., by capturing a deeper understanding of **A**'s *value chains* to be able to reflect it in the data supply ones. Practically speaking, that would imply that a previously not supplied data element is identified to be beneficial to increase the value, thus changing the DSC structure, and although that would require extra cost for the provider, it could be presented to the agent **A** as a value adding service and afforded in delta value sharing model, that in turn would reinforce the data consumer trust and satisfaction.

4. CONCLUSIONS

The case for a formalized modelling of Data Supply Chains has been introduced, its aim is to create a modular approach that could tackle the complexity tipping point of modern digital enterprises. A causality linkage between the desired outcome of the Data Consumer and the underline status quo of the available data has also been introduced. The concept of Data Debt has been defined as a versatile quantity to gauge the benefit deriving from the DSC itself. A simple example of a practical application of the concept has been provided, drawing a parallel between a quality appreciation model (Kano's) and an optimized approach to converge to minimum value from DSC in an accelerated fashion. Most importantly the introduction of a Cost/Value model has allowed to firmly correlate the quantification of data debt to existing nomenclature of phases (POC, MPV, etc.) adopted in the development of DSCs, phases which are now identified to specific level of debt reductions.

ACKNOWLEDGEMENTS

The authors are grateful to the organizers of a talk addressed to the students of the Master in Data Science administered by University of Naples Federico II for incentivising them to further develop the key ideas behind this paper.

REFERENCES

[1] Ballou, D., Wang, R., Pazer, H., & Tayi, G. K. (1998) "Modeling information manufacturing systems to determine information product quality", *Manage. Sci*., Vol. 44, No. 4, pp462–484.

[2] Batini, C., Cappiello, C., Francalanci, C., & Maurino, A. (2009) "Methodologies for data quality assessment and improvement", *ACM Comput. Surv*., Vol. 41, No. 3, pp1-52.

[3] Erto, P., Vanacore, A., & Staiano, M. (2011). "A service quality map based on Kano's theory of attractive quality", *TQM Journal*, Vol. 23, No. 2, pp196-215.

[4] Houhamdi, Z., & Athamena, B. (2019) "Impacts of information quality on decision-making", *Glob2l Bus. Econ. Rev.*, Vol. 21, No. 1, pp26–42.
[5] Kano, N., Seraku, N., Takahashi, F., & Tsjui, S., (1984) "Attractive quality and must-be quality", *Hinshitsu*, Vol. 14, No. 2, pp147-56.
[6] Li, A., Zhang, L., Qian, J., Xiao, X., Li, X.-Y., & Xie, Y. (2019) "TODQA: Efficient Task-Oriented Data Quality Assessment", *Proceedings of 2019 15th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN). IEEE*, pp81-88
[7] Petrakos, G., Conversano, C., Farmakis, G., Mola, F., Siciliano, R., & Stavropoulos, P. (2004). "New ways of specifying data edits", *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, Vol. 167, No. 2, pp249–274.
[8] Silvola, R., Harkonen, J., Vilppola, O., Kropsu-Vehkapera, H., & Haapasalo, H. (2016) "Data quality assessment and improvement", *Int. J. Bus. Inf. Syst.*, Vol. 22, No. 1, pp62–81.
[9] Batini, C. & Scannapieca M.(2006) *Data Quality – Concepts, Methodologies and Techniques*. Springer, Berlin, Heidelberg.

AUTHORS

Roberto Maranca, during more than 25 years of experience in the world of IT and Data, has spent most his working life with General Electric in their Capital Division, where, since 2014 as Chief Data Officer for their International Unit he has implemented Data Governance, Data Quality and Advanced Analytics, spanning from supporting risk model validation to enabling divestitures and leading their regulatory reporting initiatives. After a year as Group Chief Data Officer at Lloyds Banking Group, shaping a new Data Strategy and dividing his time between the BCBS 239 and GDPR programs, he has joined Schneider Electric as Data Excellence VP delving into the cultural and methodological aspects of becoming a data driven company. Roberto Maranca has got a Master's Degree in Aeronautical Engineering from Federico II Naples University.

Michele Staiano is a senior researcher in Statistics, Technology and Analysis of Data, STAD, in the Department of Industrial Engineering at University of Napoli Federico II. He has lectured probability, statistics, fundamentals of reliability and innovation courses, and recently developed statistical protocols for Multi-Scale Integrated Analysis of Societal and Ecosystem Metabolism which contributes to integrated research and whole system-level evaluation of sustainability of energy, water, land, food and economies. Currently he is serving as tutor for many students with backgrounds in engineering as well as economics, aiming at helping them to develop actionable data science applications. Michele Staiano holds a Master's Degree in Aeronautical Engineering and a PhD in Computational Statistics and Applications, both received from Federico II Naples University.

APPRAISAL STUDY OF SIMILARITY-BASED AND EMBEDDING-BASED LINK PREDICTION METHODS ON GRAPHS

Md Kamrul Islam, Sabeur Aridhi and Malika Smail-Tabbone

Universite de Lorraine, CNRS, Inria, LORIA, 54000 Nancy, France

ABSTRACT

The task of inferring missing links or predicting future ones in a graph based on its current structure is referred to as link prediction. Link prediction methods that are based on pairwise node similarity are well-established approaches in the literature and show good prediction performance in many real-world graphs though they are heuristic. On the other hand, graph embedding approaches learn low-dimensional representation of nodes in graph and are capable of capturing inherent graph features, and thus support the subsequent link prediction task in graph. This appraisal paper studies a selection of methods from both categories on several benchmark (homogeneous) graphs with different properties from various domains. Beyond the intra and inter category comparison of the performances of the methods our aim is also to uncover interesting connections between Graph Neural Network(GNN)-based methods and heuristic ones as a means to alleviate the black-box well-known limitation.

KEYWORDS

Link Prediction, Graph Neural Network, Homogeneous Graph & Node Embedding.

1. INTRODUCTION

One of the most interesting and long-standing problems in the field of graph mining is link prediction that predicts the probability of a link between two unconnected nodes based on available information in the current graph such as node attributes or graph structure [1].The prediction of missing or potential links helps us toward the deep understanding of structure, evolution and functions of real-world complex graphs [2]. Some applications of link prediction include friend recommendation in social networks [3], product recommendation in e-commerce [4], and knowledge graph completion [5].

A large category of link prediction methods is based on some heuristics that measure the proximity between nodes to predict whether they are likely to have a link. Though these heuristics can predict links with high accuracy in many graphs, they lack universal applicability to any kind of graphs. For example, the common neighbor heuristic assumes that two nodes are more likely to connect if they have many common neighbors. This assumption may be correct in social networks, but is shown to fail in protein-protein interaction (PPI) networks [6]. In case of using these heuristics, it is required to manually choose different heuristics for different graphs based on prior beliefs or rich expertise.

On the other hand, machine learning methods have shown their impressive performance in many real-world applications like image classification, natural language processing etc. The built models assume that the input data is represented as independent vectors in a vector space. This

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 81-92, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111106

assumption is no longer applicable for graph data as graph is a non-Euclidean structure and the nodes in a graph are linked to some other nodes [7]. To overcome this limitation, a lot of efforts have been devoted to develop novel graph embeddings where the nodes, edges, graphs are represented in a low-dimensional vector space. In last decade, graph embedding has been established as a popular supporting tool for solving several analytical problems in graphs like node classification, node clustering, link prediction. The embedding approaches represent a part of a graph (or the whole graph) in a low dimensional vector space while preserving the graph information [8]. There are some review studies in the literature which focus either on similarity-based approaches [9], [10] or embedding-based approaches [8], [11] for link prediction task in graphs. Thus, to the best of our knowledge, a study including methods from both categories is missing in the literature. In this paper, we try to fill this gap. We first introduce the link prediction problem and briefly describe selected similarity-based and embedding-based methods. Then, we evaluate their performances on different types of graphs, namely homogeneous graphs. We compare their performances on diverse graph groups (sharing characteristics). We also propose a few interesting connections between similarity-based and embedding-based methods.

2. LINK PREDICTION APPROACHES

Consider an undirected graph at a particular time t where nodes represent entities and links represent the relationships between pair entities (or nodes). The link prediction problem is defined as discovering or inferring a set of missing links (existing but not observed) in the graph at time $t + \Delta t$ based on the snapshot of the graph at time t. Several link prediction approaches have been proposed in the literature. We focus on the two popular categories: (1) similarity-based approaches and (2) embedding-based approaches.

2.1. Similarity-Based Link Prediction

The similarity-based approach is the most commonly used approach for link prediction which is developed based on the assumption that two nodes in a graph interact if they are similar. Generally, the links with high similarity scores are predicted as truly missing links. The definition of similarity is a crucial and non-trivial task that varies from domain to domain even from the graph to graph in the same domain [9]. As a result, numerous similarity-based approaches have been proposed to predict links in small to large graphs. Some similarity-based approaches use the local neighbourhood information to compute similarity score are known as local similarity-based approach. Another category of similarity-based approaches is global approaches that use the global topological information of graph. The computational complexity of global approaches makes them unfeasible to be applied on large graphs as they use the global structural information such as adjacency matrix [9]. For this reason, we are considering only the local similarity-based approaches in the current study. We have studied six popular similarity-based approaches for link prediction. Considering the citations for a duration from publishing to the year 2020, we define popularity of each approach as the average citation per year.

Table 1 summarizes the approaches with the basic principle and similarity function. These approaches in Table 1 except CCLP (Clustering Coefficient-based Link Prediction) [16] use node degree, common neighborhood or links among common neighborhood information to compute similarity score.

Table 1. Summary of studied similarity-based approaches. The similarity function is defined to predict a link between two nodes *x* and *y*. Γ*x* and Γ*y* denote the neighbour sets of nodes x and y respectively.

Approach	**Principle**	**Similarity-function**
Adamic-Adar (AA) [3]	Variation of CN where each common neighbour is logarithmically penalized by its degree	$S^{AA}(x,y)=\sum_{z\in\Gamma x\cap\Gamma y}\frac{1}{\log\lvert\Gamma z\rvert}$
Resource Allocation (RA) [12]	Based on the resource allocation process to further penalize the high degree common neighbours by more amount	$S^{RA}(x,y)=\sum_{z\in\Gamma x\cap\Gamma y}\frac{1}{\lvert\Gamma z\rvert}$
Preferential Attachment (PA) [13]	Based on the rich-get-richer concept where the link probability between two high degree nodes is higher than two low degree nodes	$S^{PA}(x,y)=\lvert\Gamma x\rvert\times\lvert\Gamma y\rvert$
Hub Promoted Index (HPI) [14]	Promoting link formation between high-degree nodes and hubs	$S^{HPI}(x,y)=\frac{\lvert\Gamma x\cap\Gamma y\rvert}{max(\Gamma x,\Gamma y)}$
Local Leicht-Holme- Newman (LLHN) [15]	Utilizing both of real and expected amount of common neighbours between a pair of nodes to define their similarity	$S^{LLHN}(x,y)=\frac{\lvert\Gamma x\cap\Gamma y\rvert}{\Gamma x\times\Gamma y}$
Clustering Coefficient-based Link Prediction (CCLP) [16]	Quantification of the contribution of each common neighbour by utilizing the local clustering coefficient of nodes	$S^{CCLP}(x,y)=\sum_{z\in\Gamma x\cap\Gamma y}CC_z$

AA, RA and CCLP handcraft the computation of weight of each common neighbours based on their neighbourhood size or clustering co-efficient (CC) [16]. On the other hand, HPI, PA and LLHN assigns equal weights to neighbours. These local similarity-based approaches except PA work well when the graphs have a high number of common neighbours between a pair of nodes. However, LLHN suffers from outlier (infinite similarity score) when one of the end nodes has no neighbour. HPI also suffers from the outlier (infinite similarity score) when both of end nodes have no neighbour.

2.2. Graph Embedding-Based Link Prediction

A graph embedding approach embeds the nodes of a graph into low-dimensional vector space where connected nodes are closer to each other. The embedding vector of a link is then computed based on the embedding of end nodes and a classifier is used to classify it as existent or non-existent link. Random walk-based and neural network-based embedding are two popular methods of embedding [8]. The first one samples the nodes based on the random walk process in graph and adopts skip-gram model to represents them in a low-dimensional vector. The second category is designed based on neural network (NN). The success of NN in image, speech, text processing where data can be represented in Euclidean form, motivates researchers to study GNNs as a kind of NN that operates directly on graphs. GNNs provide an end-to-end graph embedding [8]. In our study, we are interested in a specific GNN architecture called convolution GNN (ConvGNN) [7]. Inspired by the convolution operation of NN, ConvGNNs compute the embedding of a node by aggregating its own and neighbours information. In the following, we present four embedding-based link prediction approaches including one random-walk based (Node2Vec) and three GNN-based (WLNM, SEAL, GAT). We choose Node2Vec to represent simple non-deep learning

methods, WLNM to represent the methods which learn only structural features, SEAL to represent the methods which maximize the use of available information (structural, node attributes, latent features) and GAT to represent the methods which define different roles of different neighbours.

2.2.1. Node2Vec:

Motivated by the classical skip-gram model in natural language processing, Grover & Leskovec [17] developed Node2Vec representation learning approach that optimizes a neighbourhood preserving objective function using Stochastic Gradient Descent (SGD). Node2Vec starts with a fixed size neighbourhood sampling using guided random walk. Unlike the classical random walk, Node2Vec defines a 2nd order random walk that interpolate between BFS(Breadth First Search) and DFS(Depth First Search)-based sampling strategy where two parameters p and q are used to compute the transition probability during the walk. These parameters control how fast the walk explores and leaves the neighborhood of the starting node. The node embedding is then generated based on the popular skip-gram model where the co-occurrence probability among the neighbours those appear within a window.

2.2.2. Weisfeiler-Lehman Neural Machine (WLNM):

Based on the well-known Weisfeiler-Lehman (WL) canonical labelling algorithm [18], Zhang & Chen [19] developed the Weisfeiler-Lehman Neural Machine (WLNM) to learn the structural features from the graph and use it in the link prediction task.

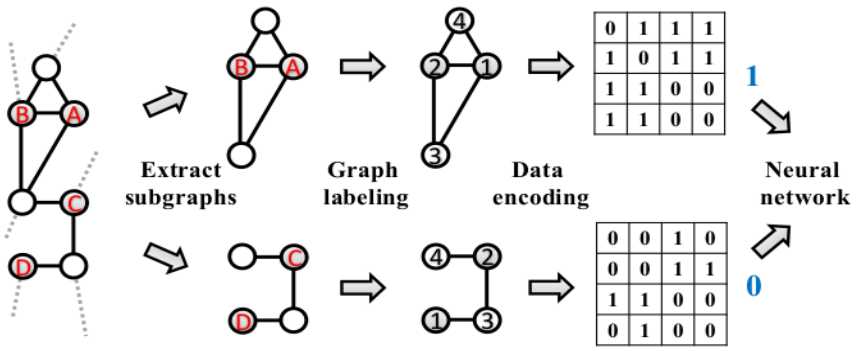


Figure 1. Illustration of WLNM [19] with existent(A,B) and non-existent link(C,D)

As illustrated in Figure 1, WLNM is a three steps link prediction approach that starts with extracting sub-graphs those contain a predefined number of neighbour nodes, labelling and encoding the nodes in the sub-graph using WL algorithm and ends with training and evaluating the neural network.

WLNM is a simple GNN-based link prediction approach which is able to learn the link prediction heuristics from a graph. The downside of WLNM is that it truncates some neighbours to limit the sub-graph size to a user-defined size which are may be informative for the prediction task.

2.2.3. Learning from Sub-graphs, Embeddings and Attributes (SEAL):

Zhang & Chen [20] developed a Conv GNN-based link prediction approach called SEAL to learn from latent and explicit features of nodes along with the structural information of graph. Unlike

WLNM, SEAL is able to handle neighbours of variable size. The overall architecture of the approach is shown in Figure 2.

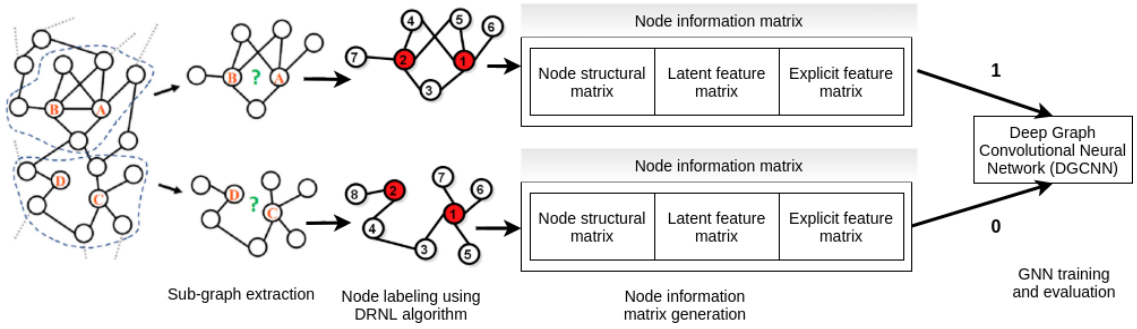


Figure 1. Architecture of SEAL approach [20]

Like WLNM, SEAL also consists of three major steps: (1) sub-graph extraction and node labelling, (2) node information matrix construction, and (3) neural network training and evaluation. SEAL utilizes the available information in the graph to improve the prediction performance. However, SEAL is limited to be applied on homogeneous graphs though many real work graphs are heterogeneous graphs. Moreover, the use of latent feature affects the computational time of SEAL.

2.2.4. Graph Attention Networks (GAT):

In Graph Convolutional Networks (GCN) [21], the convolution operation is defined based on close neighbors where all neighbors contribute equally which affects the prediction performance. To overcome this shortcoming, Velickovic et al. [22] presents GAT by leveraging attention mechanism for learning different weights (or coefficients) to different nodes in a neighborhood. The attention learning mechanism starts with defining a graph attention layer where the input is the set of node features, $h= \{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_N\}$ for N nodes. The layer produces a transformed set of node feature vectors h= $h' = \{\vec{h}'_1, \vec{h}'_2, .., \vec{h}'_N\}$, where h_i and h'_i are input and output embeddings of the node e_i. The attention layer is defined as Equation 1.

$$c_{ij} = f_a(W\vec{h}_i, W\vec{h}_j) \tag{1}$$

where c_{ij} is the attention coefficient of the edge (e_i, e_j), $\vec{h}_i, \vec{h}_j$ are embeddings of nodes e_i, e_j, W is a parametrized linear transformation matrix mapping the input features to a higher dimensional output feature space, and f_a is a shared attention mechanism. GAT uses the LeakyReLU nonlinearity as the activation function of the attention layer. The coefficient indicates the importance of node e_j to node e_i. GAT uses the following softmax function (Equation 2) over the first order neighbours of a node including itself to compute the normalized attention coefficient, α_{ij} of the edge (e_i, e_j).

$$\alpha_{ij} = softmax(c_{ij}) = \frac{\exp(c_{ij})}{\sum_{k \in N_i} \exp(c_{ik})} \tag{2}$$

where N_i is the set of neighbours for node e_i. The output embedding of the node e_i is generated using the attention coefficients as in Equation 3.

$$\vec{h}'_i = \sum_{j \in N_i} \alpha_{ij} W \vec{h}_j \tag{3}$$

GAT extends the single head concept to multi-head mechanism to learn more stable attentions by averaging the coefficients over multi-head attentions. For link prediction, the embedding of end nodes are feed into a fully connected NN.

3. EXPERIMENTAL DESIGN

3.1. Experimental Data

We perform the comparative study of the above discussed similarity and embedding based link prediction approaches in simple and undirected graphs from different domains. To evaluate and describe the performance of the link prediction approaches, we choose ten benchmark graphs from different areas: Ecoli [23], FB15K [24], NS [25], PB [26], Power [27], Router [28], USAir [29], WN18 [30], YAGO3-10 [31], and Yeast [32]. FB1K, WN18 and YAGO3-10 are popular knowledge graphs. These knowledge graphs consist of subject-relationship type-object triples. However, as the studied approaches are applicable to homogeneous graphs only. We simplify these knowledge graphs by overlooking the relation names and considering links as undirected links. The topological statistics of the graph datasets are summarized in Table 2. Based on the number of nodes, these graphs are categorized into small/medium graphs with less or equal 10,000 nodes and large graphs with more than 10,000 nodes.

Table 2. Topological statistics of graph datasets: number of nodes (#Nodes), links(#Links), average node degree (NDeg), clustering coefficient (CC), network diameter (Diam) and description. Large graphs are shaded with gray color.

Graphs	#Nodes	#Links	NDeg	CC	Diam	Description
Ecoli	1805	42325	46.898	0.350	10	Nodes: Operons in E.Coli bacteria Edges: Biological relations between operons
FB15K	14949	260183	44.222	0.218	8	Nodes: Identifiers of Freebase knowledge base (KB) entity Edges: Link between Freebase entities
NS	1461	2742	3.754	0.878	17	Nodes: Researchers who publish papers on network science Edges: Co-authorship of at least one paper
PB	1222	14407	23.579	0.239	8	Nodes: US political blog page Edges: Hyperlinks between blog pages
Power	4941	6594	2.669	0.107	46	Nodes: Electrical power stations (e.g. generators, transformers) of western US

						Edges: Power transmission between stations
Router	5022	6258	2.492	0.033	15	Nodes: Network router Edges: Router-router interconnection for providing router-level internet
USAir	332	2126	12.807	0.749	6	Nodes: US airports Edges: Link between two airports if there is at least one direct flight between them
WN18	40943	75769	3.709	0.077	18	Nodes: Entities (or synsets) corresponds to English word senses Edges: Lexical relations between sysnets
YAGO 3-10	113273	758225	18.046	0.114	14	Nodes: Entities (such as movies, people, cities, etc.) in YAGO KB Edges: Relations between entities
Yeast	2375	11693	9.847	0.388	15	Nodes: Proteins in yeast Edges: Protein-protein interaction in yeast network

3.2. Construction of Train and Test Sets

We follow a random sampling protocol to evaluate the performance of the studied approaches [19]. We prepare train and test set from the experimental graphs. For training dataset, we randomly select 90% existing links (termed as positive train set) and an equal number of non-existing links (termed as negative train set). The remaining 10% existing links (termed as positive test set) and an equal number of non-existing links (termed as negative test set) form the test set. At the same time, the graph connectivity of the training set and the test set is guaranteed. We prepare five train and five test sets for evaluating the performance of the approaches.

For evaluating the performance of similarity-based approaches, the graph is built from the positive training dataset whereas, for embedding-based approaches, the graph is built from original graph that contains both of positive train and test datasets. However, a link is temporarily removed from the graph to train it to the embedding-based approaches or to predict its existence. The performance is quantified by defining two standard evaluation metrics, precision and AUC (Area Under the Curve). All of the approaches are run on a Dell Latitude 5400 machine with 32GB memory and core i7 (CPU 1.90GHz) processor.

3.3. Precision and AUC Computation

Precision describes the fraction of missing links which are accurately predicted as existent links [33]. To compute the precision, the predicted links from a test set are ranked in decreasing order of their scores. If L_r is the number of existing links (in the positive test set) among the L-top ranked predicted links then the precision is defined as Equation 4.

$$Precision = \frac{L_r}{L} \tag{4}$$

An ideal prediction approach has a precision of 1.0 that means all the missing links are accurately predicted. We set L to the number of existent links in the test set. However, there are some challenges with this optimistic way of computing the precision. What if the similarity score is (close to) 0.0 of the lowest ranked link? This issue creates the difficulty to make a separation

between some positive and negative test links. Choosing a threshold when defining L_r could be a potential solution to overcome this problem. The distribution of unnormalized similarity scores are different for graphs from different domains and even for two different datasets from the same domain. Moreover, it is nearly impossible to know the distribution of unnormalized similarity score in advance for graph dataset. These two facts make it infeasible task for the user to define the threshold. To overcome this problem, we define a threshold as the average of the maximum and minimum score in top-L links. We compute the number of positive test links in top-L links (as L_r) as those having similarity scores above the threshold.

On the other hand, the metric AUC is defined as the probability that a randomly chosen existing link has a higher similarity score than a randomly chosen non-existing link [33]. Suppose, n existent and n non-existent links are chosen from positive and negative test sets. If n_1 is the number of existent links having a higher score than non-existent links and n_2 is the number of existent links having equal score as non-existent links then AUC is defined as Equation 5.

$$AUC = \frac{n_1 + 0.5 n_2}{n} \tag{5}$$

We consider half of the total links in the positive test set and negative test set to compute AUC.

4. EXPERIMENTAL RESULTS

The prediction approaches are evaluated in each of the five sets (train and test set) of each graph and performance metrics (precision, AUC) are recorded. We measure the precision in two different ways based on the top-L test links as described in Section 3.3. We compute the threshold-based precision only for similarity-based approaches as embedding-based approaches do learn the threshold. The maximum and minimum similarity scores are computed from the top-L for each test set of each graph. Table 3 shows the results in each of the seven small/medium and three large-size graphs. Each value of the table is the mean over the five test sets. The standard deviation values of both metrics for all approaches in all graphs are very small and they are not included in the table.

It can be clearly seen from Table 3 that the ranges of unnormalized similarity scores are different for different similarity-based approaches and also different in different datasets for the same similarity-based approach. Moreover, the minimum similarity scores are very low (close to 0) in some datasets. These observations prove that in real-world applications, it is difficult to choose a threshold and to assess good precision for similarity-based approaches.

From Table 1, the similarity-based approaches are mostly defined based on the common neighbourhood. As expected, they show low precision (without defining threshold) and AUC values in sparse graphs (low CC, low node degree) like Power, router and high precision for other well-connected graphs in Table 3. Exceptionally, PA shows better prediction performance in sparse graphs as it considers individual node degree instead of common neighbourhood for computing similarity score. The precision scores using the threshold-based method drops drastically in most of the cases as many falsely predicted positive links are identified (i.e. predicted links with very low scores). Surprisingly, HPI shows competitive threshold-based precision value in NS dataset. No single similarity-based approach wins in all small/medium size graphs.

As expected, embedding-based approaches show very good precision and AUC scores across all of the small/medium size graphs compared to similarity-based approaches. What about their comparative performances? No single approach wins in all datasets. Node2Vec shows highest precision scores in some datasets though it is simpler than other embedding-based approaches. The consideration of more distant neighbours in embedding computation during random walk could be the most possible reason behind this success. The use of latent information along with structural information in SEAL for the datasets during prediction task likely explains the improvement of the metric AUC. The best tuning of parameters could be the most possible reason behind the best balance between the prediction metrics in GAT. Table 3 shows that embedding-based approaches provide high-performance metrics in all graphs while similarity-based approaches perform well in some graphs (in terms of optimistic precision). Considering the three large graphs (FB15K, WN18 and YAGO3-10), the prediction metrics for similarity-based approaches are much lower than small/medium scale graphs, especially in WN18 and YAGO3-10 graphs. Likewise the results in small/medium size graphs, the precision scores of these approaches further drops drastically to less than 0.1 when applying the threshold. Unsurprisingly, the prediction scores for embedding-based approaches in large graphs are high as in small/medium scale graphs. The notable point in the prediction metrics for large graphs is that Node2Vec is less competitive than other embedding-based approaches in these large graphs.

Table 3. AUC and Precision (Prec) values with Max Scores (Mx scr) and Min Scores (Mn scr) in small/medium graphs. Precision with * mark (Prec*) is computed based on threshold in top-L links. Graph-wise highest metrics are indicated in bold fonts while approach-wise highest metrics are shown in underline.

Approach	**Metric**	**Ecoli**	**NS**	**PB**	**Power**	**Router**	**USAir**	**Yeast**	**FB15K**	**WN18**	**YAGO 3-10**
AA	Prec	0.9	0.87	0.86	0.17	0.07	0.92	0.83	0.77	0.13	0.15
	Prec*	0.06	0.15	0.01	0.02	0.01	0.16	0.06	0.0002	0.0002	0.0018
	Mx scr	32.84	5.83	33.41	3.04	5.6	16.69	23.71	418.6	57.32	24.44
	Mn scr	2.86	1.14	0.58	0	0	2.7	0	0.12	0	0
	AUC	0.93	0.94	0.92	0.58	0.54	0.94	0.91	0.82	0.56	0.48
PA	Prec	0.78	0.69	0.83	0.49	0.41	0.85	0.79	0.79	0.63	0.83
	Prec*	0.05	0.02	0.01	0.02	0.01	0.13	0.06	0.0003	0.0006	0.0006
	Mx scr	65679	362	61052	53	2397	8298	10642	9881842	10637	2426939
	Mn scr	3532	12	855.7	4	1	739.3	95	942.67	6.33	109
	AUC	0.8	0.66	0.90	0.46	0.43	0.90	0.86	*0.88*	*0.64*	0.88
RA	Prec	0.91	0.87	0.86	0.17	0.07	0.92	0.83	0.77	0.13	0.15
	Prec*	0.03	0.15	0.01	0.03	0.01	0.1	0.07	0.0003	0.0002	0.0011
	Mx scr	1.7	1.8	4.19	0.84	1.32	2.83	2.37	72.06	20.67	5.16
	Mn scr	0.19	0.4	0.03	0	0	0.32	0	0	0	0
	AUC	0.94	0.94	0.92	0.58	0.54	0.94	0.91	0.84	0.57	0.57
HPI	Prec	0.9	0.87	0.8	0.17	0.07	0.91	0.83	0.69	0.13	0.15
	Prec*	0.2	0.96	0.15	0.13	0.02	0.45	0.7	0.0959	0.0796	0.0476
	Mx scr	1	1	1	1	1	1	1	1	1	1
	Mn scr	0.33	0.83	0.21	0	0	0.77	0	0.05	0	0
	AUC	0.94	0.94	0.85	0.58	0.54	0.91	0.9	0.75	0.56	0.47
LLHN	Prec	0.89	0.87	0.74	0.17	0.07	0.87	0.83	0.64	0.13	0.15
	Prec*	0.001	0.13	0.001	0.03	0.003	0.03	0.01	0.0008	0.0046	0.0003
	Mx scr	0.32	1	0.42	2.06	0.83	0.58	0.67	0.28	1	1
	Mn scr	0	0.1	0	0	0	0.01	0	0	0	0
CCLP	AUC	0.91	0.93	0.76	0.58	0.53	0.77	0.9	0.57	0.57	0.45
	Prec	**0.96**	0.73	0.86	0.08	0.07	0.91	0.82	0.78	0.08	0.14
	Prec*	0.06	0.21	0.01	0.01	0.01	0.18	0.06	0.0015	0.0006	0.0013

	Mx scr	30.6	8	27	1.2	1.1	21.1	39.2	51.74	1.67	20.77
	Mn scr	1.8	0.3	0.3	0	0	2.9	0	0.01	0	0
WLNM	AUC	**0.95**	0.87	0.91	0.54	0.53	0.94	0.9	0.84	0.54	0.57
	Prec	0.87	0.84	0.78	0.84	**0.89**	0.85	0.87	0.67	**0.84**	0.68
SEAL	AUC	0.93	0.95	0.93	0.76	0.92	0.86	0.86	0.68	0.79	0.72
	Prec	0.81	*0.96*	0.8	0.66	0.8	**0.91**	0.89	0.77	0.61	**0.86**
	AUC	**0.95**	**0.99**	**0.94**	0.77	**0.94**	**0.94**	**0.98**	**0.96**	**0.87**	**0.97**
GAT	Prec	0.84	0.93	0.84	0.72	0.81	0.88	**0.91**	**0.85**	0.74	0.84
	AUC	0.85	0.90	0.86	0.7	0.79	0.87	0.89	0.87	0.79	0.83
Node2Vec	Prec	0.91	**0.97**	**0.91**	**0.86**	0.8	0.81	0.85	0.79	0.83	0.82
	AUC	0.9	0.96	0.9	**0.82**	0.75	0.85	0.94	0.88	0.79	0.8

Embedding-based link prediction approaches show better performance because they learn heuristics from graphs. However, it is not clear which heuristic(s) are learned. We want to take benefit from this study to get insight of such heuristics by comparing the performances of similarity-based heuristics with performances of embedding-based approaches on the same datasets. In one hand, from Table 1 and Table 3, AA, RA and CCLP –which heuristically assign high weights to nodes with high degrees or cluster coefficients – show better precision on FB15K, PB, NS, USAir, and Yeast compared to other graphs. GAT also shows better precision on these graphs than other graphs. This may indicate that GAT learns similar heuristics as AA, RA and CCLP. In the other hand, WLNM considers the role of each neighbour equally like HPI, LLHN, and PA. WLNM, HPI, LLHN and PA show better performance scores on Power, Router, and WN18 graphs, confirming that they are heuristically compatible.

Table 4. Top-2 ranked similarity-based approaches with higher agreement with embedding-based approach for test link decision. Numbers in () represent the agreement percentages.

Graph	**WLNM**	**SEAL**	**GAT**	**Node2Vec**
Ecoli	HPI(69), RA(69)	LLHN(80), RA(79)	HPI(70),RA(69)	RA(70), LLHN(70)
NS	CCLP(65),AA(63)	AA(70),CCLP(68)	AA(61),PA(61)	AA(70),CCLP(68)
PB	HPI(68),PA(64)	RA(68),PA(66)	LLHN(61),RA(59)	AA(68),RA(68)
Power	HPI(63),LLHN(63)	PA(63),HPI(62)	AA(67),RA(67)	PA(63),RA(62)
Router	PA(52),LLHN(47)	PA(66),LLHN(51)	CCLP(65),RA(65)	CCLP(69),AA(68)
USAir	AA(78),CCLP(78)	LLHN(90),HPI(88)	CCLP(77),AA(75)	RA(90),LLHN(90)
Yeast	CCLP(75),PA(74)	CCLP(70),AA(69)	CCLP(75),AA(71)	CCLP(70),AA(69)
FB15K	RA(32),HPI(31)	LLHN(30),HPI(28)	HPI(28),LLHN(27)	HPI(26),AA(24)
WN18	PA(44),LLHN(42)	PA(40),HPI(32)	PA(28), AA(26)	PA(36), CCLP(31)
YAGO3-10	PA(34),AA(26)	PA(44), AA(24)	PA(38),CCLP(32)	PA(42),RA(34)

In order to further explore their connections, we compute the percentage of agreements in link existence between the embedding-based and the similarity-based approaches. Table 4 shows the top-2 ranked similarity-based approaches when they are ranked in decreasing order of their percentage of agreements on each graph for each embedding-based approach. Overall, embedding-based approaches show higher percentages of agreements to similarity-based approaches in small/medium graphs than in large graphs. Considering all graphs, HPI, PA and LLHN are three frequent heuristics which have higher agreement to WLNM and SEAL approaches. On the other hand, AA, RA and CCLP show frequent agreements with GAT. These agreements align to the previous discussion on the nature of learned heuristics in embedding-based methods. However, low agreement percentage values (in Table 4) but high precision scores (in Table 3) for embedding-based approaches in many graphs like FB15K, Ecoli, NS suggest the existence of other learned heuristics that are not included in this study.

The performance of the studied methods was also assessed in terms of average computational time (data will be made available on request). As expected, similarity-based approaches are faster as they don't require training. As for embedding-based approaches, Node2Vec requires the smallest time as it does not use deep NN like the other embedding-based methods. The computational time of SEAL is the best as it utilizes the structural and explicit features like WLNM and GAT along with latent features like Node2Vec. We also noticed that the computational time of embedding-based methods grows with the size of datasets by more amount than the similarity-based methods.

5. CONCLUSIONS

In this paper, we study several link prediction approaches, looking for their performances and connections. We focused on two categories of methods: similarity-based methods and embedding-based learning methods. The studied approaches were evaluated on ten graph datasets with different properties from various domains. The precision of similarity-based approaches was computed in two different ways to highlight the difficulty of tuning the threshold for deciding the link existence based on the similarity score. The experimental results show the expected superiority of embedding-based approaches. Still, each of the similarity-based approaches is competitive on graphs with specific properties. The possible links between the handcrafted similarity-based approaches and current embedding-based approaches were explored using (i) prediction performance comparison to get an idea about the learned heuristics and (ii) agreement percentage on the diverse graphs. Our observations constitute a modest contribution to the 'black box' limitation of GNN-based methods.

One perspective of this work is to achieve a good trade-off between prediction accuracy and computational time by developing an embedding-based link prediction approach in a distributed and parallel environment. In addition, the approach is expected to be applicable to heterogeneous graphs such as knowledge graphs.

REFERENCES

[1] Z. Xu, C. Pu, and J. Yang, "Link prediction based on path entropy," *Physica A:Statistical Mechanics and its Applications*, vol. 456, pp. 294–301, 2016.

[2] Z. Shen, W.-X. Wang, Y. Fan, Z. Di, and Y.-C. Lai, "Reconstructing propagation networks with natural diversity and identifying hidden sources," *Nature Communi-cations*, vol. 5, no. 1, pp. 1–10, 2014.

[3] L. A. Adamic, and E. Adar, "Friends and neighbors on the web," *Social Networks*, vol. 25, no. 3, pp. 211–230, 2003.

[4] Y. Koren, R. Bell, and C. Volinsky, "Matrix factorization techniques for recommender systems," *Computer*, vol. 42, no. 8, pp. 30–37, 2009.

[5] M. Nickel, K. Murphy, V. Tresp, and E. Gabrilovich, "A review of relational machine learning for knowledge graphs," Proceedings of the IEEE, vol. 104, no. 1, pp. 11–33, 2015.

[6] I. A. Kov´acs, K. Luck, K. Spirohn, Y. Wang, C. Pollis, S. Schlabach, W. Bian, D.-K.Kim, N. Kishore, T. Hao,et al., "Network-based prediction of protein interactions," *Nature Communications*, vol. 10, no. 1, pp. 1–8, 2019.

[7] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and S. Y. Philip, "A comprehensive survey on graph neural networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 1, pp. 4-24, 2020.

[8] P. Cui, X. Wang, J. Pei, and W. Zhu, "A survey on network embedding," *IEEE Transactions on Knowledge and Data Engineering*, vol. 31, no. 5, pp. 833–852, 2018.

[9] V. Martı´nez, F. Berzal, and J.-C. Cubero, "A survey of link prediction in complex networks," ACM Computing Surveys, vol. 49, no. 4, pp. 1–33, 2016.

[10] L. L¨u, and T. Zhou, "Link prediction in complex networks: A survey," *Physica A: Statistical Mechanics and its Applications*, vol. 390, no. 6, pp. 1150–1170, 2011.

[11] H. Cai, V. W. Zheng, and K. C. C. Chang, "A comprehensive survey of graph embedding: Problems, techniques, and applications," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 9, pp. 1616–1637, 2018.
[12] T. Zhou, L. L¨u, and Y.-C. Zhang, "Predicting missing links via local information," *The European Physical Journal B*, vol. 71, no. 4, pp. 623–630, 2009.
[13] A.-L. Barab´asi, and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.
[14] E. Ravasz, A. L. Somera, D. A. Mongru, Z. N. Oltvai, and A.-L. Barab´asi, "Hierarchical organization of modularity in metabolic networks," *Science*, vol. 297, no. 5586, pp. 1551–1555, 2002.
[15] E. A. Leicht, P. Holme, and M. E. Newman, (2006) "Vertex similarity in networks," *Physical Review E*, vol. 73, no. 2, p. 026120.
[16] Z. Wu, Y. Lin, J. Wang, and S. Gregory, "Link prediction with node clustering coefficient," *Physica A: Statistical Mechanics and its Applications*, vol. 452, pp. 1–8, 2016.
[17] A. Grover, and J. Leskovec, "Node2vec: Scalable feature learning for networks," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016, pp. 855–864.
[18] B. Weisfeiler, and A. A. Lehman, "A reduction of a graph to a canonical form and analgebra arising during this reduction," *Nauchno-Technicheskaya Informatsia*, vol. 2, no. 9, pp. 12–16, 1968.
[19] M. Zhang, and Y. Chen, "Weisfeiler-lehman neural machine for link prediction," in *Proceedings of the 23rd ACM SIGKDD International Conference on KnowledgeDiscovery and Data Mining* , 2017, pp. 575–583.
[20] M. Zhang, and Y. Chen, "Link prediction based on graph neural networks," in *Advances in Neural Information Processing Systems*, 2018, pp. 5165–5175.
[21] T. N. Kipf, and M. Welling, "Semi-supervised classification with graph convolutional networks," in *Proceedings of International Conference on Learning Representations*, 2016, pp. 4700–4708.
[22] P. Velickovic, G. Cucurull, A. Casanova, A. Romero, P. Lio, and Y. Bengio, "Graph attention networks," in *International Conference on Learning Representations*, 2018, pp. 1-12.
[23] H. Salgado, A. S. Zavaleta, S. G. Castro, D. M. Z´arate, E. D. Peredo, F. S. Solano,E. P. Rueda, C. B. Martı´nez, and J. C. Vides, "Regulondb (version 3.2): Transcrip-tional regulation and operon organization in escherichia coli k-12," *Nucleic Acids Research*, vol. 29, no. 1, pp. 72–74, 2001.
[24] A. Bordes, N. Usunier, A. Garcia-Duran, J. Weston, and O. Yakhnenko, "Translating embeddings for modeling multi-relational data," in *Advances in Neural Information Processing Systems*, 2013, pp. 2787–2795.
[25] M. E. Newman, "Finding community structure in networks using the eigen vectors of matrices," *Physical Review E*, vol. 74, no. 3, p. 036104, (2006)
[26] R. Acklandet al., "Mapping the us political blogosphere: Are conservative bloggers more prominent?" In *Blog Talk Downunder 2005 Conference, Sydney*, 2005.
[27] D. J. Watts, and S. H. Strogatz, "Collective dynamics of small-world networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.
[28] N. Spring, R. Mahajan, and D. Wetherall, "Measuring isp topologies with rocket-fuel," *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 4, pp. 133–145, 2002.
[29] M. S. Handcock, D. R. Hunter, C. T. Butts, S. M. Goodreau, and M. Morris, "Statnet: An r package for the statistical modeling of social networks," 2003, [Online] Available: http://www.csde.washington.edu/statnet.
[30] A. Bordes, X. Glorot, J. Weston, and Y. Bengio, "A semantic matching energy function for learning with multi-relational data," *Machine Learning*, vol. 94, no. 2, pp. 233–259, 2014.
[31] F. Mahdisoltani, J. Biega, and F. M. Suchanek, "Yago3: A knowledge base from multilingual wikipedias," in *7th Biennial Conference on Innovative Data Systems Research*, 2013.
[32] C. Von Mering, R. Krause, B. Snel, M. Cornell, S. G. Oliver, S. Fields, and P. Bork, "Comparative assessment of large-scale datasets of protein-protein interactions," *Nature*, vol. 417, no. 6887, pp. 399–403, 2002.
[33] L. Pan, T. Zhou, L. L¨u, and C. K. Hu, "Predicting missing links and identifying spurious links via likelihood analysis," *Scientific Reports*, vol. 6, no. 1, pp. 1–10, 2016.

CREDIT CARD FRAUD DETECTION USING SUPERVISED AND UNSUPERVISED LEARNING

Vikas Thammanna Gowda

Department of Electrical Engineering and Computer Science,
Wichita State University, Kansas, USA

ABSTRACT

In the present monetary situation, credit card use has gotten normal. These cards allow the user to make payments online and even in person. Online payments are very convenient, but it comes with its own risk of fraud. With the expanding number of credit card users, frauds are also expanding at the same rate. Some machine learning algorithms can be applied to tackle this problem. In this paper an evaluation of supervised and unsupervised machine learning algorithms has been presented for credit card fraud detection.

KEYWORDS

Credit card fraud detection, Supervised learning, Unsupervised learning.

1. INTRODUCTION

With the increase in internet usage, online shopping has become a trend and growing rapidly as it has become a one stop place for shoppers' diverse purchase list. There are over 1.9 billion online shoppers worldwide and USA alone has over 240 million shoppers. According to US Census Bureau News, in the third quarter of 2020 there has been an increase of 36% in online sales when compared to that in 2019. Debit card or credit card is used as the main mode of payment for online sales which has led to a raise in frauds. According to a report by Shift CC Processing, credit card frauds has resulted in $24.26 billion in 2018 and US leads as the most credit card fraud prone country with 38.6% of reported credit card frauds. It is necessary to support the payment systems with an efficient fraud detection capability to minimize unwanted adversary activities.

Credit card fraud detection is based on analysis of a card's spending behaviours and identifying their transactions into fraudulent and legitimate transactions. Various difficulties are related with credit card fraud detection: (1) fraudulent behaviour profiles are dynamic in nature that is fraudulent transactions generally appear as though genuine ones; (2) credit card transaction datasets are rarely available due to privacy and security concerns and the accessible datasets are profoundly imbalanced; (3) optimal feature selection for the models; (4) suitable metric to evaluate performance of models on skewed credit card fraud data. Many techniques have been applied to credit card fraud detection such as artificial neural network [1], genetic algorithms [2,3], frequent item set mining [4], decision trees [5], migrating birds optimization algorithm [6], naïve Bayes [7].

The objective of this paper is to evaluate an imbalanced dataset based on few performance parameters using supervised machine learning (a. *Logistic Regression*, b. *Support Vector Machine* (SVM), c. *Random Forest*) and unsupervised machine learning (a. *Isolation Forest*, b.

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 93-99, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111107

Local Outlier Factor, c. *k-Means*) algorithms and determine the best algorithm for credit card fraud detection. The rest of the paper is organised as following. A brief literature review is done in section 2. In section 3, we study the fundamentals of the algorithms used in this paper. Section 4 deals with the parameters used in this paper to determine the best algorithm. Experimental results are analysed in section 5 and concluded in section 6.

2. RELATED WORK

In recent days credit card fraud detection has drawn a lot of research interest and several techniques and strategies for detection. The work in [8] gives an exhaustive discussion on the difficulties and issues of fraud detection research. Mohammad et. al., [9] inspected the most well-known sorts of credit card fraud and the current nature-inspired detection strategies that are utilized in detection methods. A detailed comparison is made between decision tree and support vector machine by Sahin and Duman [10] in detecting credit card fraud. They divide the entire dataset into three groups which differ in ratio between fraudulent transactions and legitimate ones and develop a series of seven decision tree and SVM based models. The experimental results indicate that decision tree-based model is better than SVM model.

In 2019, Naik et. al., [11] have used naïve Bayes, logistic regression J48 and adaboost algorithms for credit card fraud detection and observed that the highest accuracy is obtained for both adaboost and logistic regression algorithms. Since both the algorithms had the same accuracy, time factor was taken into consideration to determine that adaboost algorithm works well to detect credit card fraud.

Sailusha et. al., [12] compares random forest and adaboost algorithms as machine learning techniques for credit card fraud detection. Both the algorithms have same accuracy but when precision, recall and F1 scores are considered, the random forest algorithm has the highest value than adaboost algorithm. Lorenzo et. al., [13] have used isolation forest and local outlier factor for anomaly detection. It works better on unlabelled dataset. The algorithm allows avoiding the subtask of detection.

3. ALGORITHMS

Machine learning is an art of programming computer, so they can learn from data. Machine learning systems can be classified according to the amount and type of supervision they get during training process. There are four major categories: Supervised Learning, Unsupervised Learning, Semi Supervised Learning, Reinforcement Learning. In Supervised Learning [14], the training data carries a label (desired solution) that is fed to the algorithm. The training data in Unsupervised Learning is unlabelled, and the system tries to learn by itself without a teacher. Semi Supervised Learning deals with partially labelled training data, usually a lot of unlabelled data and a little bit of labelled data. In Reinforcement Learning, the algorithm learns a policy of how to act given an observation of the world. Every action has some impact in the environment, and the environment provides feedback that guides the learning algorithm.

3.1. Supervised Machine Learning Algorithms

The learning process in a simple supervised learning model is divided into two steps: training and testing. During the training process, the training data is taken as input in which features are extracted and learned by the learning algorithm to build the learning model [15]. In testing process, the predictions are made on the test data using the model that was built in the training

process. Supervised learning is the most common technique used in the classification problems. Let us see the three supervised learning algorithms used in this paper.

Logistic Regression: It is basically a probabilistic model which makes use of a logistic function to model a binary dependent variable. A logistic model has a dependent variable with two possibilities such as pass/fail, true/false, 0/1. The output of this function will be one of the possibilities with a probability value. The logit function is the logarithm of the odds ratio (probability of an event occurring). The function maps the input in the range [0,1] to a real-number range.

$$odds\ ratio = \frac{p}{1-p}$$

Where p = probability of the positive event

$$logit = \log(odds\ ratio)$$
$$logit = \log(\frac{p}{1-p})$$

Support Vector Machine: It is a classifier that maps feature from the non-linear input space to a higher dimensional feature space. The objective of the support vector machine algorithm is to find a hyper plane in an N-dimensional space that distinctly classifies the data points. This converts complex classification problems to linear in a higher dimensional space. For any two classes of data points there are many possible hyperplane that separates the data points and the goal is to find one such hyperplane whose distance between the data points are at a maximum distance. Maximizing the margin distance provides some reinforcement so that future datapoints will be classified with more confidence.

Random Forest: This is basically an ensemble classifier (ensemble method is about combining models to an ensemble such that the ensemble has a better performance than the individual model on an average). It combines through a majority decision tree classifier and the output is combined through a majority. Random Forest can be understood as bagging (bagging is similar to majority voting but uses some learning algorithm to fit models on different subsets of the training data) with decision trees, but instead of growing the decision trees by basing the splitting criterion on the complete feature set, we use random feature subsets. To summarize, in random forests, the decision tree is fit on different bootstrap samples, and for each decision tree, a random subset of features is selected at each node upon optimal split.

3.2. Unsupervised Machine Learning Algorithms

It refers to the utilization of Artificial intelligence algorithms to recognize patterns in datasets containing datapoints that are neither classified nor labelled. Unlike supervised learning, data is not split into training and testing datasets. The algorithms are thus allowed to classify labels and/or group the datapoints in the datasets without having any external guidance in performing that task. It allows the system to identify pattens within datasets on its own. Unsupervised learning system will group unsorted information according to similarities and differences even though there are no categories provided. Unsupervised Learning is the most common technique in the clustering problems. Let us see the three unsupervised learning algorithms used in this paper.

Local Outlier Factor: Outliers are patterns in the datasets that do not conform to the expected behaviour. There are mainly two types of outliers: Global Outliers and Local Outliers. In global

outliers the datapoints are significantly different from the rest of the dataset. In local outliers, the datapoints are significantly different from their neighbours in the dataset. Local outlier factor is a score that tells how likely a certain data is an outlier. It is a calculation that looks at the neighbours of a certain point to find out its density and compare this to the density of other points later. It performs well when the density of the data is not the same throughout the dataset.

Isolation Forest: It is similar to random forest and is built on the basis of decision trees. It explicitly identifies anomalies or outliers rather than profiling normal datapoints. It isolates observations by randomly selecting a feature and then randomly selecting a split value between the maximum and minimum values of that selected feature. The split depends on how long it takes to separate the points. In principle, outliers are less frequent than regular observation and are different from them in terms of values as they lie further away from the regular observations in the feature space. When a forest of random trees collectively produces shorter path lengths for samples, they are highly likely to be anomalies.

K-means: It is an iterative method that tries to partition the dataset into 'K' pre-defined distinct non-overlapping clusters where each datapoint belongs to only one cluster. It tries to make the intra-cluster datapoint as similar as possible while keeping the cluster as far as possible. It assigns datapoints to a cluster such that the sum of squared distance between the datapoints and the cluster centroid is at the minimum. The less variations we have within the clusters, the more homogeneous the datapoints are within the same cluster. In K-means algorithm, we first specify the number of clusters K and initialize centroids by shuffling the dataset and then randomly selecting K data points for centroids without replacement. Continue iterating until there is no change to the centroids or until the iteration process has been completed.

4. PERFORMANCE MEASURE

To evaluate the performance of a particular model, we make use of various parameters. Confusion matrix is a summary table showing how good the model is at prediction by plotting the number of correct predictions against the number of incorrect predictions. It has four categories: *True Positive* (TP), here the predicted value matches the actual value. Actual value was positive, and the model predicted a positive value. *True Negative* (TN), here the predicted value matches the actual value. The actual value was negative, and the model predicted a negative value. *False Positive* (FP), here the predicted value was falsely predicted. Actual value was negative, but the model predicted a positive value. *False Negative* (FN), here the predicted value was falsely predicted, the actual value was positive, but the model predicted a negative value.

Accuracy is a measure of how many correct predictions your model made. It is a good basic metric to measure the performance of a model, but the downside of a simple accuracy is that it works well in balanced datasets and becomes poorer metric in unbalanced datasets.

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Recall is a measure of how many true positives get predicted out of all the positives in the dataset. It is also called as sensitivity. The recall value can often be turned by tuning several parameters of the machine learning model. A high recall means that most of the positive cases was labelled as positive. A low recall means that there is a high number of false negative.

$$recall = \frac{TP}{TP + FN}$$

Precision is a measure for the correctness of a positive prediction. It means that if a result is predicted as positive, how sure can you be that the result is actual positive.

$$precision = \frac{TP}{TP + FP}$$

As with recall, precision can be turned by tuning the parameters of the model. A higher precision typically leads to a lower recall and higher recall leads to a lower precision. So, there is a trade-off between precision and recall.

F1 is a combination of precision and recall, namely their harmonic mean. It is needed when the balance between precision and recall must be maintained.

$$F1 = 2\,\frac{precision * recall}{precision + recall}$$

5. EXPERIMENTAL RESULTS

The dataset for the experiment was taken from Kaggle [18] website. It contains transactions made by credit cards in 2013. The dataset is labeled and contains fraudulent transactions with 492 out of total transactions of 284,807. Therefore, the data is considered to be unbalanced since the fraudulent cases are 0.173%. Figure 1 shows the distribution of dataset. It consists of 30 columns without the column labels. In order to conserve privacy, a PCA projection was applied to all columns excluding: time and amount features. Therefore, all columns are numerical variables. The labels columns contain a breakdown of the two classes where 0 and 1 correspond to a valid transaction and fraud, respectively.

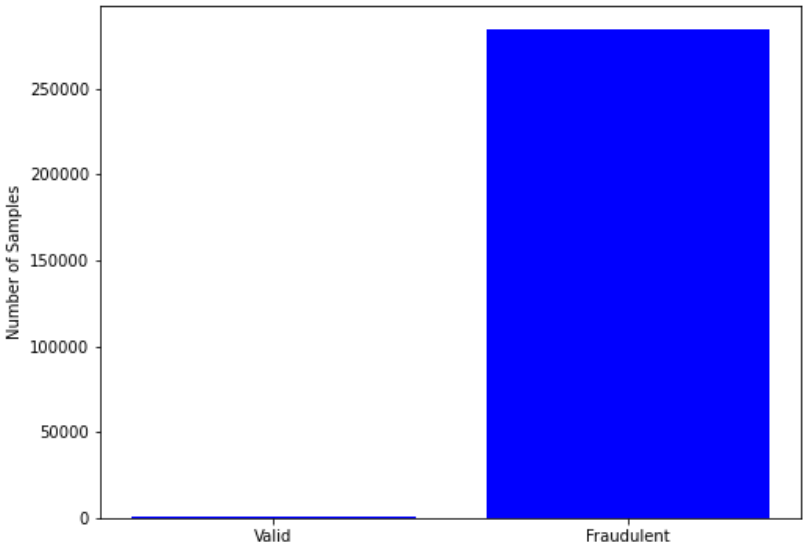


Figure 1. Distribution of dataset

The main purpose of this study is to demonstrate how the various algorithms perform on the dataset. Figure 2 shows the accuracy scores for all the algorithms. The highest accuracy scores are averaged about 99% but these accuracy scores are misleading since, accuracy metric is only

well suited for balanced datasets. Table 1 shows the calculations of accuracy, precision, recall and F1 scores which will help in determining the best algorithm.

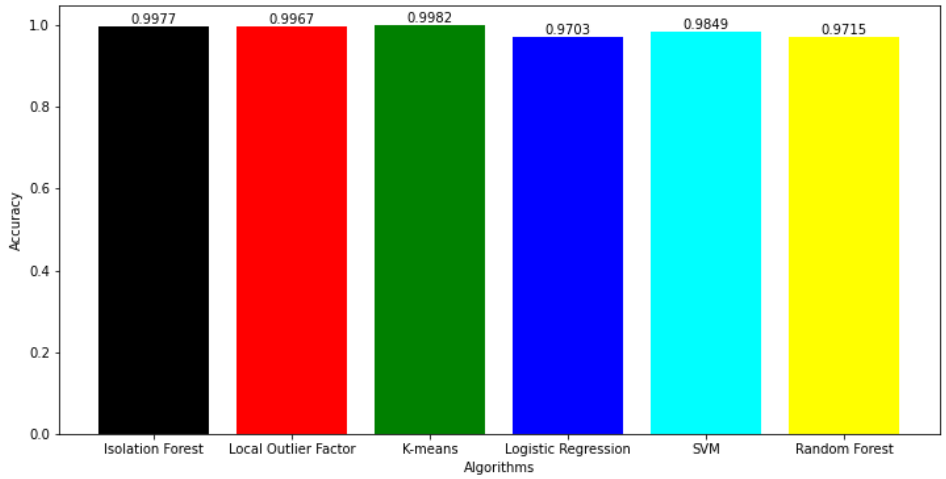


Figure 2. Accuracy scores for each algorithm.

Table 1. Performance measure for supervised and unsupervised learning algorithms.

Model	F1 score	Accuracy	Recall	Precision
Logistic Regression	**0.9326**	**0.9703**	**0.909**	**0.9574**
SVM	**0.9479**	**0.9849**	**0.9191**	**0.9785**
Random Forest	**0.9435**	**0.9715**	**0.9293**	**0.9583**
Isolation Forest	**0.67**	**0.9977**	**0.67**	**0.67**
Local Outlier Factor	**0.25**	**0.9967**	**0.25**	**0.25**
K-means	**0.926**	**0.9982**	**0.879**	**0.9798**

Precision gives us an idea of how many times the algorithm has detected the fraud correctly, recall gives an idea of how much it detects and F1 score helps in maintaining the precision recall trade off. Based on these ideas, it is observed that precision value for K-means algorithm is highest, recall value is highest for random forest algorithm and F1 score is highest for support vector machine algorithm. Precision value for support vector machine is very close to the precision score for K-means and has a very good recall value of 0.9191 which is next to recall value of random forest. Support vector machine algorithms performs very well for credit card fraud detection with an accuracy of 98.49% and a high precision/recall value.

6. CONCLUSION

We have developed supervised and unsupervised models with the goal to detect fraudulent transactions from a large unbalanced dataset. Comparative results in terms of the comparison metric is the percentage of correctly identifying fraudulent transactions and precision, recall, accuracy and F1 score have been presented. In fact, accuracy can be misleading where it could misrepresent a machine learning technique. For example, local outlier factor has an accuracy of 99.67% but performs poorly based on precision and recall values. So precision, recall and F1 score values plays a significant role in deciding the best algorithm for fraud detection. K-means algorithms is the best among the unsupervised learning algorithms and support vector machine performs well among all the algorithms used.

REFERENCES

[1] Ogwueleka F N, (2011). Data Mining Application in Credit Card Fraud Detection System, Journal of Engineering Science and Technology Vol 6, No 3, pp 311-322..

[2] Rama Kalyani K and Uma Devi D, (2012). Fraud Detection of Credit Card payment system by Genetic Algorithm, International Journal of Scientific and Engineering Research, Vol 3 Issue 7,pp 1-6 ISSN 2229-5518.

[3] Meshram P L and Bhanarkar P, (2012). Credit and ATM card fraud detection using Genetic approach, International Journal of Engineering Research and Technology, Vol 1 Issue 10, pp- 1-5 ISSN 2278-0181.

[4] Seeja K R and Zareapoor M, (2014). Fraud Miner: A Novel credit card fraud detection model based on Frequent Itemset Mining, The Scientific World Journal Hindawi Publishing Corporation, Volume 2014 Article ID 252797, pp 1-10.

[5] Patil S, Somavanshi H, Gaikwad J, Deshmane A and Badgujar R (2015). Credit card fraud detection using Decision Tree induction algorithm, International Journal of Computer Science and Mobile Computing, Vol 4 Issue 4 pp 92-95 ISSN: 2320-088x.

[6] Duman E, Buvukkava A and Elikucuk I (2013). A novel and successful credit card fraud detection implemented in a Turkish bank. In Data Mining Workshops 2013. 13th International Conference on IEEE pp 162-171.

[7] Bhnsen A C, Stojanovic A, Aovada D and Ottersten B (2014). Improved credit card fraud detection with calibrated probabilities. SIAM International Conference on Data Mining pp 677-685. Society for industrial and applied mathematics.

[8] Bolton R J and Hand D J (2002). Statistical fraud detection: a review. Statistical Science 17(3), 235-249

[9] Behdad M, Barone L, Bennamoun M and French T (2012). Nature inspired techniques in the context of fraud detection. IEEE transaction on System Management and Cybernetics Part C, 42(6) 1273-1290.

[10] Sahin Y and Duman E (2011), Detecting credit card fraud by Decision Tree and Support Vector Machine. Lecture notes in Engineering and Computer Science, 2188(1).

[11] Heta Naik, PrashastiKanikar (2019). Credit card fraud detection based on Machine Learning Algorithms, International Journal of Computer Applications (0975-8887) Volume 182 No 44 March 2019.

[12] R. Sailusha, V. Gnaneswar, R. Ramesh and G. R. Rao, "Credit Card Fraud Detection Using Machine Learning," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, pp. 1264-1270, doi: 10.1109ICICCS48265.2020.9121114

[13] L. Meneghetti, M. Terzi, S. Del Favero, G. A Susto and C. Cobelli, "Data-Driven Anomaly Recognition for Unsupervised Model-Free Fault Detection in Artificial Pancreas", IEEE Transactions On Control Systems Technology, pp. 1-15, 2018

[14] Nasteski, Vladimir. (2017). An overview of the supervised machine learning methods. HORIZONS.B. 4. 51-62. 10.20544/HORIZONS.B.04.1.17.P05.

[15] Sandhya N. dhage, Charanjeet Kaur Raina. (2016) A review on Machine Learning Techniques. In International Journal on Recent and Innovation Trends in Computing and Communication, Volume 4 Issue 3.

[16] Sperandei, Sandro. (2014). Understanding logistic regression analysis. Biochemia medica. 24. 12-8. 10.11613/BM.2014.003.

[17] Powers, David &Ailab,. (2011). Evaluation: From precision, recall and F-measure to ROC, informedness, markedness & correlation. J. Mach. Learn. Technol. 2. 2229-3981. 10.9735/2229-3981.

[18] https://www.kaggle.com/mlg-ulb/creditcardfraud

[19] Q. Zhang, N. Koudas, D. Srivastava, and T. Yu. Aggregate query answering on anonymized tables. Pages 116-125, 2007.

DENSE-RES NET FOR ENDOSCOPIC IMAGE CLASSIFICATION

Quoc-Huy Trinh and Minh-Van Nguyen

Department of Computer Engineering, Ho Chi Minh University of Science,
Ho Chi Minh City, Vietnam

ABSTRACT

We propose a method that configures Fine-tuning to a combination of backbone DenseNet and ResNet to classify eight classes showing anatomical landmarks, pathological findings, to endoscopic procedures in the GI tract. Our Technique depends on Transfer Learning which combines two backbones, DenseNet 121 and ResNet 101, to improve the performance of Feature Extraction for classifying the target class. After experiment and evaluating our work, we get accuracy with an F1 score of approximately 0.93 while training 80000 and test 4000 images.

KEYWORD

Kvasir dataset, dense-res, medical image, classification, deep neural network.

1. INTRODUCTION

In recent years, the number of people that have been affected by colorectal cancer (CLC) is increasing. It is also on a third of the world for many years. However, can we diagnose and prevent CLC is a crucial issue for the health organization. Some studies illustrate that almost 95% of CLC is from the adenomatous polyp. The resection of Colorectal adenomatous polyps can reduce the CLC. On the other hand, the best way to deal with CLC is early diagnosis and have straight treatment.

Nowadays, the growing up of population is parallel with the increase of CLC also the number of people accepts for the CLC examination is getting higher. However, the detection technique for polyps in the past and in some country, current is dependent on almost all human tasks by doctors experienced and ability, which can easily be affected by environmental factor and can be inefficient.[1]

Recently, there are many approaches to classification these classes by using backbones, such as ResNet 50, Densnet 169, Efficientnet, etc. Almost all results of these approaches are high, but there is an issue that is the bias for some classes in the dataset. For this reason, we proposed Dense-Res Net for classification endoscopic images.

2. RELATED WORK

In later years, there are many kinds of research in the classification, detection of Gastrointestinal (GI) and endoscopic images. Almost all research uses Deep Learning with Deep Convolution architecture such as LeNet, AlexNet, ResNet, DenseNet and GoogleNet [7]. The results of those research are higher and cost low computational. Distinct from simple CNNs, the Deep

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 101-108, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111108

Convolution architectures extract feature better and more obviously [8]. Furthermore, these features are good to localize the area of symptoms on the images.[5]

In 2021, research creates a framework that uses a three-stage framework for diagnosing gastrointestinal diseases. They have three stages:

- First is the Image pre-processing step which is feature extraction by Deep architecture
- Next is Handcrafted Feature Extraction and Reduction.
- The last is Fusion Feature before being classified.

The result of this research achieves 94.75% accuracy, which is the highest test score on the Kvasir Dataset by using ResNet 50.[6]

Our project is inspired by studies of Transfer Learning and using Deep Neural Network to diagnose Endoscopic images [4]. Moreover, in later years, Dense-ResNet and Ensembling Dense Network- Residual Network are used to classify image on Imagenet.[2]

3. DATASET

To do this task, we use Kvasir Dataset. The Kvasir Dataset is collected using endoscopic equipment at VestreViken Health Trust (VV) in Norway. The VV consists of 4 hospitals and provides health care to 470.000 people. One of these hospitals (the Bærum Hospital) has a large gastroenterology department from where training data have been collected and will be provided, making the dataset larger in the future. Furthermore, the images are carefully annotated by one or more medical experts from VV and the Cancer Registry of Norway (CRN).[3]

The dataset consists of 80000 images in 10 folds for cross-validation in the training and evaluating process. 80000 images are split into eight classes: dyed-lifted-polyps, dyed-resection-margins, esophagitis, normal-cecum, normal-pylorus, normal-z-line, polyps and ulcerative-colitis.[3]

We use Kvasir dataset v2 consisting of 80000 images in 10 folds for the training process.

For evaluating the method, we propose the Kvasir dataset v1 containing 4000 images in 8 classes to be the test set to evaluate the metrics.

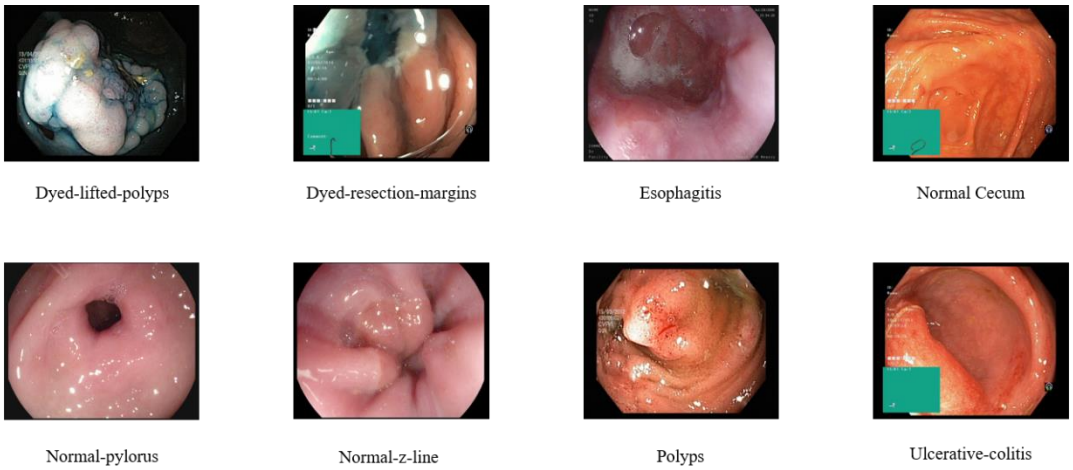


Figure 1. Eight classes in Kvasir dataset

4. METHODS

In the methods, we use 2 backbones are DenseNet 121 and ResNet 101 to build our model architecture. The dataset for training and evaluation of the architecture is from Kvasir Dataset and some parameter can be changed to get the better result.

4.1. Data Pre-Processing

After loading data, we resize all the images to the size (256,256), then we split the dataset into the training set and validation set in the ratio of 0.75:0.25. After resizing and splitting the validation set, we rescale the data pixel down to be in the range [-1,1] by divide by 127.5. Then we use the application of ResNet to preprocess input.

4.2. Data Augmentation

To reduce the Overfitting problem, we use augmentation to generate the data randomly by random flip images and random rotation with an index of 0.2.

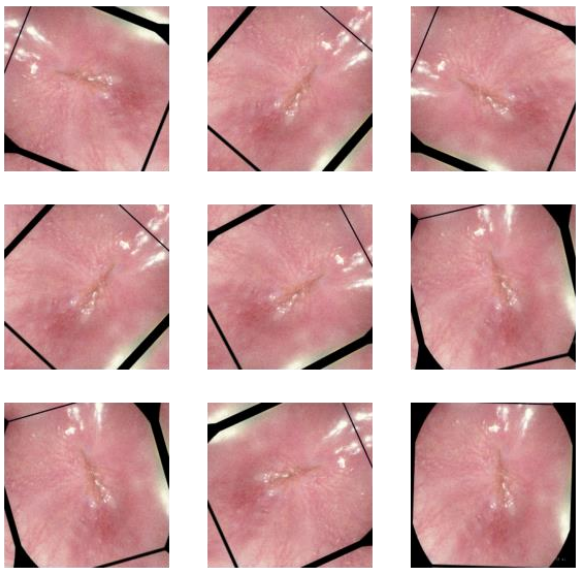


Figure 2. Data after Augmentation

4.3. Network Architecture

In our architecture, we propose to use ResNet 101 and DenseNet 121 backbones for the first layers. We will have two pipes: ResNet 101 and DenseNet. The output of ResNet 101 will be extracted, by a Conv2D, to have the same shape as DenseNet 121 output. After feature extraction, they are added to create the feature map before coming to global Average Pooling layers for being classified.

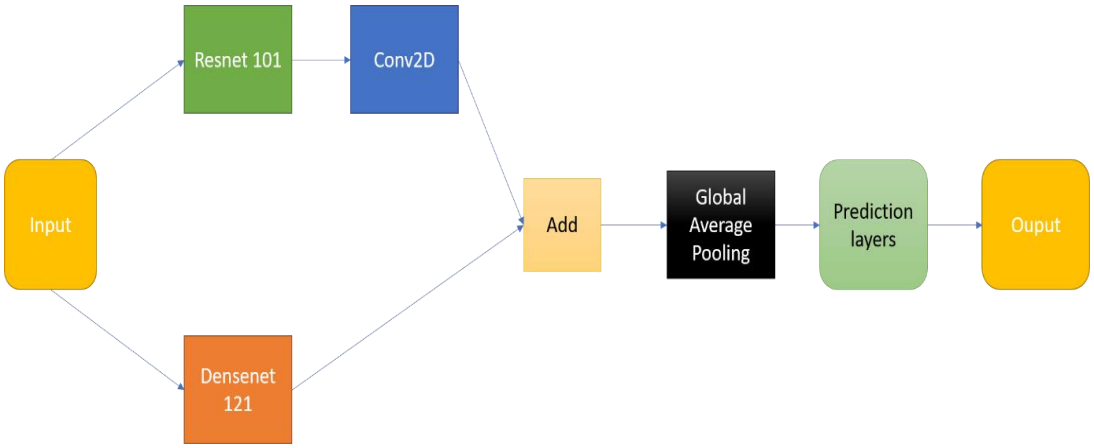


Figure 3. Visualize Dense-Res Net architecture

The figure below will illustrate our work and model that we design:

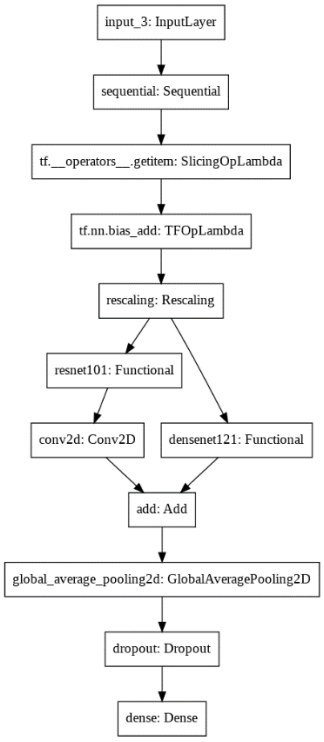


Figure 4. Visualize full model architecture include pre-processing layers

4.4. Training Model

Our models are initialized with pre-trained weight from TensorflowImagenet. We use a batch size of 32 for training data with an image's size of (256,256). We use RMSprop with a learning rate is 0.0001 for optimizer and evaluate the training process by accuracy and F1-score. For the loss function, we use Sparse Categorical Cross-entropy. We train the model with 20 epochs and get the checkpoint that has the highest validation loss.

Firstly, we freeze all the complicated layers of DenseNet and ResNet. Then, we start to train for the first time and get the result:

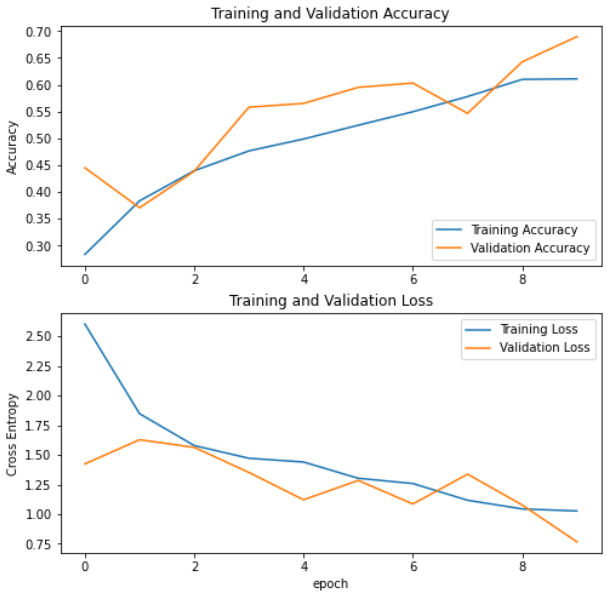


Figure 5. The learning curve for the first training

After the first training, we unfreeze all layers in both ResNet and DenseNet, and we define the model fine-tune from layer 100th. We have the result for the second training process:

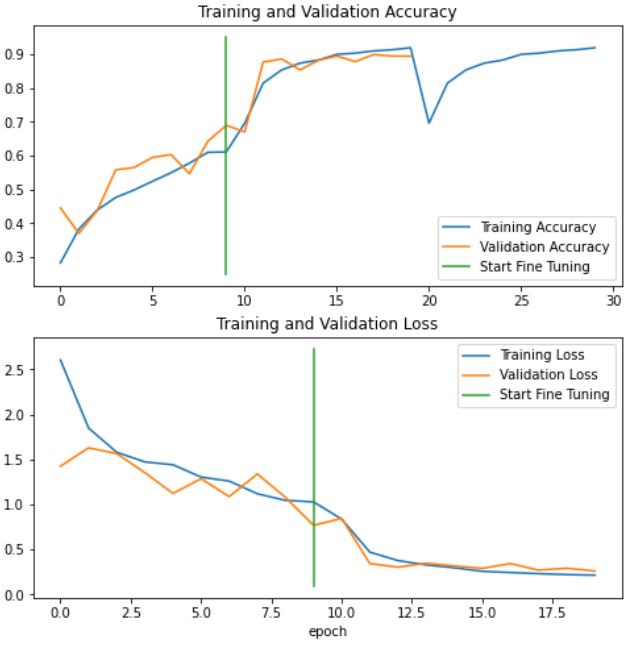


Figure 6. The learning curve for the second training

4.5. Evaluation

After training on Kvasir dataset V2, we approach testing with the data of 4000 images from Kvasir dataset v1. We have the result below:

Table 1. Evaluation of model on Kvasir dataset v1

Metrics	**Value**
Accuracy	0.9263
Precision	0.93375
Recall	0.92625
F1 Score	0.92625

The model has good performance with an accuracy of approximately 0.93. The other measurement scores have the same trend with that accuracy, demonstrating that this model has well-perform on this dataset.

The confusion matrix below evaluates the performance of each class:

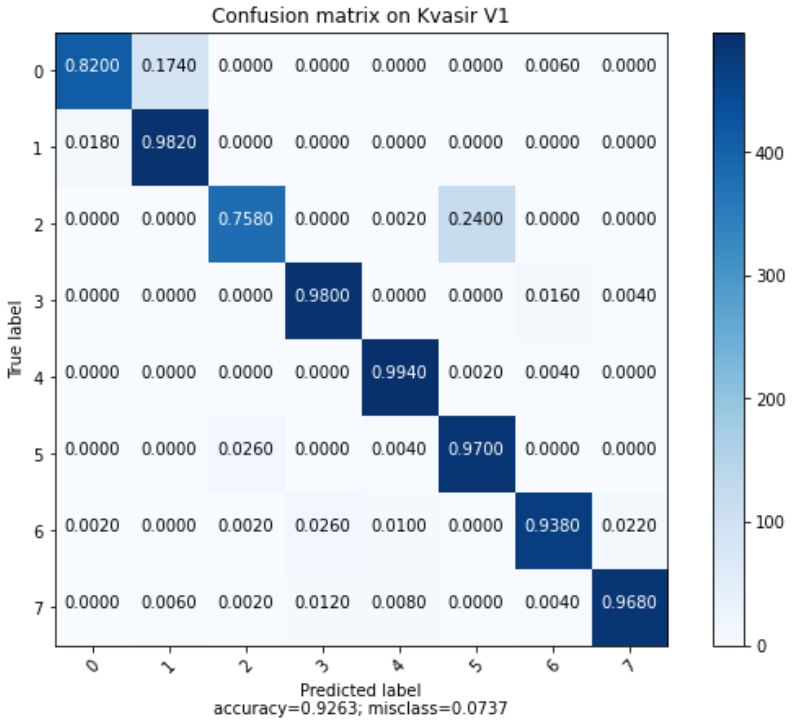


Figure 7. Confusion matrix evaluate performance of model on Kvasir Dataset V1

By the Confusion matrix, we can see some false prediction on label 1 and label 5, which belong to dyed-resection-margins and normal-z-line. Dyed-resection-margins and normal-z-line have predicted to dyed-lifted-polyps and esophagitis.

To deal with these problems, we propose methods to have better pre-processing data by reducing the noise, such as a green box on the endoscopic images.

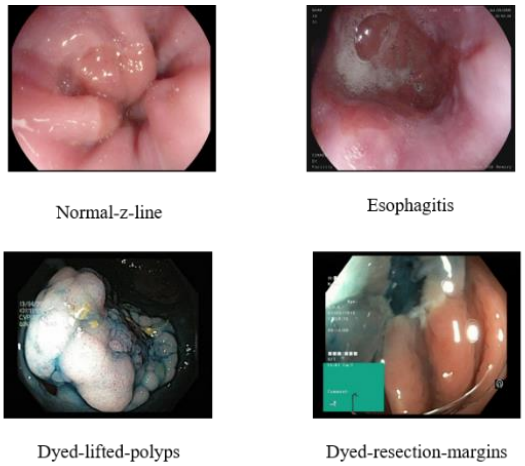


Figure 8. Comparison of False prediction

5. DISCUSSION

Although our method achieves a high score, there some limitations in our experiment. Therefore, we need to improve. Initially, the model can probably get overfitting if we have little training data. Furthermore, it is necessary to do more experiments to choose the better parameter and the number of layers to freeze.

In the future, we can optimize the parameter and add some Batch Normalization layers to optimize computational cost and improve the score of the model.

6. CONCLUSION

We demonstrated the proposal of using Res-Dense Net with Fine-tuning technique to classify endoscopic images. The result of our research is positive, which are 0.9263 for accuracy and 0.92625 for F1 score. However, there are some drawbacks that we have to do to improve the performance of the model, such as pre-processing data, reduce noise, change the size of the image to train.

Furthermore, we can apply ResNet101 V2 or DenseNet 169 backbone to have better feature extraction and better performance of the model.

7. ACKNOWLEDGMENT

This research is partially supported by the research funding from the Faculty of Information Technology, University of Science, Ho Chi Minh city, Vietnam.

REFERENCES

[1] Chien-Hsiang Huang, Hung-Yu Wu, and Youn-Long Lin: HarDNet-MSEG: A SimpleEncoder-Decoder Polyp SegmentationNeural Network that Achieves over 0.9 Mean Dice and 86 FPS.
[2] Victor Cheung: DenResNet: Ensembling Dense Networks and Residual Networks
[3] Konstantin Pogorelov, Kristin Ranheim Randel, Carsten Griwodz, SigrunLosadaEskeland, Thomas de Lange, Dag Johansen, Concetto Spampinato, Duc-Tien Dang-Nguyen, Mathias Lux, Peter Thelin Schmidt, Michael Riegler, Pål Halvorsen, Kvasir: A Multi-Class Image Dataset for Computer Aided

Gastrointestinal Disease Detection, In MMSys'17 Proceedings of the 8th ACM on Multimedia Systems Conference (MMSYS), Pages 164-169 Taipei, Taiwan, June 20-23, 2017.

[4] Trung-Hieu Hoang, Hai-Dang Nguyen, Viet-Anh Nguyen, Thanh-An Nguyen, Vinh-Tiep Nguyen, Minh-Triet Tran: Enhancing Endoscopic Image Classification with Symptom Localization and Data Augmentation, in Proceedings of the 27th ACM International Conference on Multimedia.

[5] Nini Rao, Hongxiu Jiang, Chengsi Luo: Review on the Applications of Deep Learning in the Analysis of Gastrointestinal Endoscopy Images., Article in IEEE Access - September 2019.

[6] Omneya Attalah and Maha Sharkas: GASTRO-CADx: a three stages framework for diagnosing gastrointestinal diseases, PeerJ Computer Science.

[7] Konstantin Pogorelov, Kristin Ranheim Randel, Carsten Gri-wodz, Sigrun Losada Eskeland, Thomas de Lange, Dag Johansen, Concetto Spampinato, Duc-Tien Dang-Nguyen, Mathias Lux, Peter Thelin Schmidt, Michael Riegler, and P ̊alHalvorsen. Kvasir: A multi-class image dataset for computer aided gastrointestinal disease detection. In Proceedings ofthe 8th ACM on Multimedia Systems Conference, MMSys'17, page 164–169, New York, NY, USA, 2017. Association for Computing Machinery.

[8] Dinh Viet Sang, Tran Quang Chung, Phan Ngoc Lan, Dao Viet Hang, Dao Van Long, Nguyen Thi Thuy: AG-CUResNeSt: A Novel Method for Colon Polyp Segmentation, Artificial Intelligence in Medicine, May 6 2021.

AUTHORS

Quoc-Huy Trinh and Minh-Van Nguyen Study Bachelor of Computer Science at Ho Chi Minh University of Science Ho Chi Minh city, Vietnam

USING MULTILINEAR FEATURE SPACE TO ACCELERATE CNN CLASSIFICATION

Michel Andre L .Vinagreiro[1], Edson C. Kitani[2],
Armando Antonio M. Lagana[1] and Leopoldo R. Yoshioka[1]

[1]Laboratory of Integrated Systems,Escola Politecnica da
Universidade de Sao Paulo, Sao Paulo, Sao Paulo,Brasil
[2]Department of Automotive Electronics, Fatec Santo Andre,
Santo Andre, Sao Paulo, Brasil

ABSTRACT

Computer vision plays a crucial role in ADAS security and navigation, as most systems are based on deep CNN architectures the computational resource to run a CNN algorithm is demanding. Therefore, the methods to speed up computation have become a relevant research issue. Even though several works on acceleration techniques found in the literature have not yet been achieved satisfactory results for embedded real-time system applications. This paper presents an alternative approach based on the Multilinear Feature Space (MFS) method resorting to transfer learning from large CNN architectures. The proposed method uses CNNs to generate feature maps, although it does not work as complexity reduction approach. When the training process ends, the generated maps are used to create vector feature space. We use this new vector space to make projections of any new sample in order to classify them. Our method, named MFS-CNN, uses the transfer learning from pre trained CNN to reduce the classification time of new sample image, with minimal loss in accuracy. Our method uses the VGG-16 model as the base CNN architecture for experiments; however, the method works with any similar CNN model. Using the well-known Vehicle Image Database and the German Traffic Sign Recognition Benchmark we compared the classification time of original VGG-16 model with the MFS-CNN method and our method is, on average, 17 times faster. The fast classification time reduces the computational and memories demand in embedded applications that requires a large CNN architecture.

KEYWORDS

Convolutional Neural Networks, Deep Learning Acceleration, Advanced Driver Assistance Systems.

1. INTRODUCTION

The use of computer vision in Advanced Driver-Assistance Systems (ADAS) for environment mapping with images turns possible the recognition of persons, lane road, animals, vehicles, and traffic signs in real-time. The first algorithms designed for computer vision were based on image processing techniques, such as colour segmentation, the histogram of oriented gradients, and cross-correlations. Image processing techniques show good performance for time operation and have an easy implementation. The drawbacks of the techniques above are loss of performance in different light conditions, severe precipitation, mist, and occlusions. In this way, the necessity of robust solutions for ADAS environments rise and, the application of neural networks and Convolutional Neural Networks (CNNs) turns a new research field.

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 109-122, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111109

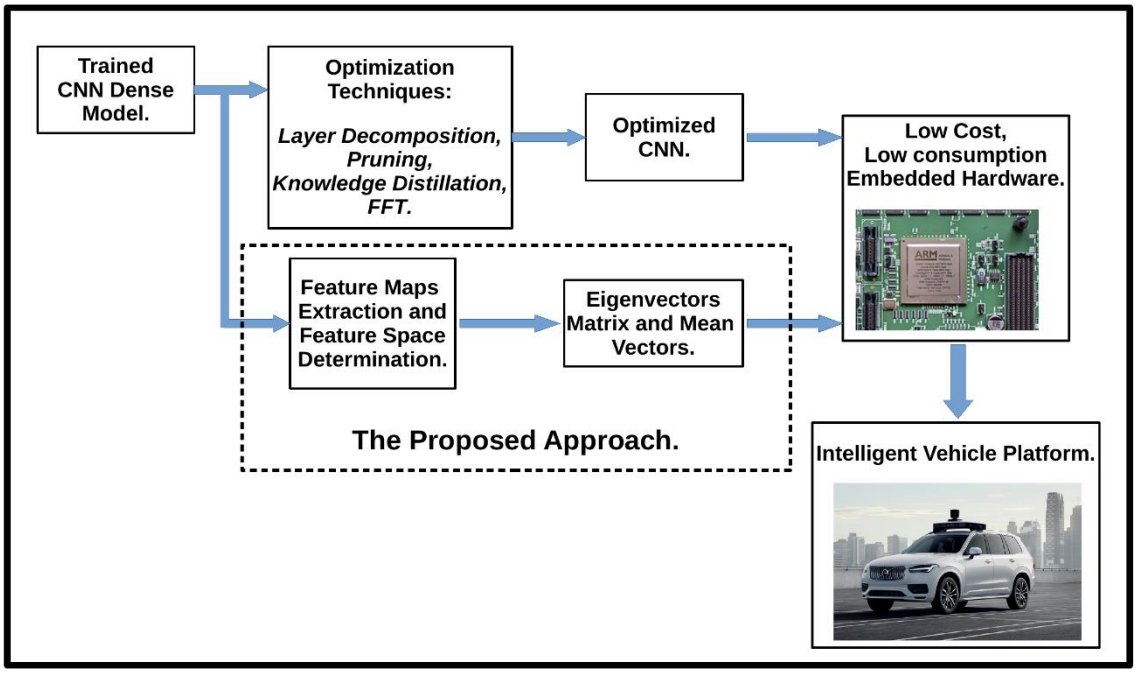


Figure 1. Illustration of the CNN reduction methods for ADAS applications. After train the dense model, the traditional methods reduces the complexity of the model. After the reduction, the embedded hardware platform host the minimal model. Differently, our proposed framework does not reduce the model complexity, however uses the kernel knowledge presents on the maps to determine the feature spaces and use it for the classification process.

At the end of the ’90s, Lecun*et.al* published in [1] and [2] the development and application of Convolutional Neural Networks (CNN). CNN is considered a Deep Learning algorithm and achieved the best performance in image recognition, localization, and segmentation tasks, compared with the traditional image processing techniques [3] and [4], mainly due to CNN’s ability to extract a large number of features from input images. When Krizhevsky *et al.*, [5] won the Imagenet-2012 challenge, the breakthrough occurred, achieving a significant performance improvement than previous architecture. Another successful architecture is the deep neural network proposed in [6], called VGG-16 (Visual Geometry Group), which showed the importance of depth architecture to achieve high-performance classification tasks.

Large-scale CNN networks such as VGG-16 is applicable in many classification tasks, including ADAS, mainly used for visual detection and mapping the environment. Computer vision is a essential subsystems that compose ADAS used in vehicles mainly for safety, lane keeping, and collision avoidance systems. CNN is often used in self-driven vehicles to detect and recognize vehicles, persons, animals, and other obstacles. However, CNN’s application for real-time operation requires more attention when running in vehicle’s embedded platforms due to the need for high-spec hardware (RAM, CPU, and GPU). Some new approaches proposes to deal with the real-time requirements as the problem mentioned above. One is the development of CNN architectures with high performance and low computation cost [7] or compact and less powerful versions of large-scale architectures [8]. Other research lines focus on accelerating the classification time of large CNNs using strategies to optimize kernel activations [9]. The method uses the Single Value Decomposition (SVD) as a low-rank approximation approach to accelerate the classification time of very deep CNNs. Other researches that present methods for acceleration of CNNs are [10] and [11]. In [12], the authors present a study on the relationship between operating speed and accuracy in CNN network’s applications used in the object detection within

an image. That work conducts a study of the balance between accuracy and time of operation through variations of characteristics of the architectures, such as extractors of features, resolution of the input images, etc. The study published in [13] proposes to factorize the convolutions into 2D kernels instead of 3D convolutions. The work reports that the accuracy did not reduce severely and, the time of classification and training decreased a lot. The method proposed in [14] is an evolution of pruning methods for large CNN architectures [15]. The method's purpose is to use the PCA to the network analysis to discover and determine which kernels produce the largest variance results during the training process, thus reducing the accumulated error. Using those kernels and layers, the CNN model is retrained with a compressed version of the architecture. Figure 1 shows the applicability of CNN reductions methods and our proposed framework for the ADAS platform. Unlike the methods presented previously, this paper presents a new approach applied to any large-scale CNN architectures. It uses feature maps for determining the reduced dimensional space. Using this new space, we generate low dimensional samples and train an external classifier. In figure 2 show our proposed method. Despite the universality of our method, we will use the VGG-16 network as the basis for the experiments to validate our method's effectiveness. The rest of the paper is organized as follows. Section II describes a basic CNN structure and an overview of the PCA and MPCA method applied to pattern recognition in images, section III describes the proposed method. Section IV presents the experiments and discusses the results. Finally, section V presents the conclusion.

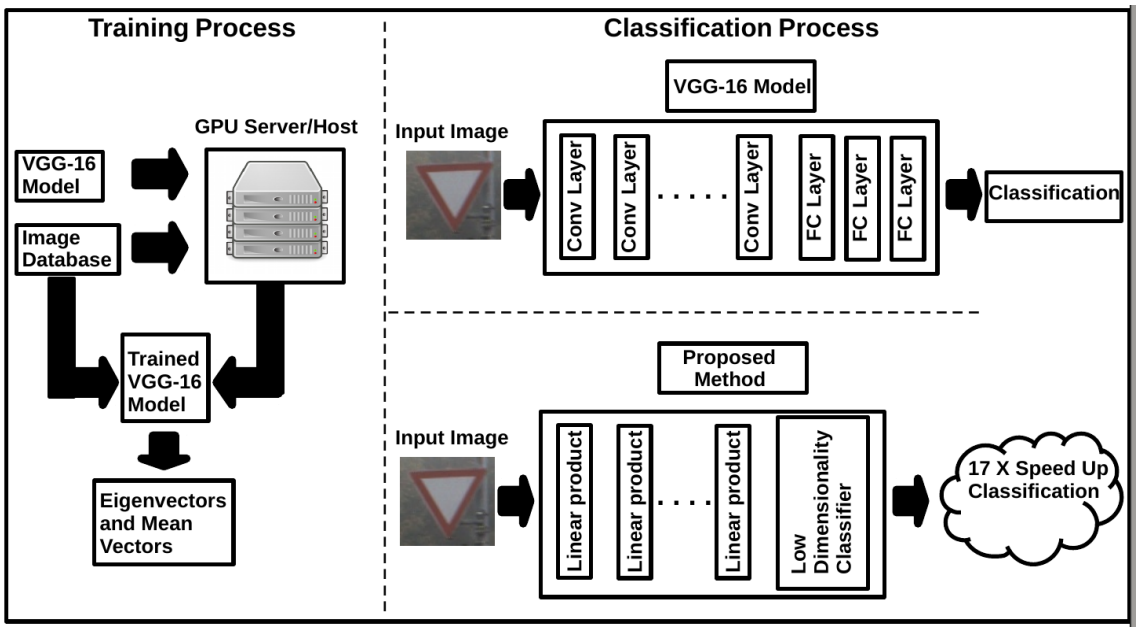


Figure 2. **Left side**: We train the VGG-16 model on the database with a cloud GPU server. With the trained model, we use the same database to extract banks of eigenvectors and mean vectors used to reduce the architecture. **Right side**: The VGG-16 model and the proposed method comparison: The substitution of the convolution processes by the chain of products accelerate the classification 17 times.

2. THEORETICAL BASEMENTS

2.1. Convolutional Neural Networks

CNN structures are usually composed of three types of layers. The first, called the convolutional layer, has the function of extracting many features from images by convolution processes between regions of the input image and the layers' kernels. Every internal kernel element is an

adjustable parameter adapted during the training phase, and the activation function determines the final output of the kernel [16]. The kernel slides by the whole image according to the parameters stride and padding. All the convolution process outputs are arranged in the feature map matrix [16], and the kernel for each convolutional layer generates the feature maps. The second layer, called sub pooling, uses the feature maps generated by previous convolutional layers. The regions of feature maps are sub-sampling, and the output of the layer is a reduced dimension feature maps. The operators of subsample can be the *maxpooling*, *meanpooling*, or *minpooling*. The maxpooling operator is the most used. Finally, the third layer, called fully connected (FC), consists of neuron units disposed of in interconnected multilayers. The input of the first FC layer consist of all flattens feature maps from the last convolutional layer. The last FC layer can be a probabilistic function or a classifier, such as *Support Vector Machines* (SVM) or *Radial Basis Functions* (RBF).

2.2. PCA and MPCA

One of PCA's main applications [17] in image processing has been the dimensionality reduction of samples. Even though PCA has 120 years, since Karl Pearson proposed it in 1901, it remains very current and useful. Fundamentally, PCA creates a centred and orthogonal basis from the data's covariance matrix, maximizing the variance corresponding to the largest eigenvalues. This orthogonal basis is used to map the input data X into this new PCA space rotating the data distribution according to the highest variance feature to the lowest nonzero variance feature. Formally, PCA will find an orthogonal matrix $\mathbf{\Phi}$ that maps $\mathbb{X} \in \mathbb{R}^n$ to $\mathbb{Z} \in \mathbb{R}^p$, where $p << n$.

The eigenvectors of $\mathbb{X}$ covariance matrix are called *Principal Components* of set $\mathbb{X}$ new feature space. The projection of any arbitrary $\boldsymbol{x}$ sample into the new PCA feature space can be defined by $\mathbf{z} = \mathbf{\Phi}^T\mathbf{x}$, where $\mathbf{\Phi}$ is an orthogonal matrix whose the *kth* column is the *kth* eigenvector from the covariance matrix $\mathbf{\Sigma} = \mathbf{\Phi\Lambda\Phi}^T$ and $\mathbf{\Lambda}$ is the diagonal matrix whose *k* is the *kth* eigenvalue of $\mathbf{\Sigma}$.
The idea behind the PCA is that the projection of any sample $\boldsymbol{x}$ from the original space to the new PCA space will not change the original distribution once PCA is a linear approach based on the covariance matrix $\mathbf{\Sigma}$ of input matrix $\boldsymbol{X}$. However, to deal with tensors in the CNN convolution layer, we need to consider a different approach, such as Multilinear PCA (MPCA) as proposed by [18].

Lu et al. [18] proposed Multilinear PCA (MPCA) for tensor objects as a multidimensional object, mainly related to videos and images. Considering a sequence of frames from a video file, $\mathbf{A} \in \mathbb{R}^{l1\times l2\times\ldots\times ln}$ will be the tensor object of nth-order and each frame $\mathbb{U}_{lk} \in \mathbb{R}^{i\times j}$, where k = 1, 2,…, N. Although, MPCA will reduce the total dimensionality from N ×i×j to P ×i×j, where P << N.

The MPCA requires a stack of input data $\mathbf{X}_k \in R^{i\times j}$ to project the tensor object $\mathbf{A}$ to the new reduced tensor space. The reduction occurs by the product of tensor $\mathbf{A}$ by a matrix $\mathbf{U} \in R^{in\times jn}$ denoted as $\mathbf{A}\times\mathbf{U}$, and $\mathbf{U}$ corresponds to the N projections matrices that maximize the M scatter of the tensors defined by $\boldsymbol{\psi}_{\mathbf{A}}=\mathbf{\Sigma}_M \|\mathbf{A} - \mathbf{A}_\mathbf{m}\|$, where $\mathbf{A}_\mathbf{m}$ is the mean tensor.

3. THE PROPOSED METHOD

3.1. Definition

The proposed method adapted for VGG-16 is divided into four phases, as shown in the following:

• **Phase 1**: Initial step consists of applying the pre-processing to convert all images to the gray-scale and resize them to 224 × 224 pixels.

• **Phase 2**: The original VGG-16 model is trained with these pre-processed samples.
• **Phase 3**: M image samples of the training subset, with $M < N$, are presented to the trained VGG-16 model and generates K_l feature maps for each image in each layer $l = \{1, 2, 3,..., 13\}$ were K_l is the number of kernels of the layer l. Each feature map is concatenated and arranged in the matrix $\boldsymbol{X}^{(l)}$ of size $V \times n$, where V is the product of M per K_l and, $n = H^2$, where $H \times H$ is the input size. Before applying the PCA, the mean vector of $\boldsymbol{X}^{(l)}$ is extracted and stored:

$$\boldsymbol{x}_m^{(l)} = \frac{1}{V}\sum_{i=1}^{V} \boldsymbol{x}_i \tag{3.1}$$

The covariance matrix of $\boldsymbol{X}^{(l)}$ is computed as:

$$Cov(\boldsymbol{x}^{(l)}) = \frac{1}{V}\sum_{i=1}^{V} (\boldsymbol{x}_i - \boldsymbol{x}_m^{(l)})(\boldsymbol{x}_i - \boldsymbol{x}_m^{(l)})^T \tag{3.2}$$

The p_l eigenvectors of the covariance matrix of $\boldsymbol{X}^{(l)}$ related with nonzero eigenvalues compose the matrix $\boldsymbol{A}^{(l)}$, with dimensionality $p_l \times n$. The matrix $\boldsymbol{A}^{(l)}$ and the mean vector $\boldsymbol{x}^{(l)}$ are the output of phase three.

• **Phase 4**: The last step consist of applying phase three for all layers of the model.

For each layer l, the feature maps must be resized to $H \times H$, where $H = \sqrt{p_{(l-1)}}$, except for the first layer. This resize turns possible the process of the dot product that will generate the low dimensional samples.

At the end of all phases, matrices of eigenvectors and mean vectors for all layers are generated. In the dense models, the chain of subtractions and products using the matrices of eigenvectors and the mean vectors replaces convolutional processes. This replacement accelerates the time of classification.

The main objective of this work is to reduce the overall classification time for a new image sample. We call our proposed method *Multilinear Feature Space Convolutional Neural Network* (MFS-CNN).

Figure 3 illustrates the proposed method.

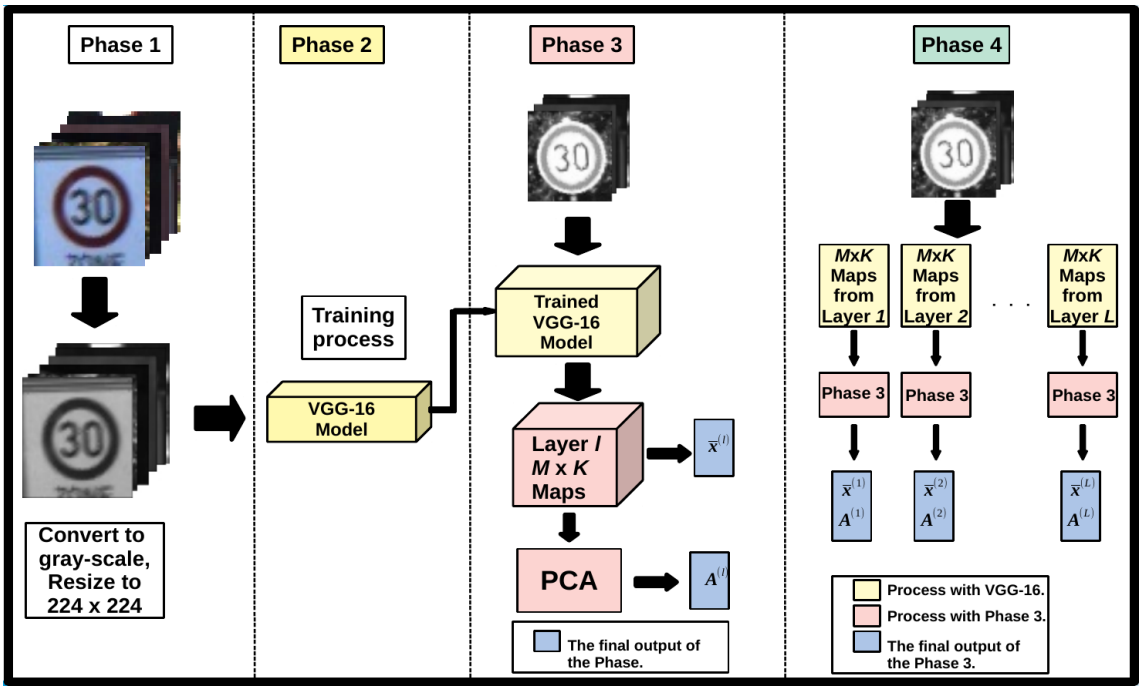


Figure 3. The illustration of the processes to obtain the matrix of eigenvectors and the mean vector for each layer. In phase one, all samples of the image database are pre-processed. The image samples are converters to grey-scale and resize to 224 × 224. After the pre-processes, phase two consists of the training and validation of the VGG-16 model. In phase three, M image samples are presented to trained VGG-16 model to generate $M \times K_l$ features maps per layer. For each l layer, the mean vector $\boldsymbol{x}^{(l)}$ and the matrix of eigenvectors $\boldsymbol{A}^{(l)}$ are computed. Phase 4 consists of computing the mean vector and the eigenvectors matrix for all layers of the original VGG-16 model.

3.2. Generating Samples with Low Dimensionality

Projecting any new image onto Feature Map Space requires resizing the image sample, *Imt*, in 224 × 224 pixels. In the second step, the new image is concatenated to vector $\boldsymbol{xt}$, $1 \times n$, with n = 50176. The projection of $\boldsymbol{xt}$ into space of the first layer, $\boldsymbol{z}(\boldsymbol{xt})^{(1)}$, $1 \times p_1$ occurs by the subtraction of mean vector $\boldsymbol{x}^{(1)}$ and the dot product with $\boldsymbol{A}^{(1)}$. The vector $\boldsymbol{z}(\boldsymbol{xt})^{(1)}$ is projected into space of the second layer by the same process above, generating $\boldsymbol{z}(\boldsymbol{xt})^{(2)}$, and then projected into space of the third layer, and repeating the process until the last layer as shown in equations 3.3, 3.4 and 3.5 respectively.

$$\boldsymbol{z}(\boldsymbol{xt})^{(1)} = (\boldsymbol{xt} - \boldsymbol{x}_m^{(1)})(\boldsymbol{A}^{(1)})^{(T)} \tag{3.3}$$

$$\boldsymbol{z}(\boldsymbol{xt})^{(2)} = (\boldsymbol{z}(\boldsymbol{xt})^{(1)} - \boldsymbol{x}_m^{(2)})(\boldsymbol{A}^{(2)})^{(T)} \tag{3.4}$$

$$\boldsymbol{z}(\boldsymbol{xt})^{(L)} = (\boldsymbol{z}(\boldsymbol{xt})^{(L-1)} - \boldsymbol{x}_m^{(L)})(\boldsymbol{A}^{(L)})^{(T)} \tag{3.5}$$

As mentioned early, the low dimensional samples are used to train and validate an external classifier that substitutes the fully connected layers of the VGG-16 model.

4. EXPERIMENTAL RESULTS

A set of experiments were conducted to evaluate the capability of MFS-CNN to speed up the classification time with minimal accuracy loss. The first experiments with six scenarios varying parameters were conducted. To exploit the best scenario, we used the cross-validation experiments at all scenarios and, the results were organized and presented in tables. To prevent overfitting, the training and validation of all classifiers use the *early stopping* method.

The difficulty of reproduction of CNN's reduction approaches turns impractical the use in experiments with these approaches. These implementations are crucial for compare our proposed method and obtain an overall situation of the proposed method in the research area.

4.1. Datasets

4.1.1. Vehicle Image Database

Universidad Politécnica de Madrid [19] to evaluate computer vision algorithms for automotive applications built it. This image database is composed of 7325 images of road lanes with the presence of vehicles or not. The images belonged to two classes and were collected under a different angle, environments, and light conditions. The images have dimensions of 64 × 64 pixels. Because of the unbalance of the database, with a different number of images per class and corrupted images, we used only 5400 of 7325 available. The best result achieved in the training process of model VGG-16 was 98.7% accuracy in the test set after 31 epochs, a learning rate of 10^{-6}, and a mini-batch size of 20.

4.1.2. German Traffic Sign Detection Benchmark (GTSDB)

This image database is available at *Institut Für Neuroinformatik* of *Ruhr-Universitat Bochum* [20]. The database contains more than 50,000 images of traffic signs distributed in 43 classes. Simultaneously, the images were captured in several environments, different angles of view, light conditions, and different dimensions. We randomly select four classes of images to conduct the experiments. The best result achieved in the training process of the VGG-16 model was 99.7% of accuracy in the test set at 24 epochs, with learning a rate of 10^{-6} and a mini-batch size of 100.

4.2. Experiments Scenario Description

The experiments consist of the training and test of an external classifier with the samples projected on layers. The speedup (SPU) of the time for classification is measured by:

$$SPU = \frac{t_{VGG}}{t_{MFS\_CNN}} \tag{4.1}$$

Where t_{VGG} is the time of classification of an arbitrary sample by trained VGG-16 model and t_{MFS_CNN} is the time of classification by our proposed method.

Before initializing the experiments, we have to compute the low dimensional samples considering the first seven and, after this, all layers spaces. For the first layer, were extracted V - 1 eigenvectors and, for remains layers $p_{(l-1)}$. To compose the matrices of eigenvectors it was used different numbers of eigenvectors p_l for each layer. The first ranked eigenvectors chosen from each layer that produced the best result were: 6889, 6724, 4096, 3364, 2304, 2116, 1600, 1444, 1156, 1024, 900, 784, 676, from the first to the last layer, respectively. We used different

scenarios to conduct the experiments. The experiments use all or part layer spaces to obtain the final vector. Besides, different combinations of eigenvectors to compose eigenvectors' matrix, using these vectors to train and validate the external classifier. In the following, we describe the scenarios used in the experiment.

The scenarios are summarized in table I and the results of each scenario are presented in tables IV to IX, respectively. Before starting the experiments to check if the method effectively speeds up the classification time, we conducted cross-validation experiments to define which classifiers achieve higher accuracy values.

Table 1. Experiments Scenario Description

Scenario	Layers Selected	Eigenvectors Selection
1	All 13 layers	First Ranked
2	First seven layers	First Ranked
3	All 13 layers	Last Ranked
4	All 13 layers	Randomly
5	First seven layers	Last Ranked
6	First seven layers	Randomly

4.2.1. Cross-Validation Experiments

Before the random selection for subsets mounting, we set the k parameter of the k-fold algorithm as five, which always reserves 20% of total samples to test.

For each k-fold round, the VGG-16 model is trained with *k -1* subsets designed for the training process and validate with remain. We used M = 1000 randomly selected samples from the training subsets for generating the feature maps. All samples of the training subsets generate the low dimensional samples to train the external classifier. The proposed method was validated with the low dimensional samples generated with the same image sample subset used to validate the original VGG-16 model.

In the experiments described in this section were used the following external classifiers: *Adaboost, Decision Tree, K-Nearest Neighbour, Naive Bayes, Random Forest* and *Multi-Layer Perceptron and SVM*.

The best cross-validation results were achieved considering scenario 1. The tables 2 and 3 presents the best results from each classifier using validation subsets.

In the database 1 [19], the best value achieved by the Adaboost classifier occurred when the number of estimators was set to 200. In the KNN classifier, the best value for the *k* parameter for all folds was 1. The multi-layer perceptron classifier has three layers. The first layer has 1024 units; the intermediary layer has 256 and, the output layer 2 units. The activation function for the hidden layers and the output layer are *Relu* and *softmax*, respectively. The learning rate was fixed in 10^{-4}, and the mini-batch size was 20. The best accuracy value in the fold was achieved after 24 epochs. The SVM classifier utilized the *linear kernel*.

Table 2. Cross-Validation Accuracy Performance on Database 1, best results highlighted in bold.

Classifier	Fold 1	Fold 2	Fold 3	Fold 4	Fold 5
Adaboost	93.0%	92.2%	91.9%	92.9%	92.1%
D. Tree	85.6%	83.1%	84.6%	84.4%	84.4%
K-NN	90.0%	88.1%	89.4%	90.3%	89.5%
MLP	97.1%	97.2%	96.8%	97.0%	**97.3%**
N. Bayes	85.1%	83.1%	82.0%	83.9%	82.6%
R. Forest	86.1%	86.9%	88.8%	88.4%	87.8%
SVM	88.8%	88.4%	77.5%	83.0%	89.0%
VGG-16	97.8%	98.4%	97.5%	97.6%	**98.8%**

In the database 2 [20], due to a large amount of memory required to store eigenvectors' matrices, we randomly choose four classes of 43. The best value achieved by the Adaboost classifier occurred when the number of estimators was set as 200. In the KNN classifier, the best value for the *k* parameter for all folds is 1. The multilayer perceptron classifier has three layers. The first layer has 1024 units, the intermediary layer has 1024 and, the output layer four units. We used as activation function for the hidden layers and the output layer are *Relu* and *softmax*, respectively. The learning rate has fixed in 10^{-5}, and the mini-batch size is 25. The best accuracy value in fold 1 occurred at 26 epochs. The SVM classifier utilized the *Radial Basis Function kernel*.

Table 3. Cross-Validation Accuracy Performance on Database 2, best results highlighted in bold.

Classifier	Fold 1	Fold 2	Fold 3	Fold 4	Fold 5
Adaboost	93.6%	93.7%	93.2%	92.2%	91.8%
D.Tree	87.6%	88.3%	89.1%	87.5%	88.5%
K-NN	97.2%	97.2%	97.9%	98.1%	97.7%
MLP	**99.6%**	99.2%	99.2%	99.5%	99.2%
N. Bayes	68.7%	69.7%	69.4%	67.0%	68.4%
R. Forest	83.1%	83.2%	84.3%	84.0%	83.7%
SVM	97.5%	98.0%	97.7%	98.2%	97.8%
VGG-16	**99.7%**	98.5%	98.7%	99.4%	99.2%

Comparing the results presented in the tables, the classifiers that achieved the best overall results were the MLP and SVM, except for the first image database were Adaboost overcome SVM.

4.2.2. Speedup Experiments

The accuracy values achieved in the scenario 1 using all databases are closest to the original VGG model. Table 4 summarizes the results achieved in image databases 1 and 2.

Table 4. Speedup Performance on Database 1 and 2 for Scenario 1, best results highlighted in bold.

Database 1		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	**97.3%**	**16.9**
MFS-CNN-Adaboost	93.0%	17.1
VGG-16	**98.8%**	-
Database 2		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	**99.6%**	**16.8**
MFS-CNN-SVM	98.2%	16.8
VGG-16	**99.7%**	-

As expected in scenario 1, the loss compared with VGG-16 is minimal. The minimal loss probably occurs by the use of ordered high representation eigenvectors. That produce high information integrity as related by various works that use the PCA method. However, the best performance of the Adaboost classifier overcome SVM will investigate further.

We can easily conclude that the acceleration compared with scenario number 1 is due to the reduced number of layers. The global augment of loss can suggest that the performance is related to the totality of layers used in the classification task. Despite scenario 3 use all layers, the selection of eigenvectors with less associated eigenvalues decreases the global performance. The use of a random selection of eigenvectors in scenario 4 reduces performance smoothly, but both the accuracy and acceleration remain close to scenario 1. This minimal loss and high acceleration can indicate high redundancy of eigenvectors.

We can observe that the selection of eigenvectors is irrelevant when the method uses only the first layers. However, we can conclude that the complete solution for architecture reduction uses all layer spaces. Although, understand the operation in the first layers may elevate the acceleration without increase the loss.

Table 5. Speedup Performance on Database 1 and 2 for Scenario 2, best results highlighted in bold.

Database 1		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	95.1%	17.3
MFS-CNN-SVM	83.6%	17.5
VGG-16	**98.8%**	-
Database 2		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	96.2%	17.2
MFS-CNN-SVM	98.2%	16.8
VGG-16	**99.7%**	-

Table 6. Speedup Performance on Database 1 and 2 for Scenario 3, best results highlighted in bold.

Database 1		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	96.4%	16.9
MFS-CNN-SVM	86.6%	16.5
VGG-16	**98.8%**	-
Database 2		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	98.4%	16.7
MFS-CNN-SVM	96.6%	16.6
VGG-16	**99.7%**	-

Table 7. Speedup Performance on Database 1 and 2 for Scenario 4, best results highlighted in bold.

Database 1		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	96.9%	16.9
MFS-CNN-SVM	88.8%	16.5
VGG-16	**98.8%**	-
Database 2		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	98.7%	16.7
MFS-CNN-SVM	97.7%	16.8
VGG-16	**99.7%**	-

Table 8. Speedup Performance on Database 1 and 2 for Scenario 5, best results highlighted in bold.

Database 1		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	95.0%	17.2
MFS-CNN-SVM	83.6%	17.3
VGG-16	**98.8%**	-
Database 2		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	95.8%	17.1
MFS-CNN-SVM	95.8%	17.4
VGG-16	**99.7%**	-

Table 9. Speedup Performance on Database 1 and 2 for Scenario 6, best results highlighted in bold.

Database 1		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	95.2%	17.1
MFS-CNN-SVM	83.2%	17.0
VGG-16	**98.8%**	-
Database 2		
Classifier	**Accuracy**	**SPU**
MFS-CNN-MLP	96.1%	17.0
MFS-CNN-SVM	95.5%	17.3
VGG-16	**99.7%**	-

The VGG-16 model with 10 classes uses approximately 1.6 GB of RAM. The expansion of memory occupancy occurs during the training process. When the database has many images, the training process on computers with limited memory space without GPU turns the process impractical.

The memory occupied by the proposed method occurs mainly due to the tensor of maps stored in the memory, with $H \times H \times M \times K_l$ bytes per layer, where H represents the dimensions of maps. We observed that the growth of memory occupation is dependent on the number of M samples. The value of M needs to be great when the database has a large number of samples and classes. This rise is due to the necessity of representation of the total diversity of the database. Due to this drawback, the extraction of matrices of eigenvectors and mean vectors is infeasible when the image database has a large number of samples.

When the classification process of a new sample occurs in the VGG-16 model, the occupation of memory is due mainly to the storage of part of kernels weighs and the creation of the *Kl* feature maps in the current layer in forwarding propagation mode. In the classification task, the proposed method occupies memories mainly with matrices of eigenvectors and mean vectors. The size of low dimensional samples is only of few kilobytes.

To perform the experiments, we used the *Google Colab service*. The service offers a cloud computing server with 32 GB of RAM and an *Nvidia Tesla K80 GPU, Nvidia Tesla T10* or similar. The service was used only to train the original VGG-16 model. To extract the feature maps, compute the eigenvectors, train the external classifiers, and execute the test experiments, it was used a personal computer with 8 GB of RAM and an *Intel Core i5 Vpro* processor.

All processes for extracting and storage the matrices of eigenvectors and mean vectors lasted six hours. The size of archives totalled 685 MB of RAM for 10 classes. The proposed method

achieved satisfactory results in the experiments but demonstrates be not feasible with many classes and samples. This drawback is due to the high occupancy memory by the tensors.

Additionally, the method is not effective when the objects of interest in the images have a high variance of size and position and not aligned since the method is based on linear PCA.

In recent years, different works achieved good results by pruning [22] or compressing [23] large CNN architectures. However, our approach uses the ranked eigenvectors for reducing the classification time and not reducing the size of the architecture.

5. CONCLUSIONS

In this paper, we presented an alternative method that focuses on the knowledge's of CNN's kernels associated with a low complexity classifier to reduce the time of classification while preserving part of the performance reached by CNN.

The results have shown that MFS-CNN is efficient in ADAS classification problems with a limited number of classes. The method is helpful in classification applications that use CNNs for embedded applications, with low computational resources in computer vision applications for the autonomous vehicle. The experiments with scenario 4 and 6 showed a reasonable accuracy with a high speed-up rate. In scenarios 4 and 6, we randomized the eigenvectors selection and, even though the loss in accuracy was minimal. It is an indication that we have a high redundancy spread along all eigenvectors.

In the next step of this research, we will extend the application for other ADAS problems, such as license plate and vehicle type classification. The low consumption of the method turns the implementation and operation appropriate to the vehicular low-cost embedded platforms. These platforms are used mainly for performing real-time computer vision tasks.

In addition, we will evaluate a method to choose the minimum amount of the most significant eigenvectors, not considering only the eigenvalues as mentioned in this work, but the accuracy and reduced time for classification. The new version of MFS-CNN will handle reasonably a high number of samples and classes, outperforming the current drawback.

REFERENCES

[1] YannLeCun and YoshuaBengio, (1998) "Convolutional networks forimages, speech, and time series", *The handbook of brain theory and neural networks*. MIT Press, Cambridge, MA, USA, 255–258.

[2] Y. Lecun, L. Bottou, Y. Bengio and P. Haffner , (1998) "Gradient-based learning applied to document recognition", *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278-2324.

[3] H. R. Kher and V. K. Thakar, (2014) "Scale Invariant Feature Transform Based Image Matching and Registration", *Fifth International Conference on Signal and Image Processing*, Bangalore, India, pp. 50-55.

[4] N. Dalal and B. Triggs, (2005) "Histograms of oriented gradients for human detection", *IEEE Computer Society conference on Computer Vision and Pattern Recognition (CVPR'05)*, San Diego, CA, USA, 2005, pp. 886-893.

[5] Alex Krizhevsky, IlyaSutskever, and Geoffrey E. Hinton, (2012) "ImageNet classification with deep convolutional neural networks", *In Proceedings of the 25th International Conference on Neural Information Processing Systems - Volume 1 (NIPS'12)*, Curran Associates Inc., Red Hook, NY, USA, 1097–1105.

[6] K.Simonyan and A. Zisserman, (2014) "Very deep convolutional networks for large-scale image recognition", *in International Conference on Learning Representation (ICLR)*,San Diego, CA, USA.

[7] Sandler, M. et al, (2018) "Mobilenetv2: Inverted residuals and linear bottlenecks", *in proceedings of the IEEE conference on computer vision and pattern recognition*. [S.l.: s.n.], p. 4510–4520.
[8] Huang, R.; Pedoeem, J.; Chen, C., (2018) "*Yolo-lite: A real-time object detection algorithm optimized for non-gpu computers*", In: . [S.l.: s.n.], p. 2503–2510.
[9] X. Zhang, J. Zou, K. He and J. Sun., (2016) "Accelerating Very Deep Convolutional Networks for Classification and Detection", *Pattern Analysis and Machine Intelligence*, vol. 38, no. 10, pp. 1943-1955.
[10] V. Vanhoucke, A. Senior, and M. Z. Mao, (2011) "Improving the speed of neural networks on CPUs,"*in Deep Learning and Unsupervised Feature Learning Workshop*, NIPS.
[11] E. Denton, W. Zaremba, J. Bruna, Y. LeCun and R. Fergus, (2014) "Exploiting linear structure within convolutional networks for efficient evaluation", *in Advances in Neural Information Processing Systems (NIPS)*.
[12] J. Huang et al., (2017) "Speed/Accuracy Trade-Offs for Modern Convolutional Object Detectors", *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Honolulu, HI, 2017, pp. 3296-3297.
[13] M. Wang, B. Liu and H. Foroosh, (2017) "Factorized Convolutional Neural Networks", *2017 IEEE International Conference on Computer Vision Workshops (ICCVW)*, Venice, 2017, pp. 545-553.
[14] I. Garg, P. Panda and K. Roy, (2020) "A Low Effort Approach to Structured CNN Design Using PCA", *in IEEE Access*, vol. 8, pp. 1347-1360.
[15] J. M. Alvarez and M. Salzmann., (2017) "Compression-aware training of deep networks", *CoRR*, vol. abs/1711.02638.
[16] Ian Goodfellow, YoshuaBengio, and Aaron Courville., (2016) "Deep Learning", *The MIT Press*.
[17] I.T Jolliffe, (2002) "Principal Components Analysis", 2nd Ed. *Springer Series in Statistics*.
[18] H. Lu, K. N. Plataniotis and A. N. Venetsanopoulos, (2008) "MPCA: Multilinear Principal Component Analysis of Tensor Objects", *in IEEE Transactions on Neural Networks*, vol. 19, no. 1, pp. 18-39.
[19] J. Arrospide, L. Salgado, M. Nieto, (2012) "Video analysis based vehicle detection and tracking using an MCMC sampling framework", *EURASIP Journal on Advances in Signal Processing*, vol. 2012.
[20] S. Houben, J. Stallkamp, J. Salmen, M. Schlipsing, C. Igel, (2013) "Detection of Traffic Signs in Real-World Images: The German Traffic Sign Detection Benchmark", *International Joint conference on Neural Networks*, 1288, 2013.
[21] Krizhevsky, Alex, (2012) "Learning Multiple Layers of Features from Tiny Images, *University of Toronto*, Sourced from Microsoft Academic*https://academic.microsoft.com/paper/3118608800*.
[22] X. Ruan et al., (2020) "EDP: An Efficient Decomposition and Pruning Scheme for convolutional Neural Network compression", in *IEEE Transactions on Neural Networks and Learning Systems*.
[23] X. Yu, T. Liu, X. Wang and D. Tao, (2017) "On Compressing DeepModels by Low Rank and Sparse Decomposition", *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Honolulu,HI, 2017, pp. 67-76.

AUTHORS

Michel André L. Vinagreiro Is graduate in engineering, master's student and researcher with Laboratory of Integrated systems, Escola Politecnica da Universidade de Sao Paulo, Sao Paulo, Sao Paulo, Brasil.

Edson C. Kitani Is P.h.D degree by Escola Politecnica da Universidade de Sao Paulo andgraduation professor in Fatec Santo Andre, Santo Andre, São Paulo, Brasil.

Armando AntonioM. Lagana Is P.h.Ddegreeby Escola Politecnica da Universidade de Sao Paulo, graduation professor and researcher with Laboratory of Integrated systems, Escola Politecnica da Universidade de Sao Paulo, Sao Paulo, Sao Paulo, Brasil.

Leopoldo R. Yoshioka Is P.h.D degree by Tokyo Institute of Technology, graduation professor and researcher with Laboratory of Integrated systems, Escola Politecnica da Universidade de Sao Paulo, Sao Paulo, Sao Paulo, Brasil.

PARALLEL EVOLUTIONARY BICLUSTERING OF SHORT-TERM ELECTRIC ENERGY CONSUMPTION

Diego P. Pinto-Roa[1,4*], Hernán Medina[4], Federico Román[4], Miguel García-Torres[1,2], Federico Divina[1], Francisco Gómez-Vela[1], Félix Morales[1], Gustavo Velázquez[1], Federico Daumas[1], José L. Vázquez-Noguera[1], Carlos Sauer Ayala[3] and Pedro E. Gardel-Sotomayor[5]

[1]ComputerEngineerDepartment, Universidad Americana, Paraguay,
[2]Division of Computer Sience, Universidad Pablo de la Ovide, Seville, Spain
[3]Facultad de Ingeniería, Universidad Nacional de Asunción, Paraguay
[4]Facultad Politécnica, Universidad Nacional de Asunción, Paraguay,
[5]Universidad Católica de Asunción, Ciudad del Este, Paraguay

ABSTRACT

The discovery and description of patterns in electric energy consumption time series is fundamental for timely management of the system. A bicluster describes a subset of observation points in a time period in which a consumption pattern occurs as abrupt changes or instabilities homogeneously. Nevertheless, the pattern detection complexity increases with the number of observation points and samples of the study period. In this context, current bi-clustering techniques may not detect significant patterns given the increased search space. This study develops a parallel evolutionary computation scheme to find biclusters in electric energy. Numerical simulations show the benefits of the proposed approach, discovering significantly more electricity consumption patterns compared to a state-of-the-art non-parallel competitive algorithm.

KEYWORDS

Biclustering, Big data, Electric energy consumption, Parallel evolutionary computation.

1. INTRODUCTION

The electricity demand is continuously growing, due to different reasons, e.g., population increment, but even lifestyle that demands more energy. For this reason, it is essential to monitor the distribution-level consumption to detect abnormal activity, such as a higher than usual demand on some systems. Doing that that would allow the system managers to carry out actions that can correct such abnormal situations.

Different data analysis techniques are usually used in the processing of these data, such as classification [1,2], forecasting [2–8], and clustering [9–12]. To this aim, biclustering can come in handy. In fact, in biclustering, it is possible to group data in two dimensions simultaneously; an example is a bicluster that can group energy consumption and time.

Biclustering has been mostly applied in bioinformatics, particularly in the context of microarray data. The primary purpose is to find subsets of genes presenting similar patterns, in terms of

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 123-137, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111110

expression values, under a subset of experimental conditions [13]. For instance, in [14], a scatter search approach based on linear correlations among genes is used to find biclusters. In [15], the authors proposed a multi-objective evolutionary algorithm (MOEA) to detect biclusters presenting particular characteristic. Biclustering has also been applied in other fields, such as social network datasets [16] or text mining [17]. In [18], a biclustering method identifies the most suitable group of user friends in social network datasets. In [19], a multi-objective biclustering algorithm was applied for the first time to the time series of the electricity consumption in smart buildings.

The energy consumption data can be usefully treated as time series data over a period. These time-series data are extensively used in different applications such as science, engineering, finance, economics, communications, control, health care, government, among others [22,21]. Clustering time series, which can be defined as identifying the homogeneous groups of time-series data based on their similarity [22], is an important technique that can provide knowledge from raw energy data [23]. Traditional clustering techniques are not always enough in all applications because these techniques usually only look for similarities in the entire time series. In some cases, finding similarities over specific periods is significant.For example, finding consumers with shared electricity consumption characteristics at limited periods, like peak demand hours, can yield better customer segmentation. Good customer segmentation can improve the performance of demand response programs [24]. Biclustering methods could fit to study concrete periods on energy consumption time series [22]. Biclustering consists of simultaneous partitioning of samples and their attributes (features) into subsets (classes). Samples and features classified together are supposed to have high relevance to each other [19].

Although competitive techniques addressed the bicluster problem, there is a large margin to be improved as the solution space grows, as is the case with energy consumption time series. In this context, parallel computing has emerged as a promissory alternative. The parallel-evolutionary computation finds satisfactory solutions reducing the computation time in high complexity problems [26]. Consequently, in this paper, we propose developing a parallel-computing architecture extending one of the most competitive state-of-the-art techniques presented by Divina et al. [19] to the energy consumption time series.

The paper is organized as follows. Section 2 presents the relate works while Section 3 presents an introduction of the electric energy consumption data and some basic notions of biclustering and evolutionary computation. Section 4 describes the procedures of the proposed Parallel Evolutionary Biclustering, while Section 5 shows the data, the simulation setup, and results. Finally, Section 6 gives the main conclusions and future works.

2. RELATED WORKS

Understanding different patterns of energy consumption, or measuring the environmental impact of energy production, can help in the development of new strategies to respond to the growing energy demand [27] and, therefore, to have a more sustainable energy policy respectively [28].
Many papers have been published recently aiming at improving power consumption prediction and pattern discovery. To this end, machine learning (ML) approaches emerge as the most important [29-31].

As example, the work presented by Liu et al. [32], where the authors presented a support vector machine (SVM) method to forecasting and diagnose public buildings energy consumption based on different input parameters, such as historical energy consumption data, climatic factors and time-cycle factors. The work was carried out on a dataset from city of Wuhan (China), and their

results showed that they were able to detect that air conditioning energy consumption was abnormal for four days in September.

In a recent work presented in [33], the authors proposed a model predictive control system with adaptive machine-learning-based building models for building automation and control applications. The results show that the proposed model reduces 58.5% cooling thermal energy consumption in the office and 36.7% cooling electricity consumption in the lecture theatre, when it is compared against their respective original control.

Artificial neural networks (ANNs) stand out as one of the most important approach among the different ML-based techniques for analysis and prediction of short-term energy consumption patterns [34-36]. As representative work, the early one presented by Nizami and Ai-Garni [37], which proposed a two-layer forward-fed ANN to study how weather-related characteristics can affect the prediction of monthly electricity consumption.

Recently, new ensemble methods are also gaining interest due to their improved results by combining several techniques. As example, the work by Divina et al. [12], where the authors proposed a new strategy based on ensemble learning in order to tackle the short-term load forecasting problem. The approach was based on the predictions produced by three base learning methods.

While clustering techniques have been less used in the literature for the analysis of energy data than others ML approaches, it is worth noting that there are several relevant works in this field. For example, the work by Diao et al. [38], where the authors proposed to identify and classify behaviour of occupants with direct energy consumption outcomes and energy time use data through unsupervised clustering. The results showed that the model was able to automatically estimating energy consumption on even larger geographic scale. Another example is presented by Perez-Chacon et al. [39], where clustering techniques was also used to identify energy consumption pattern in smart cities in a big data context. The authors proposed a parallelized method, based on the study of four clustering validity indices, to extract electric energy consumption patterns in big data time series. The method was tested using electricity consumption for the years 2011–2017 for eight buildings of a public university. Finally, in a recent work by Divina et al. [16], the authors proposed the first application of a biclustering algorithm to detect anomalies in the energy consumption patter. The algorithm was applied on data from smart buildings of a Spanish university campus. The results achieved showed that the proposed approach can help policy makers in detecting irregular situations.

3. BACKGROUND

This section introduces the electric energy consumption data and provides the basic concepts of biclustering and evolutionary computation.

3.1. Electric Energy Consumption Dataset

Electric energy consumption data are usually modeled as a time series since it consists of a discrete sequence of data points measured at equal time intervals [19]. Let $Y = \{Y_i\}_{i=1}^{N}$ be a sample of N univariate time series where $Y_i = \{Y_{i,t}\}_{t=1}^{T}$ is a univariate time series characterized by T real values. Then, the sample Y can be represented through a matrix $M_{N\times T}$. On the other hand, let us define a bicluster b as a submatrix $S_{I\times J}$, with $|I| \leq N$ and $|J| \leq T$. In the context of time

series,$S_{I\times J}$ is subject to the additional condition that columns are consecutive, i.e., $J = \{j_k, j_k + 1, j_k + 2, \dots, j_k + |J| - 1\}$. Given a function $f(b)$that measures the quality of a bicluster b, the objective is to find the best B biclusters $\{b_k\}_{k=1}^{B}$ according to $f(.)$.

In our context, each time series represents a sequence of sensor data collected over time. Therefore, the data can be viewed as $N \times T$ energy consumption data matrix EM. EM is a real matrix, where each element e_{ij} represents the electric energy consumption (expressed in kWh) as measured by sensor i on sample j. We can then see a bicluster as the measurements registered by a subset of sensors over a subset of consecutive days. For example, let us look at Figure 1 a five-sensor array for 40 sample days at the left side, while three biclusters are at the right side. The bicluster arrows correspond to sensors while the columns the consecutive days where a pattern was observed.

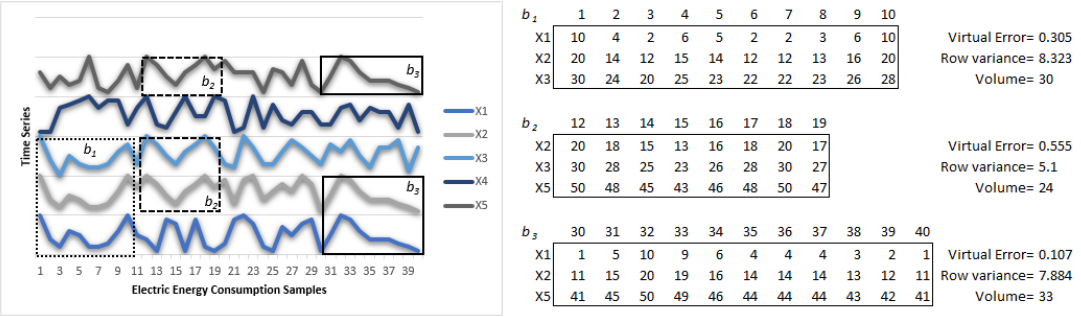


Figure 1: A five-time series with 40 electric energy consumption samples.

3.2. Bicluster quality measure

This work aims to identify a subset of sensors that present a similar behaviour during a time period. Particularly, we are interested in detecting unusual peaks of consumption [19]. From the biclustering perspective, the goal is to find large high quality biclusters that represent an interesting pattern found in the data. In this work, we use as a bicluster quality measure, the Transposed Virtual Error or simply Virtual Error (*VE*) from here [40]. *VE* computes the general tendency within the bicluster along the columns. In order to define *VE*, we first introduce the concept of virtual pattern. Given a bicluster b, the virtual pattern p is defined as the set $p = \{p_j\}_{j=1}^{|J|}$, so that p_j is given by the expression:

$$p_j = \frac{1}{|I|}\sum_{i=1}^{|I|} b_{ij}, \tag{1}$$

Where b_{ij} the elements of the bicluster b, p_j represents the average value of all sensors for a specific sample. For the bicluster b_1 given in Figure 1, the average value of the three sensors is provided in the last row p.

The *VE* of bicluster b is defined as:

$$VE(b) = \frac{1}{|I|\cdot|J|}\sum_{i=1}^{|I|}\sum_{j=1}^{|J|}\left|\hat{b}_{ij} - \hat{p}_j\right|, \tag{2}$$

where $\hat{b}_{ij}$ and $\hat{p}_j$ refer to standardized value of the elements of the bicluster b and virtual condition j as follows:

$$\hat{b}_{ij} = \frac{b_{ij}-\mu(EM_i)}{\sigma(EM_i)}, 1 \leq i \leq |I|, 1 \leq j \leq |J|, \quad (3)$$

$$\hat{p}_j = \frac{p_j-\mu(p)}{\sigma(p)}, 1 \leq j \leq |J| \quad (4)$$

With b_{ij} the elements of b, and $\mu(.)$ and $\sigma(.)$ refer to the mean and standard deviation, EM_i refers to all elements of sensor i that belong to b. The standardization of the values is introduced to be able to capture the consumption pattern of a sensor regardless of the real values registered.

The measure *VE* is a measure of coherent tendency. Lower values refer to a more robust pattern in the bicluster. A value of zero means that the bicluster contains perfectly coherent patterns. Nevertheless, the use of *VE* may yield to find biclusters characterized by flat patterns. Such flat biclusters are not interesting since we aim at finding abnormal activities, which are often related to peaks in consumption patterns. To overcome this issue, and favors fluctuating and coherent patterns, the row variance (*var(b)*) of a bicluster *b* can be used and defined as:

$$var(b) = \frac{\sum_{i\in I, j\in J}(b_{ij}-\mu(b_i))^2}{|I|\cdot|J|}, \quad (5)$$

Finally, to find large biclusters, we introduce, as another objective function, the volume of a bicluster *V(b)*, which measures the number of elements $b_{ij} \in b$. So, we aim at finding biclusters characterized by low values of virtual error *VE*, with high row variance *var(b)* and volume *V(b)*. As an example of these values, at the right side of Figure 1, we can see *VE(b)*, *var(b)*, and *V(b)* of biclusters.

3.3. Evolutionary Computation

An evolutionary algorithm (EA) [41–43] is based on the biological concepts of evolution, for example, the survival of the fittest. Such concepts are used to evolve candidate solutions toward much better solutions. In fact, an EA is a population-based stochastic iterative strategy, where an initial population of candidate solutions is evolved to improve the quality of the solutions. Usually, the initial population consists of random solutions. Genetic operators, such as selection, crossover, and mutation, are then used in order to simulate generations to obtain a new evolutionary population. These operators distinguish them from other nature inspirations like swarm artificial and physical algorithms [19]. Each evolutionary generation consists of two main processes: (a) create new candidate solutions and (b) competition for survival.

EA generates new individuals by selecting a subset of individuals from the population, performs crossover on the subset, and then injects new genetic material by mutation. Selected individuals, called parents, will then be used to generate new solutions called offspring. The descendants inherit attributes of the ancestor via the crossover and not present via mutation. This dual approach is the main strength of EA as a search algorithm, a concept called knowledge exploitation vs. exploration.

Another fundamental concept is that EA encodes solutions to be represented in individuals by chromosome. EA refers to a solution as to the phenotype and to an individual encoding it as a genotype. The literature reports many proposals to this aim, with binary string encoding being the most widely used for the easy implementation of binary crossover and mutation [44]. In this

encoding, a binary string is used, where the meaning is assigned to each bit. In this way, a solution can be encoded, and an individual can be decoded.

As previously mentioned, in each generation, some individuals are selected to generate new solutions. The selection is usually based on the quality of the solutions encoded by individuals. This means that a quality measure should be assigned to each individual. This measure is called a fitness function. The selection mechanisms usually tend to assign more probabilities of being selected to the fittest individuals. Fitness is the point of connection between EAs and the optimization problem. The fitness function design depends on the objective function of the problem. In consequence, it performs at the phenotypic level.

Once individuals have been selected, crossover and/or mutation are used to produce offspring. A crossover is used to swap genetic material between two parents, while mutation is used to introduce small random changes that can help escape local optima. These operators are applied at the genotype level.

After that offspring are generated, they compete with older individuals for surviving to the next generation. A common strategy, called elitism, is also to let the fittest individual of a generation survive to the next generation.

EAs have shown good performance in exploring huge search spaces, which is the space of all possible solutions to a problem. This capacity is due to the intrinsic parallelism achieved by the population search and the stochastic nature of EAs, which allow them to efficiently search for a solution and with the capability of escaping local optima. Initialization, selection, crossover, and mutation are stochastic procedures. In this way, EAs represent a strong alternative to greedy heuristic and competitive metaheuristic [19].

EAs have been successfully used in various problems, such as planning [44], parameter settings [45], design [46,47], knowledge extraction [48], feature selection [49], planification [50,51], simulation and identification [52], control [53] and classification [44–57].

The problem of finding a set of biclusters with some desirable features on a given matrix can be addressed as a search problem. In this case, the solution space contains all possible biclusters that can be obtained from the matrix.

4. PARALLEL BICLUSTER SEARCH

In this section, we will describe our proposed parallel version of the algorithm Sequential Covering (SC) [13], called PSC (Parallel SC), aimed at reducing the computational time required by the algorithm. In order to implement our proposal, we decided to employ a master/slave model. First, we describe the original version of the SC algorithm, and then we will provide details on its parallelization.

4.1. Sequential Covering

In brief, SC implements a sequential covering strategy, which consists of calling several times an evolutionary biclustering algorithm (EBI) until a stopping criterion is reached. SC finds biclusters with maximum volume while minimizing the effect of overlapping among biclusters. The general scheme of SC is shown in Figure 2.

Procedure SC
begin
1:Initialize L to ∅;
2: $wp(e_{ij}) \leftarrow \emptyset$
3:**while (~**Stopping Criterion)
4: $b \leftarrow$ EBI;
5: **if** $b \neq \emptyset$ **then**
6: Add b to L;
7: Update wp (e_{ij});
8: **else** $b = \emptyset$
9: stop;
10: **end while**
end

(a) Pseudocode of the SC procedure

Procedure EBI
begin
1: Initialize population;
2: Evaluate population;
3:**while (~**Stopping Criterion)
4: Select parents;
5: Cross parents;
6: Mutate offspring;
7: Evaluate offspring;
8: Update population;
9: **end while**
10:**return***b*
end

(b) Pseudocode of the EBI procedure

Figure 2: General scheme of the original EBI procedure.

Given a threshold δ, EBI returns either a bicluster or nothing depending on whether the virtual error of the bicluster is lower than δ or not. The biclusters found are stored in a list L and the stopping criterion is reached after running the procedure a maximum number of times. In order to avoid overlapping among biclusters as much as possible, each element of the input energy matrix e_{ij} is given a weight w_{ij} whose value depends on the number of biclusters to which e_{ij} belongs. In particular, the weights are defined as in equation 5.

$$w_p(e_{ij}) = \begin{cases} 0 & if\ |Cov(e_{ij})| = 0 \\ \dfrac{\sum_{n \in N, m \in M} e^{|Cov(e_{mn})|}}{e^{|Cov(e_{ij})|}} & if\ |Cov(e_{ij})| > 0 \end{cases} \quad (6)$$

In the above equation, N is the number of rows, M the number of columns, $|Cov(e_{ij})|$the number of biclusters to which e_{ij} belongs to. As shown, higher values of the weight correspond to a larger number of biclusters containing an element.

Figure 2b outlines the pseudocode of the EBI. It initializes the initial population with biclusters containing a single element and then, such population evolves employing recombination of selected pairs of parents and crossover and mutation operators. Parents are selected using a tournament approach. The crossover and mutation operators have a probability associated of p_c = 0.85 and p_m = 0.2. EBI is an elitist algorithm where the best individual survives to the next generation. The evolution stops after a maximum number of generations (g_{max}). Finally, elitism is also applied with a probability of p_e = 0.9, the best individual replaces the worst in the new population. The best individual is returned if it is a δ-bicluster.

Individuals encode a single bicluster using an array of $N + T$ bits. The first N bits are associated to each sensor while the other T bits to each electrical energy consumption sample. Figure 3 shows an example of individual encoding a bicluster for a matrix of dataset of N = 5 sensors and

T = 40 electrical energy consumption samples. The encoded bicluster contains $|I|$ = 3 rows and $|J|$ = 11continuous columns, i.e., b = [01101000000000001111111111100000000000000000000].

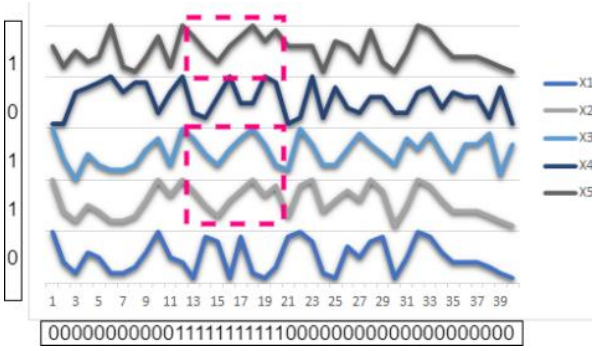


Figure 3: Example of an individual encoding a bicluster containing three rows and eleven continuous columns.

The fitness function of an individual b, in EBI, is defined as follows:

$$f(b) = \frac{VE(b)}{\delta} + \frac{1}{var(b)} + penalty + w\_d, \tag{7}$$

where *VE(b)* is the virtual error of the bicluster b and *var (b)* is the variance associated with the sensors in the bicluster. *penalty* is computed as:

$$penalty = \sum_{i \in I, j \in J} w_p(e_{ij}) \tag{8}$$

with I and J corresponding to the sensors and continuous days belonging to the bicluster b. *penalty* measures the sum of the weights of each element that belongs to b and its purpose is to avoid overlapping among biclusters. $w_p(e_{ij})$ is calculated using the expression (5). Finally, w_d is given by the expression:

$$w\_d = w_V \cdot \left(w_r \cdot \frac{\delta}{row_b} + w_c \cdot \frac{\delta}{col_b} \right) \tag{9}$$

where w_V is a weight associated with the volume of the bicluster, row_b and col_b refer to the number of sensors and continuous days of a bicluster, respectively, and w_r and w_c correspond to the weights assigned to the number of sensors and continuous days, respectively. The search bias can vary by changing the values of the weights. The final goal of EBI is to minimize the fitness function. Following the recommendations of [38], the values were set to w_V = 1, w_r = 1 and w_c = 10.

4.2. Parallel Sequential Covering

The algorithms have problems finding global optimal when the search space is huge, as in the case of bicluster search. This is due to the unavoidable convergence in regions of good

performance that not necessarily contain the global optima. To overcome this drawback, it is necessary to perform several independent runs. Each independent run has a different initial population and a different convergence region.

The simulation runs an EA sequentially or parallelly. The latter reduces the computational time by using the available computational resources.

In this context, parallelization of evolutionary algorithms emerges as a critical strategy in high-performance computing [57, 58]. Among the different parallelization strategies, we initially applied the master-slave parallelization. In this approach, a central computer, the master, distributes the tasks to the different worker computers, the slaves, to perform the tasks independently. The workers return the results to the master, who collects and processes the result. As mentioned above, Parallel Sequential Covering (PSC) is the proposed adaptation of SEBI to a master-slave architecture. Basically, PSC increases the explored search space size by running, in parallel, the SC procedure. The details about the adaptation are given in Figure 4. First, the master receives, as input, the data and runs the SC procedure on each slave. The input data contains energy matrix and evolutionary parameters. Since each SC returns a maximum number of B biclusters, the master will receive, at the end of the executions, a total of at most $SL \cdot B$ biclusters, with SL the number of slaves. Finally, the set of biclusters L will be composed of the union of each L_i returned.

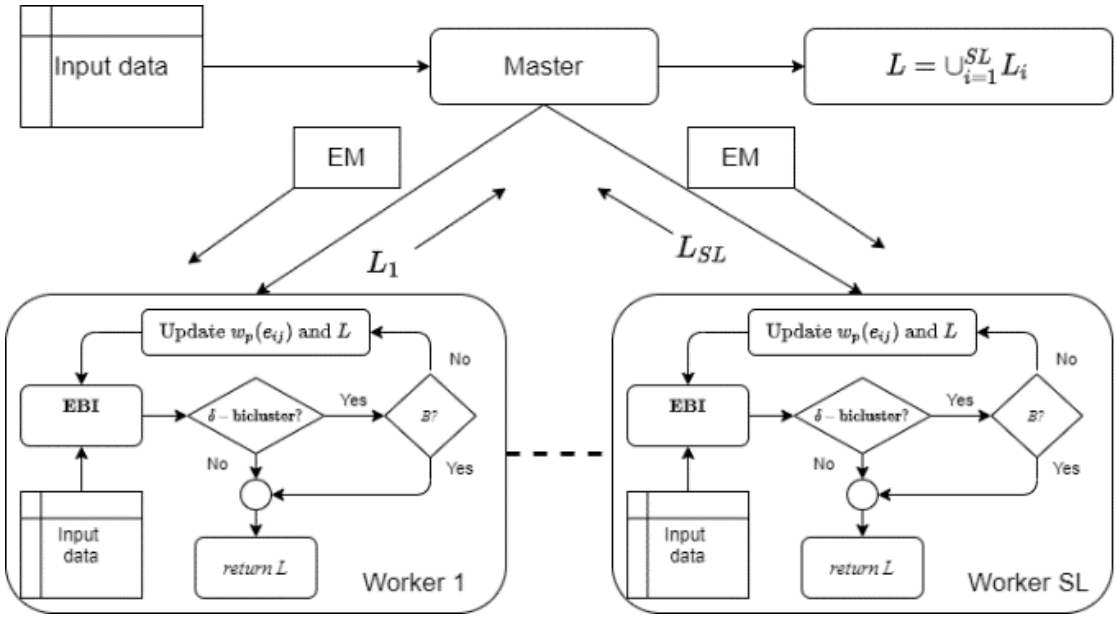


Figure 4: Workflow of the master-slave architecture of the PSC approach.

5. RESULTS AND DISCUSSION

In this section, we assess the quality of the PSC method for finding biclusters on the electric energy consumption data. This dataset contains 744 samples of electric energy consumption for 184 sensors gathered in December of 2013.

When the search space size is large, the choice of a correct set of parameter values is critical and might need many trials. Though what is essential is the description of a precise fitness function, as the parameter values will only help reach the goal defined by that function, i.e., the evolutionary algorithm might need much more time to converge. The results might not be good. Additionally, if we have limited time but enough computer resources, it is possible to perform parallel tests. We have run various preliminary resultsfor set the parameters of the algorithms. Table 1 shows the parameters setting. It is important to note that every time that PS calls EBI, it runs $PS \times g_{max}$ evaluations of potential biclusters, and the size of the search space is about 2^{n+m}, with n samples and m sensors. Thus, the number of candidate biclusters evaluated by EBI could be too small compared to the number of potential biclusters when n and m are large. Therefore, the role of genetic operators and the fitness function is a key factor in correctly guiding the search toward reasonable solutions.

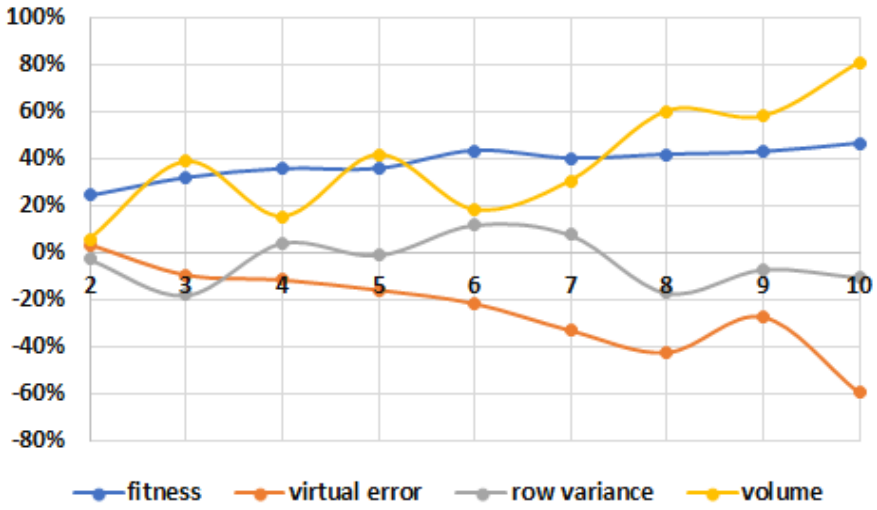
Table 1. Parameter settings of PSC.

Parameter	*Symbol*	*Value*
Population Size	*PS*	200
Number of generations	g_{max}	30
Crossover probability	p_c	0.85
Mutation probability	p_m	0.20
Elitism Probability	p_e	0.9
Weight for volume	w_V	1
Weight for sensors	w_r	1
Weight for samples day	w_c	10
Tournament Size	*ts*	4
Biclusters to find	*B*	10
Delta Biclusters	δ	10
Number of workers	*SL*	2 to 10
Number of independent runs	*NR*	30

The executions have performed a computer with Intel(R) Core (TM) i5-2520M CPU @ 2.50GHz, 4Gb RAM as the master node, and a computer with AMD A8-7410 APU processor with 8Gb RAM as worker nodes, both with Linux operating systems. The simulation was performed on a local area network. The automatization of PSC was via Apache Hadoop and Apache Spark version spark-2.3.0-bin-hadoop2.7. One core per computer worker was configured to perform the SC algorithm. All algorithms were implemented in Java language using the javac 1.8.0_201 version. Each parallel run consumed an average of 30 minutes, totaling a computation time of 150 hours (NR x 30 min x *SL*), including the SC run.

Algorithms	***Workers***	***Fitness***	***VE***	***var***	***V***
SC	1	1.86E-03	1.40E-01	1.15E+03	4.45E+02
PSC	2	1.40E-03	1.35E-01	1.12E+03	4.71E+02
	3	1.26E-03	1.53E-01	9.43E+02	6.18E+02
	4	1.19E-03	1.56E-01	1.20E+03	5.14E+02
	5	1.19E-03	1.62E-01	1.14E+03	6.31E+02
	6	1.05E-03	1.70E-01	1.29E+03	5.27E+02
	7	1.11E-03	1.86E-01	1.24E+03	5.82E+02
	8	1.08E-03	1.99E-01	9.54E+02	7.14E+02
	9	1.06E-03	1.78E-01	1.07E+03	7.04E+02
	10	9.94E-04	2.23E-01	1.03E+03	8.06E+02

(a) Table of PSC and SC experimental results



(b) Relative performance of PSC over SC

Figure 5. Experimental result of PSC and SC

Table 2 shows the average values of the different metrics. The fitness score is highly correlated with virtual error (-0.71) and volume (-0.69), while to a lesser degree with a row variation (0.06). In general, when the bicluster fitness decreases, the volume and row variance tend to increase. On the other hand, the row variance does not show a definite pattern about fitness. With these results, we can note that the algorithm finds biclusters with high-quality in volume at the cost of slightly increasing some virtual error.Figure 5 presents a graphical representation of these explanations. This figure shows the relative and normalized values of the fitness, virtual error, row variance, and volume metrics. The relative fitness with k workers is calculated as $f_k = {(f_1 - f_k)}/{f_1}$, likewise the other metrics.

The virtual error measure has a low correlation with row variation (-0.25) and a high correlation with volume (0.86). The above implies that virtual error and volume are in a trade-off relationship. With the worsening of the virtual error, the volume improves and vice versa. This result depends on the input parameters that define the algorithm's course towards some sub-region of the efficient frontier. The row variation and volume have a medium correlation of -0.59. The row variation influences the volume moderately.

Another critical aspect observed is the impact of parallelization. As the number of worker nodes increases, then the fitness score also improves. This improvement is a consequence of further exploration of the search space with the same computational time.

Figure 6 presents two examples of bicluster calculated using the PSC algorithm. In these biclusters, we can see patterns of electric energy consumption. The sensors 58, 73, and 112 and samples block 656 to 685 constitute Bicluster A, while sensors 13, 47, and 52 and samples block 557 to 585 for Bicluster B. In the figure also we can see the virtual error, row variance, and volume of biclusters. The patterns show abrupt changes of sensor groups at different times of the month. Such descriptions of electricity consumption are crucial to energy policy or decision-

making. In this context, the developed tool is promising as a pattern description system for the electricity sector.

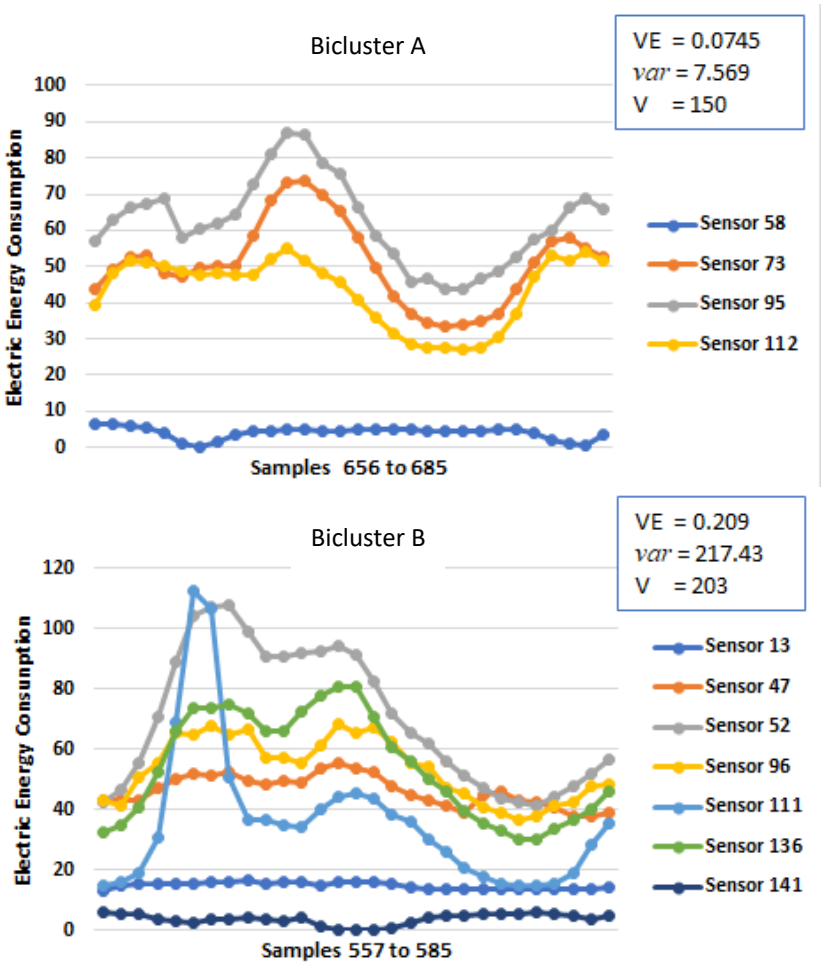


Figure 6: Examples of two biclusters calculated by PSC algorithm.

6. Conclusions and Future Work

In this paper, we have proposed, implemented, and validated a parallel alternative to an evolutionary biclustering algorithm. The proposed parallel architecture is based on the master-worker scheme to discover biclusters called Parallel Sequential Covering (PSC). The PSC was tested to locate and describe hidden patterns in a set of time series of an electrical system. Experimental results indicate that the PSC approach is promising for the study scenario, outperforming the state-of-the-art non-parallel evolutionary algorithm. A key aspect is that the quality of the solutions improves with the increasing number of workers. The algorithm converges to bicluster regions with high volume and vector variation as well as low virtual errors. These characteristics are the ones desired in the problem in question. Experiments also indicate that volume and virtual error are objective functions that conflict with each other. Therefore, we consider approaching a Parallel Pareto multi-objective optimization scheme as the next step in this research line.

Acknowledgments

This work was supported by the CONACYT, Paraguay, under Grant PINV18-661.

REFERENCES

[1] Li, X.; Bowers, C.P.; Schnier, T. Classification of energy consumption in buildings with outlier detection. IEEE Transactions on Industrial Electronics 2009, 57, 3639–3644.

[2] Wei, Y.; Zhang, X.; Shi, Y.; Xia, L.; Pan, S.; Wu, J.; Han, M.; Zhao, X. A review of data-driven approaches for prediction and classification of building energy consumption. Renewable and Sustainable Energy Reviews 2018, 82, 1027–1047.

[3] Hernandez, L.; Baladron, C.; Aguiar, J.M.; Carro, B.; Sanchez-Esguevillas, A.J.; Lloret, J.; Massana, J. A survey on electric power demand forecasting: future trends in smart grids, microgrids and smart buildings. IEEE Communications Surveys & Tutorials 2014, 16, 1460–1495.

[4] Moon, J.; Jung, S.; Rew, J.; Rho, S.; Hwang, E. Combination of short-term load forecasting models based on a stacking ensemble approach. Energy and Buildings 2020, 216, 109921.

[5] Somu, N.; MR, G.R.; Ramamritham, K. A deep learning framework for building energy consumption forecast. Renewable and Sustainable Energy Reviews 2021, 137, 110591.

[6] Jain, R.K.; Smith, K.M.; Culligan, P.J.; Taylor, J.E. Forecasting energy consumption of multi-family residential buildings using support vector regression: Investigating the impact of temporal and spatial monitoring granularity on performance accuracy. Applied Energy 2014, 123, 168–178.

[7] Divina, F.; Gilson, A.; Goméz-Vela, F.; García Torres, M.; Torres, J.F. Stacking ensemble learning for short-term electricity consumption forecasting. Energies 2018, 11, 949.

[8] Divina, F.; Garcia Torres, M.; Goméz Vela, F.A.; Vazquez Noguera, J.L. A comparative study of time series forecasting methods for short term electric energy consumption prediction in smart buildings. Energies 2019, 12, 1934.

[9] Capozzoli, A.; Lauro, F.; Khan, I. Fault detection analysis using data mining techniques for a cluster of smart office buildings. Expert Systems with Applications 2015, 42, 4324–4338.

[10] Fan, C.; Xiao, F.; Wang, S. Development of prediction models for next-day building energy consumption and peak power demand using data mining techniques. Applied Energy 2014, 127, 1–10.

[11] Zhan, S.; Liu, Z.; Chong, A.; Yan, D. Building categorization revisited: A clustering-based approach to using smart meter data for building energy benchmarking. Applied Energy 2020, 269, 114920.

[12] Rajabi, A.; Eskandari, M.; Ghadi, M.J.; Li, L.; Zhang, J.; Siano, P. A comparative study of clustering techniques for electrical load pattern segmentation. Renewable and Sustainable Energy Reviews 2020, 120, 109628.

[13] Anitha, S.; Chandran, C. Review on Analysis of Gene Expression Data Using Biclustering Approaches. Bonfring Int. J. Data Min. 2016, 6, 16.

[14] Nepomuceno, J.A.; Troncoso, A.; Aguilar-Ruiz, J.S. Scatter search-based identification of local patterns with positive and negative correlations in gene expression data. Appl. Soft Comput. 2015, 35, 637–651.

[15] Divina, F.; Pontes, B.; Giráldez, R.; Aguilar-Ruiz, J.S. An effective measure for assessing the quality of biclusters. Comput. Biol. Med. 2012, 42, 245–256

[16] Gnatyshak, D.V.; Ignatov, D.I.; Semenov, A.; Poelmans, J. Analysing online social network data with biclustering and triclustering. Concept Discovery in Unstructured Data. In Proceedings of the 2nd International Workshop, CDUD 2012, Leuven, Belgium, 6–10 May 2012; pp. 30–39

[17] Li, F.; Li, M.; Guan, P.; Ma, S.; Cui, L. Mapping publication trends and identifying hot spots of research on internet health information seeking behavior: A quantitative and co-word biclustering analysis. J. Med. Internet Res. 2015, 17.

[18] Sun, Z.; Han, L.; Huang, W.; Wang, X.; Zeng, X.; Wang, M.; Yan, H. Recommender systems based on social networks. J. Syst. Softw. 2015, 99, 109–119.

[19] Divina, F., Goméz Vela, F.A. and García Torres, M., 2019. Biclustering of smart building electric energy consumption data. Applied Sciences, 9(2), p.222.

[20] Liao, T.W. Clustering of time series data—a survey. Pattern recognition 2005, 38, 1857–1874.

[21] Rani, S.; Sikka, G. Recent techniques of clustering of time series data: a survey. International Journal of Computer Applications 2012, 52.

[22] Divina, F.; Goméz Vela, F.A.; García Torres, M. Biclustering of Smart Building Electric Energy Consumption Data. Applied Sciences 2019, 9. doi:10.3390/app9020222.

[23] Ruiz, L.; Pegalajar, M.; Arcucci, R.; Molina-Solana, M. A time-series clustering methodology for knowledge extraction in energy consumption data. Expert Systems with Applications 2020, 160, 113731.
[24] Lee, E.; Kim, J.; Jang, D. Load profile segmentation for effective residential demand response program: Method and evidence from Korean pilot study. Energies 2020, 13, 1348.
[25] Busygin, S.; Prokopyev, O.; Pardalos, P.M. Biclustering in data mining. Computers & Operations Research 2008, 35, 2964–2987.
[26] Gendreau, M., & Potvin, J. Y. (Eds.). (2010). Handbook of metaheuristics (Vol. 2, p. 9). New York: Springer.
[27] Campillo, J., Wallin, F., Torstensson, D., and Vassileva,I. (2012). Energy demand model design for forecasting electricity consumption and simulating demand responsescenarios insweden. In4th International Conference in Applied Energy 2012, July 5-8, 2012. Suzhou, China.
[28] Medina, A., Cámara, A., and Monrobel, J.-R. (2016). Measuring the socioeconomic and environmental effects of energy efficiency in-vestments for a more sustainable spanish economy. Sustainability, 8(10):1039.
[29] Abdel-Aal, R. E. and aZ, A.-G. (1997). Forecasting monthly electric energy consumption in eastern saudiarabia using univariatetime-series analysis. Energy, 22:1059–1069
[30] Newsham, G. R., &Birt, B. J. (2010, November). Building-level occupancy data to improve ARIMA-based electricity use forecasts. In Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building (pp. 13-18).
[31] Jain, R. K., Smith, K. M., Culligan, P. J., & Taylor, J. E. (2014). Forecasting energy consumption of multi-family residential buildings using support vector regression: Investigating the impact of temporal and spatial monitoring granularity on performance accuracy. Applied Energy, 123, 168-178.
[32] Liu, Y., Chen, H., Zhang, L., Wu, X., & Wang, X. J. (2020). Energy consumption prediction and diagnosis of public buildings based on support vector machine learning: A case study in China. Journal of Cleaner Production, 272, 122542.
[33] Yang, S., Wan, M. P., Chen, W., Ng, B. F., & Dubey, S. (2020). Model predictive control with adaptive machine-learning-based model for building energy efficiency and comfort optimization. Applied Energy, 271, 115147.
[34] Zheng, H., Yuan, J., & Chen, L. (2017). Short-term load forecasting using EMD-LSTM neural networks with a Xgboost algorithm for feature importance evaluation. Energies, 10(8), 1168.
[35] Chitsaz, H., Shaker, H., Zareipour, H., Wood, D., &Amjady, N. (2015). Short-term electricity load forecasting of buildings in microgrids. Energy and Buildings, 99, 50-60.
[36] Kelo, S., &Dudul, S. (2012). A wavelet Elman neural network for short-term electrical load prediction under the influence of temperature. International Journal of Electrical Power & Energy Systems, 43(1), 1063-1071.
[37] Nizami, S. J., & Al-Garni, A. Z. (1995). Forecasting electric energy consumption using neural networks. Energy policy, 23(12), 1097-1104.
[38] Diao, L., Sun, Y., Chen, Z., & Chen, J. (2017). Modeling energy consumption in residential buildings: A bottom-up analysis based on occupant behavior pattern clustering and stochastic simulation. Energy and Buildings, 147, 47-66.
[39] Pérez-Chacón, R., Luna-Romera, J. M., Troncoso, A., Martínez-Álvarez, F., & Riquelme, J. C. (2018). Big data analytics for discovering electricity consumption patterns in smart cities. Energies, 11(3), 683.
[40] Pontes, B.; Giráldez, R.; Aguilar-Ruiz, J.S. Quality Measures for Gene Expression Biclusters. PLoS ONE 2015, p. e0115497.
[41] Eiben, A.E.; Smith, J.E. Introduction to Evolutionary Computing; Springer-Verlag, 2003.
[42] Bäck, T.; Fogel, D.B.; Michalewicz, Z. Evolutionary Computation 1: Basic Algorithms and Operators; Institute of Physics Publishing, 2000.
[43] Yao, X., Evolutionary computation: A gentle introduction. In Evolutionary Optimization; Kluwer Academic Publishers, 2002; chapter 2, pp. 27–53.
[44] Goldberg, D.E.; Robert, L. Alleles, loci and the travelling salesman problem. Proceedings of 1st Int. Conf. on Genetic Algorithms; Grefenstette, J.e., Ed. Lawrence Erlbaum Associates, Hillsdale, 1985, pp. 154–159.
[45] Rocha, M.; Cortez, P.; Neves, J. Evolution of neural networks for classification and regression. Neurocomputing 2007, 70, 2809–2816. Neural Network Applications in Electrical Engineering Selected papers from the 3rd International Work-Conference on Artificial Neural Networks (IWANN

2005), https://doi.org/10.1016/j.neucom.2006.05.023.
[46] Bentley, P.J.; Corne, D.W. Creative evolutionary systems; Morgan Kaufmann Publishers Inc., 2001.
[47] Zheng, F.; Zecchin, A.C.; Newman, J.P.; Maier, H.R.; Dandy, G.C. An Adaptive Convergence-Trajectory Controlled Ant Colony Optimization Algorithm with Application to Water Distribution System Design Problems. IEEE Transactions on Evolutionary Computation 2017, 21, 773–791. doi:10.1109/TEVC.2017.2682899.
[48] Cheng, S.; Ma, L.; Lu, H.; Lei, X.; Shi, Y. Evolutionary computation for solving search-based data analytics problems. Artif. Intell. Rev. 2021, 54, 1321–1348. doi:10.1007/s10462-020-09882-x.
[49] Nakisa, B.; Rastgoo, M.N.; Tjondronegoro, D.; Chandran, V. Evolutionary computation algorithms for feature selection of EEG-based emotion recognition using mobile sensors. Expert Systems with Applications 2018, 93, 143–155. https://doi.org/10.1016/j.eswa.2017.09.062.
[50] Yamada, T.; Nakano, R. A Genetic Algorithm Applicable to Large-Scale Job-Shop Problems. Parallel Problem Solving from Nature, 2; R. Männer.; Manderick, B., Eds.; Elsevier Science Publishers, B. V.: Amsterdam, 1992.
[51] Corne, D.; Ross, P.; Fang, H.L. Fast Practical Evolutionary Timetabling. Lecture Notes in Computer Science, vol 865 (Evolutionary Computing AISB Workshop, Leeds, UK, April 1994). Springer-Verlag, 1994, pp. 251–263.
[52] Gehlhaar, D.K.; Verkhivker, G.M.; Rejto, P.A.; Sherman, C.J.; Fogel, D.B.; Fogel, L.J.; Freer, S.T. Molecular recognition of the inhibitor AG-1343 by HIV-1 protease: conformationally flexible docking by evolutionary programming. Chemistry and Biology 1995, 2, 317–324.
[53] Spencer, G.F. Automatic Generation of Programs for Crawling and Walking. Proceedings of the 5th International Conference on Genetic Algorithms, ICGA-93; Forrest, S., Ed.; Morgan Kaufmann: University of Illinois at Urbana-Champaign, 1993; p. 654.
[54] Fogel, D.B. Evolving Behavious in the Iterated Prisoner's Dilemma. Evolutionary Computation 1993, 1, 77–97.
[55] Divina, F.; Marchiori, E. Evolutionary Concept Learning. GECCO 2002: Proceedings of the Genetic and Evolutionary Computation Conference; Morgan Kaufmann Publishers: New York, 2002; pp. 343–350.reless networks. In Proceedings of the IEEE 1st International Conference on Broadnets Networks (BroadNets'04). IEEE, Los Alamitos, CA, 210–217. https://doi.org/10.1109/BROADNETS.2004.8
[56] Divina, F., and Aguilar-Ruiz, J.S., 2007, July. A multi-objective approach to discover biclusters in microarray data. In Proceedings of the 9th annual conference on Genetic and evolutionary computation (pp. 385-392).
[57] Erick Cantú-Paz, David E. Goldberg, Efficient parallel genetic algorithms: theory and practice, Computer Methods in Applied Mechanics and Engineering, Volume 186, Issues 2–4, 2000, Pages 221-238, ISSN 0045-7825, https://doi.org/10.1016/S0045-7825(99)00385-0.
[58] Coello, C. A. C., Lamont, G. B., & Van Veldhuizen, D. A. (2007). Evolutionary algorithms for solving multi-objective problems (Vol. 5, pp. 79-104). New York: Springer.

STACK AND DEAL: AN EFFICIENT ALGORITHM FOR PRIVACY PRESERVING DATA PUBLISHING

Vikas Thammanna Gowda

Department of Electrical Engineering and Computer Science,
Wichita State University, Kansas, USA

ABSTRACT

Although k-Anonymity is a good way to publish microdata for research purposes, it still suffers from various attacks. Hence, many refinements of k-Anonymity have been proposed such as l-diversity and t-Closeness, with t-Closeness being one of the strictest privacy models. Satisfying t-Closeness for a lower value of t may yield equivalence classes with high number of records which results in a greater information loss. For a higher value of t, equivalence classes are still prone to homogeneity, skewness, and similarity attacks. This is because equivalence classes can be formed with fewer distinct sensitive attribute values and still satisfy the constraint t. In this paper, we introduce a new algorithm that overcomes the limitations of k-Anonymity and l-Diversity and yields equivalence classes of size k with greater diversity and frequency of a SA value in all the equivalence classes differ by at-most one.

KEYWORDS

k-Anonymity, l-Diversity, t-Closeness, Privacy Preserving Data Publishing.

1. INTRODUCTION

Various organizations such as government agencies and hospitals release microdata for medical research, trend analysis, and other purposes. Typically, microdata is stored in a table and each row corresponds to an individual's record and each record consists of a diverse number of attributes. These attributes can be categorized into a)*Explicit Identifier* attributes: are attribute sets such as name and social security number, that explicitly identify individuals. b) *Quasi Identifier* (QI) attributes: are attribute sets such as zip code, age, and sex that cannot uniquely identify individuals, but combinations of these attributes can give away the record holder. Sweeney [1] has shown that even though neither sex, date of birth, nor zip codes uniquely identifies an individual, the combination of all three is sufficient to identify 87% of individuals in the United States. c) *Sensitive attributes* (SAs): consists of sensitive information of individuals. d) *Non-Sensitive attributes*: consists of attributes that are non-sensitive in nature which does notreveal any sort of information about the record holder.

Privacy preserving data publishing (PPDP) means releasing microdata in such a way that there is data utility of released data and at the same time privacy of an individual in the released data is maintained. Prior to data release, first, the explicit identifier attributes are removed since it uniquely identifies an individual. Then the records are horizontally partitioned into groups of records called equivalence classes and the quasi identifier attributes are generalized to ensure that quasi identifier values of all records within an equivalence class becomes identical while the sensitive attributes are unaltered.

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 139-148, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111111

Based on this approach, various privacy models have been proposed. For example, *k*-anonymity (Sweeney [1]) requires that each equivalence class must have at least *k* records that are indistinguishable from *k-1* records in terms of their quasi identifier attribute values. *l*-diversity (Machanavajjhala et al. [2]) requires that each equivalence class consists of at least a certain number of i.e., *l* "*well-represented*" values of sensitive attributes. To address the limitations of *k*-anonymity and *l*-diversity Li et al. [3] introduced the concept of *t*-closeness [9], which requires that distance between the distribution of the sensitive attribute in the entire table and the distribution of the sensitive attribute in any equivalence class to be close.

l-diversity and *t*-closeness privacy models are the extensions of *k*-anonymity model to address its limitations. This paper shows that the limitations can be addressed with an algorithm since the extensions possess its own limitations. The algorithm outputs equivalence classes with a high degree of diversity among the sensitive attributes whose distribution is very close to the distribution of sensitive attributes in the overall table with just one input parameter *k*. The algorithm can be implemented with the help of simple data structures like queue or stack.

1.1. Contributions and Organization

In this paper, we have introduced an algorithm which gives equivalence classes whose sensitive attribute distribution is close to sensitive attribute distribution in the overall table and overcomes the limitations of *k*-Anonymity and *l*-Diversity. The rest of the paper is organized as follows. In Section 2, we review some background concepts used throughout the paper. Section 3 deals with our proposed method that works in various stages and provides the algorithm for obtaining equivalence classes of size *k* with greater diversity and frequency of a SA value in all the ECs differ by at-most one. In Section 4, we analyse the algorithm and show how it defends against homogeneity, skewness and similarity attacks with experimental results and Section 5 presents conclusion and future work.

2. BACKGROUND

Consider a raw data that needs to be published as shown in Table 1. Explicit identifiers such as name and SSN are removed since they directly identify the record holder. Quasi identifiers like zip code and age cannot uniquely identify individuals but, combinations of these attributes can give away the record holder. Sweeney [1] has shown that even though neither sex, date of birth nor zip codes uniquely identify an individual, the combination of all three is sufficient to identify 87% of individuals in the United States. Attribute like disease that is closely guarded by the record holder is considered to be sensitive attribute.

Table 1. Raw Table.

No	Name	SSN	Zip Code	Age	Disease
1	Scofield	111-11-1111	47677	29	Flu
2	Linc	222-22-2222	47602	25	Flu
3	Sara	333-33-3333	47678	27	Flu
4	Henry	444-44-4444	47905	43	Cancer
5	Bagwell	555-55-5555	47909	40	Ulcer
6	Bellick	666-66-6666	47706	47	Cold
7	John	777-77-7777	47705	30	Cancer
8	Cooper	888-88-8888	47773	35	Pneumonia
9	Sucre	999-99-9999	47707	32	Bronchitis

The goal of PPDP is to protect the sensitive attribute of the record holder while still publishing enough information to maintain data utility. *k*-anonymity by Sweeney [1] is a well-known model for anonymizing the data. Here the explicit identifiers of each record are removed and quasi identifiers along with sensitive attribute are grouped. Each group is called an equivalence class where quasi identifiers are generalized and sensitive attribute is unaltered.

Definition 1: (*Equivalence Class*) An Equivalence Class is a set of anonymized records that have same values for all quasi identifier attributes, i.e., all records in each equivalence class are indistinguishable in terms of their quasi identifier attributes.

Definition 2: (*k-Anonymity*) An equivalence class is said to satisfy *k*-anonymity if every record is indistinguishable from at least *k-1* other records with respect to every set of the quasi identifier attributes. A table is said to satisfy *k*-anonymity if every equivalence class of the table satisfies *k*-anonymity.

In other words, it is like hiding something in the crowd so it would be difficult to identify, as almost everything looks alike when the entire crowd is seen.

Table 2 gives a 3-anonymous version of the raw table. The data is divided into three equivalence classes consisting of three records each, whose quasi identifiers (zip code and age) are generalized and sensitive attribute (disease) is unaltered.

Table 2. 3-Anonymous Version of Table 1.

No	Zip Code	Age	Disease
1	476**	2*	Flu
2	476**	2*	Flu
3	476**	2*	Flu
4	479**	4*	Cancer
5	479**	4*	Ulcer
6	479**	4*	Cold
7	477**	3*	Cancer
8	477**	3*	Pneumonia
9	477**	3*	Bronchitis

Attack on *k*-Anonymity: Suppose that Alex and Bob are neighbours and Alex discovers a published data as shown in Table 2. Alex knows that Bob is a 29-year old male living in zip code 47677, then Alex can easily place Bob in first equivalence class. Since all the record holders in first equivalence class of Table 2 have the same disease i.e., flu, Alex concludes that Bob has flu. This is known as homogeneity attack.

Limitations of *k*-Anonymity:

1. Does not provide protection against homogeneity attack.
2. Does not include randomization and attacker can still make inferences about data sets that may harm individuals.
3. Not good for high dimensional data.
4. Concerned only about quasi identifiers and not sensitive attribute.

Machanavajjhala et al. [2] introduced *l*-diversity as a stronger notion of privacy to overcome the limitations of k-anonymity.

Definition 3: (*l-Diversity*) An equivalence class is said to satisfy *l*-diversity if there are at-least *l* "well represented" values for the sensitive attribute. A table is said to satisfy *l*-diversity if every equivalence class of the table satisfies *l*-diversity.

Table 4 satisfies 3-diversity since there are three well represented sensitive attribute values in each equivalence class. The table also satisfies 3-anonymity.

Attack on *l*-Diversity: Suppose that Alex and Bob are neighbours and Alex discovers a published data as shown in Table 4. Alex knows that Bob is a 37-year old male living in zip code 67220, then Alex can easily place Bob in first equivalence class. Looking at the SA values, Alex concludes that Bob is suffering from some sort of stomach related disease. This is known as similarity attack. *l*-diversity fails to protect against attacks arising from an adversary's unavoidable knowledge of the overall distribution of SA values in a released table. A skewness attack may occur when the distribution of sensitive attributes in an equivalence varies significantly from that in the released table.

Table 3. Disease Table.

No	Zip Code	Age	Disease
1	67200	37	Gastric ulcer
2	67406	52	Gastritis
3	67207	35	Gastritis
4	67433	57	Flu
5	67319	41	Bronchitis
6	67302	43	Pneumonia
7	67308	46	Stomach cancer
8	67420	58	Bronchitis
9	67208	36	Stomach cancer

Table 4. 3-Diverse Version of Table 3.

No	Zip Code	Age	Disease
1	672**	3*	Gastric ulcer
2	672**	3*	Gastritis
3	672**	3*	Stomach cancer
4	674**	5*	Gastritis
5	674**	5*	Flu
6	674**	5*	Bronchitis
7	673**	4*	Bronchitis
8	673**	4*	Pneumonia
9	673**	4*	Stomach cancer

Limitations of *l*-Diversity:

1. Does not provide protection against similarity and skewness attacks.
2. *l*-diversity may be difficult and unnecessary to achieve.
3. It is concerned only about well represented sensitive attributes but not about the distribution of the sensitive attributes.

4. ALGORITHM FRAMEWORK

In this section, we present a framework for Stack and Deal algorithm. Given a microdata table*M* consisting of *r* records and *n* attributes ((*n-1*) quasi identifier attributes and one sensitive attribute) and *k*, let *A* denote the set of all attributes $\{A_1, A_2, ..., A_n\}$. Without loss of generality, let the attribute A_n be the sensitive attribute and $\{A_1, A_2, ..., A_{n-1}\}$ be quasi identifier attributes.

Stage 1: Frequency and Distribution of SA in the entire table M

A frequency table as shown in Table 5 is created that contains *s* sensitive attribute values ($S_1, S_2, S_3, ..., S_s$) and its frequency $F = (f_1, f_2, f_3, ..., f_s)$ in the entire table.

Table 5. Frequency Distribution Table of Sensitive attribute in M.

No	Sensitive Attribute	Frequency	Distribution
1	S_1	f_1	p_1
2	S_2	f_2	p_2
3	S_3	f_3	p_3
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
s	S_s	f_s	p_s

These entries are arranged in descending order, where $(f_1 \geq f_2 \geq f_3 \geq ..... \geq f_s)$ and $\sum_{j=1}^{s} f_j = r$. Distribution of the sensitive attribute in the entire table is $P = (p_1, p_2, p_3, ..., p_s)$, where $(p_1 \geq p_2 \geq p_3 \geq ..... \geq p_s)$, $p_j = f_j / r$ and $\sum_{j=1}^{s} p_j = 1$.

Stage 2: Stack and Deal the records

In this stage, a queue of records are stacked according to the frequency distribution table as shown in Table 6 i.e., all records having sensitive attribute value S_1 appears at the top of the queue and records having sensitive attribute value S_s appears at the bottom of the queue.

Table 6. Stacked Data.

No	Quasi Identifier	Sensitive Attribute
1	$\{A_1, A_2, A_{3,....,} A_{n-1}\}$	S_1
2		S_1
.		S_1
.		.
.		.
33		S_2
.		.
.		.
.		.
87		S_{s-1}
.		.
.		.
.		.
r	$\{A_1, A_2, A_{3,....,} A_{n-1}\}$	S_s

Now for dealing part, each record is popped out of the stack into *e* equivalence classes (*e = r/k)* in a cyclic order. For example, if there are ten equivalence classes then, the first record goes into first equivalence class, second record to second equivalence class and so on. When we hit the last equivalence class i.e., tenth equivalence the next record goes into the first equivalence class and the cycle continues till the stack is empty.

Observation: We see that, by following the cyclic order while populating equivalence classes we get equi-sized equivalence classes where every equivalence will get equal portions of f_j/e and frequency of a SA value in all the equivalence classes differs by at-most one.

Stage 3: Frequency and Distribution of SA in equivalence classes *E*

Once the last record is popped out, we now have *e* equivalence classes, $E = (E_1, E_2, E_3, \ldots, E_e)$ having *k* records. Similar to stage 1, frequency and distribution of SA in each equivalence class is formed, that contains sensitive attribute values $(S_1, S_2, S_3, \ldots, S_s)$ and its frequency $F = (g_1, g_2, g_3, \ldots, g_s)$. These entries are arranged in descending order, where $(g_1 \geq g_2 \geq g_3 \geq \ldots\ldots \geq g_s)$ and $\sum_{j=1}^{s} g_j = k$. Distribution of the sensitive attribute in an equivalence class is $Q = (q_1, q_2, q_3, \ldots, q_s)$, where $(q_1 \geq q_2 \geq q_3 \geq \ldots\ldots \geq q_s)$, $q_j = g_j / r$ and $\sum_{j=1}^{s} q_j = 1$. Distribution table of one equivalence class is shown below in Table 7. Earth movers distance [8] between *P* and *Q* gives the closeness between SA distribution in the overall table and the SA distribution in each equivalence class.

Table 7. Frequency Distribution Table of Sensitive attribute in an Equivalence Class.

No	Sensitive Attribute	Frequency	Distribution
1	S_1	g_1	q_1
2	S_2	g_2	q_2
3	S_3	g_3	q_3
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
s	S_s	g_s	q_s

Algorithm:

Input: micro table *M* having *r* records, *k*

Output: *e* equivalence class of size *k*

1. Let $e = r/k$.
2. Set $E_1, E_2, E_3, \ldots, E_e = \phi$
3. Sort all records in descending order of f_j (frequency of SA $(1 \geq j \geq s)$)
4. For $z = 1$ to r

$E[(z \bmod e) + 1] = M[z]$

5. ANALYSIS OF ALGORITHM FOR VARIOUS ATTACKS

In this section, we show how the Stack and Deal algorithm protects against various attacks:

Protection against Homogeneity attack:

Homogeneity attack occurs when the SA values in an EC are the same, thus an attacker learns about the sensitive information of a record holder without any additional efforts. The way to combat this is to ensure that the SA values in every EC are diverse. Our algorithm ensures that all the ECs produced are diverse in terms of their SA values.

Let F = (167, 153, 127, 103, 91, 89) and r =730. When we vary the value of k we observe that we attain maximum diversity for k = 9. We know that if an EC satisfy 9-anonymity it also satisfies 2, 3, ..., 8-anonymity as well. Since there is a trade-off between privacy and data utility, we can compromise data utility to achieve maximum diversity. Figure 1 shows the variation of k with respect to l.

We run the same experiment on Adult data set Figure 2 from UC Irvine machine learning repository and vary k from 2 to 21. We observe relatively similar behaviour on this data set too.

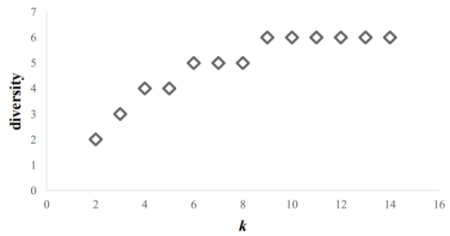


Figure 1. k vs diversity

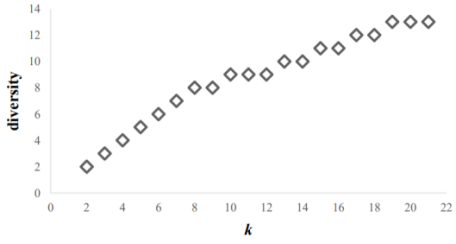


Figure 2. k vs diversity for Adult Data Set.

Protection against Skewness and Similarity attacks:

Privacy is measured by the amount of information gain of an observer/attacker. The observer has some prior belief (G_0) about the sensitive information of a record holder and some posterior belief (G_2) after seeing the released table. Information gain is the difference in these two believes. Assume that the observer is given a completely generalized form of the data P and his prior belief (G_0) changes to (G_1) by looking at the distribution of SA values in the overall table P (P is considered as public information because as long as a version of data is released, P will be known). Now, the observer is given the released data and by knowing the quasi-identifier of a record holder, the observer is able to identify an EC to which the record holder belongs to and learns the distribution of SA values represented as Q in that EC. Now this is the observer's posterior belief (G_2).

The l-diversity requirement is inspired by restricting the difference between prior belief and observer's posterior belief but, whenever the distribution of SA values within an EC varies significantly from their overall distribution in the released table. l-diversity fails to guarantee privacy allowing skewness and similarity attacks. In our method, we choose to limit the difference between (G_1) and (G_2). We can do this by ensuring that the frequencies of SA values in all the ECs are similar and limiting their difference to be as low as possible. This is because, we want to obtain ECs which are of equi sized so as to limit the information loss and if the difference in frequencies increases, Q moves further away from P. Thus, by limiting the difference in the frequencies of SA values in the EC, we can limit the difference between P and Q and there by finally limiting the gain from (G_1) to (G_2). The distance between these two distributions is calculated using earth movers distance [8].

Earth Movers Distance: For any two distributions P and Q, where $P = (p_1, p_2, p_3, \ldots, p_s)$, $Q = (q_1, q_2, q_3, \ldots, q_s)$ and $\sum_{i=1}^{s} p_i = \sum_{i=1}^{s} q_i = 1$, the earth movers distance between P and Q, denoted as $EMD\ (P,Q)$.

$$EMD\ (P,Q) = \frac{1}{s-1}\sum_{i=1}^{s}\sum_{j=1}^{i}|(p_j - q_j)|$$

The earth mover's distance can be thought of as the sum total of the portions of the p_i values that needs to be moved to other indices in P each portion scaled by the normalized distance of its movement within the m-tuple, to turn P into Q.

As an example, consider probability distributions,

P = (0.2, 0.1, 0.7)
Q = (0.3, 0.0, 0.7)
R = (0.1, 0.0, 0.9)

$EMD\ (P, Q)$ = 0.1(1/2) = 0.05, because in order to turn P into Q, 0.1 amount needs to be moved from p_2 to p_1, which is 1 index away, out of a maximum of 2 (as k-1 = 2 is the farthest movement distance in this tuple). Similarly, $EMD\ (Q, R)$ = 0.2(2/2) = 0.2 and $EMD\ (P, R)$ = 0.1(2/2) + 0.1(1/2) = 0.15.

To study the result, we plot k against EMD between P and Q of ECs generated using our algorithm and randomly generated ECs. We observe that difference between $P$and Q reduces as we increase k and our algorithm gives the minimum difference. Figure 3 represents the plot for F = (167, 153, 127, 103, 91, 89) and r=730 and varying k. We observe that for k=2 we get some ECs whose difference between P and Q is lesser than our algorithm, this is because the size of ECs for such values vary by a huge difference increasing the information loss.

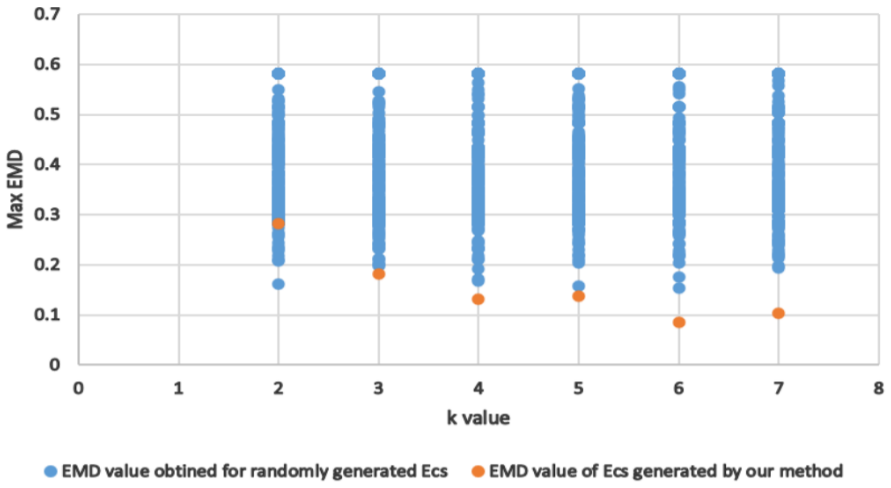


Figure 3. k vs EMD

Next, let us study the effect of increasing the difference between SA values in the ECs. For this purpose, we use Blood Transfusion data set and Haberman's Survival data set from UC Irvine machine learning repository and vary k from 2 to 20. *Rand1* and *Rand2* are the set of ECs whose difference in frequency of SA values are 2 and 3, respectively. From Figure 4 and Figure 5 we

observe that by limiting the difference in the frequencies of SA values in the EC we can limit the difference between P and Q and thereby finally limiting the gain from G_1 to G_2.

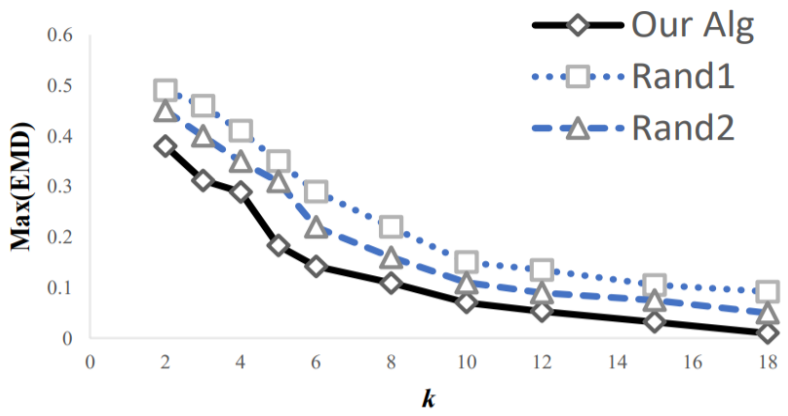


Figure 4. Variation of k in Blood Transfusion data set.

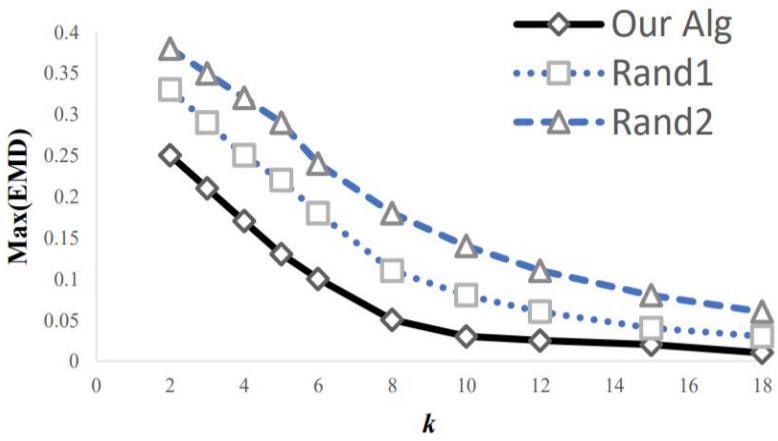


Figure 5. Variation of *k* in Haberman's Survival data set.

6. CONCLUSION AND FUTURE WORK

While *k*-Anonymity protects against identity disclosure, it does not provide sufficient protection against attribute disclosure. *l*-Diversity seeks to solve this problem by adding a condition that each equivalence class must have *l* distinct SA values. We have seen the limitations of *l*-Diversity and how we can combat them with the help of our algorithm without the requirement of *t* in *t*-Closeness. We have introduced a new algorithm that takes the input parameter *k* along with the microdata and produces equivalence classes of size *k* with a greater diversity and frequency of a SA value in all the ECs differ by at-most one thus helping in minimal data loss.

The first direction of future work is to design an algorithm that exchanges records to minimize information loss till we reach an optimal value for the information loss by making use of the parameter *t.* As a second direction, this algorithm can be generalized for Multiple Sensitive Attributes.

REFERENCES

[1] Latanya Sweeney.: k-anonymity: A model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl.-Based Syst., 10(5), pages 557-570, 2002.

[2] Machanavajjhala, Ashwin, Gehrke, Johannes, Kifer, Daniel, Venkitasubramaniam, Muthuramakrishnan: l-Diversity: Privacy Beyond k-Anonymity ACM Transactions on Knowledge Discovery From Data - TKDD. 1. 24. 10.1145/1217299.1217300.

[3] L. Ninghui, L. Tiancheng, and S. Venkatasubramanian, "t-Closeness: Privacy beyond k-anonymity and l-diversity", Proc.-Int. Conf. Data Eng., no. 3, pp. 106-115, 2007

[4] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, "Incognito: Efficient full-domain K- anonymity," in Proceedings of the ACM SIGMOD International Conference on 77 Management of Data, 2005, vol. 10, no. 5, pp. 49–60.

[5] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, "Mondrian Multidimensional K-Anonymity," in 22nd International Conference on Data Engineering (ICDE'06), 2006, vol. 2006, pp. 25–25

[6] J. Cao, P. Karras, P. Kalnis, and K.-L. Tan, "SABRE: a Sensitive Attribute Bucketization and REdistribution framework for t-closeness," VLDB J., vol. 20, no. 1, pp. 59–81, Feb. 2011.

[7] J. Soria-Comas, J. Domingo-Ferrer, D. Sanchez, and S. Martinez, "t-Closeness through Microaggregation: Strict Privacy with Enhanced Utility Preservation," IEEE Trans. Knowl. Data Eng., vol. 27, no. 11, pp. 3098–3110, Nov. 2015

[8] Y. Rubner, C. Tomasi, and L. Guibas, "The earth mover's distance as a metric for image retrieval," International Journal of Computer Vision, vol. 40, no. 2, pp. 99–121, 2000.

[9] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. Closeness: A new privacy measure for data publishing. IEEE Trans. Knowledge and Data Engineering, 22(7), 2010.

[10] Tiancheng Li , Jian Zhang , Ian Molloy , "Slicing: A New Approach for Privacy Preserving Data Publishing" IEEE Transaction on KDD (2012).

[11] B.Vani, D.Jayanthi, "Efficient Approach for Privacy Preserving Microdata Publishing Using Slicing" IJRCTT 2013.

[12] S.Gokila, Dr.P.Venkateswari, A SURVEY ON PRIVACY PRESERVING DATA PUBLISHING International Journal on Cybernetics & Informatics (IJCI) Vol. 3, No. 1, February 2014

[13] M. Patel, P. Richariya, and A. Shrivastava. A review paper on privacy preserving data mining. Compusoft, 2(9):296, 2013.

[14] C. C. Aggarwal and P. S. Yu. A general survey of privacy-preserving data mining models and algorithms. Privacy-preserving data mining, pages 11-52, 2008.

[15] Z. Huang. Extensions to the k-means algorithm for clustering large data sets with categorical values. Data mining and knowledge discovery, 2(3):283-304, 1998.

[16] J. Byun, A. Kamra, E. Bertino, and N. Li. Efficient k-anonymization using clustering techniques. pages 188-200, 2007.

[17] Q. Wei, Y. Lu, and Q. Lou. Privacy-preserving data publishing based on declustering. Pages 152-157, 2008.

[18] X. Xiao and Y. Tao. Anatomy: Simple and effective privacy preservation. pages 139-150, 2006.

[19] Q. Zhang, N. Koudas, D. Srivastava, and T. Yu. Aggregate query answering on anonymized tables. Pages 116-125, 2007.

[20] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu. Privacy-preserving data publishing: A survey of recent development. ACM Comput. Surv., 42(4):14:1-14:53, June 2010.

[21] C. Dwork. Differential Privacy. In Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP). 1–12, Venice, Itily, July 2006.

IMPACT OF E-MAINTENANCE OVER INDUSTRIAL PROCESSES

Yassine MOUMEN, Mariam BENHADOU and Abdellah HADDOUT

Laboratory of Industrial Management, Energy and Technology of Plastic and Composites Materials Hassan II University – ENSEM Casablanca, Morocco

ABSTRACT

During the course of the industrial 4.0 era, companies have been exponentially developed and have digitized almost the whole business system to stick to their performance targets and to keep or to even enlarge their market share. Maintenance function has obviously followed the trend as it's considered one of the most important processes in every enterprise as it impacts a group of the most critical performance indicators such as: cost, reliability, availability, safety and productivity. E-maintenance emerged in early 2000 and now is a common term in maintenance literature representing the digitalized side of maintenance whereby assets are monitored and controlled over the internet. According to literature, e-maintenance has a remarkable impact on maintenance KPIs and aims at ambitious objectives like zero-downtime.

KEYWORDS

E-maintenance, Maintenance, industry 4.0, industrial performance, zero-downtime.

1. INTRODUCTION

Maintenance has become one of the major influencers toward strategic objectives of companies in today's extremely competitive markets. Some results have shown that maintenance activities could range from 15% to 70% of the total production cost [1,2,3]. The cost is considered as the second largest after energy expenditures of the operational budget [1,4,6,7]. In the United States, the maintenance cost has tripled in 10 years to reach $600 billion in 1989 [1]. One more important figure related to product price structure that considers maintenance operating costs value up to 28% of the product's global cost [5].

The maintenance process is a set of required activities to keep an asset at maximum availability. These activities are mainly carried out according to certain maintenance strategies [1]. In the past, maintenance had been based mainly on corrective operations. Later, maintenance became an independent function, rather than a production sub-function [1]. A decade before, as the technologies grew and systems became more complex, maintenance has been developed as well and became enclosing technical and management knowledge. Indeed, preventive maintenance, including Time Based Maintenance (TBM) and Condition Based Maintenance (CBM), has followed the Corrective Maintenance (CM) as an upgrade, Design-Out Maintenance (DOM) and Total Productive Maintenance (TPM) have arrived gradually [1].

CM occurred in the early industrial days spontaneously when the maintenance belonged to the production process and was also known as firefighting or emergency maintenance. CM is mainly carried out after the failure [8].

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 149-156, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111112

Contrary, the preventive maintenance which intends to reduce the probability of failure or degradation of functioning of an equipment [1,9]. Preventive maintenance is divided into TBM and CBM. TBM operations are time-based and carried out following a pre-designed schedule, rolled out by the maintenance engineering team. Whereas in the CBM, the machine's parameters are monitored using sensors like vibration, temperature and pressure. In other words, preventive maintenance operations are carried out before failure. It's also considered a double edge weapon as it prevents failure and downtime, however, some good parts are replaced though.

Design-Out Maintenance is acting proactively, by focusing on equipment design in order to eliminate the cause of maintenance. DOM makes the maintenance easier in the life cycle of a product [22]. We can even say that DOM enhances one of the most important maintenance parameters, maintainability.

Maintenance strategy choice is a crucial phase to every organisation and it has a direct impact on business results and market share. Kumar Pinjala discovered a true correlation in his empirical investigation on the relationship between business and maintenance strategies; his survey's results of 150 companies in both Belgium and the Netherlands indicated that quality competitors have more proactive maintenance policies, better planning and control systems and decentralized maintenance organisation structures when compared to others [11].

The main objective of this work is illustrate a clear image about the maintenance, how it was seen? How it looks like nowadays? What would be the e-maintenance impact? And what are the tools and means required to reach desired performance.

To answer clearly all above questions mentioned, we decided to present our work as follow: First, we are going to describe the classic form of maintenance and to explain its pejorative image as it's seen as a necessary evil which is inherent, roughly, to all production systems and wherever machines would be. By next, we are going to give an insight over maintenance key parameters, in order to be able to measure properly the maintenance function performance. Afterward, an introduction, over the new concept of e-maintenance along with e-maintenance mind-set, will be presented. Finally, we discuss e-maintenance tools as described in many papers and how they can influence industrial processes.

In the long run, this paper will help authors to select the most adequate industry 4.0 tools related to maintenance. These tools are going to have a clear and direct impact avec industrial processes.

2. CLASSIC MAINTENANCE LIMITS AND KPI'S

Classic maintenance is every maintenance strategy as described before. In spite of the fact that maintenance is a necessity, most industrial actors are still considering maintenance as a necessary evil (without optimizing)[12]. This negative image was attributed to maintenance a long time ago, when only CM operations were carried out and maintenance teams came just to fix things when they broke, even more when things break down maintenance has failed [13].

A few decades ago, maintenance function was viewed as an inherent part of the production function and very tough to manage. As we go, this thought has changed and maintenance became an independent function. Table 1 shows maintenance timeline progression:

Table 1. Maintenance management on time perspective [14]

Period	Progression	How it is viewed
1940 – 1960	Maintenance as a production task	Necessary evil
1960 - 1980	Maintenance as an independent department	Technical specialization
1980 – 2000	Integration efforts	Profit contributor
2000 <	External and internal partnership	Positive cooperation

It's mandatory for the maintenance to be optimal, in order to have the same objectives of organisation ones. These objectives are mainly: cost, reliability, availability, safety, productivity, quality, environment and maintainability. However, with rapid technological progress, classic maintenance is no longer able to keep these KPIs above targets. Many papers were processed in different domains such as Food industry [15], Wastewater Treatment Plant WWTP [16], Aviation [17] and General industry [18]. They all suggest moving up from classic maintenance in order to be aligned with organisation objectives.

It has been noticed that e-maintenance is encompassing many of the solutions proposed for the maintenance to take off that pejorative image and give up suffering from deficiency of understanding and respect.

3. E-MAINTENANCE AND THE NEW WAY OF THINKING

The new way of thinking starts by giving up looking at the maintenance as a necessary evil. Maintenance has to ensure production systems availability and functionality in order to contribute to business objectives [12]. Likewise the new thinking aims to change the maintenance role from fixing breakdowns to taking into account the product life-cycle management [19].

Among the e-maintenance roles we can identify the eco-efficiency. The eco-efficiency consists of considering the maintenance in all product life phases and not only as a set of operations during the production phase. The four product life cycle phases are as follows: product design, manufacturing and assembly, usage and finally disassembly and recycling. The objective won't be producing efficiently anymore but it will be sustaining the equipment usage as late as possible while preserving equipment characteristics in terms of its availability, reliability, safety, cost, productivity and products' quality and also maintainability [21].

B. Iung, E. Levrat, A. Crespo Marquez, H. Erbe[12] have defined maintenance objectives to each product life-cycle while maintaining the global maintenance objective which is to maintain the product conditions and expected services all along its life cycle, objectives by phase are as shown below :

Table 2. Product life-cycle maintenance objectives.

Phase	Objective
Design Engineering	Ensure characteristics like : Maintainability, Reliability, Durability
Manufacturing	Preserve the above characteristics
Usage	Ensure availability, reliability
Disassembling and recycling	Ensure the durability, circular economy

The concept of eco-efficiency has converted maintenance into a major strategic tool with objectives perfectly aligned with business' ones such as: product quality, increasing production capacity, reducing products cost and optimizing deadlines.

As the maintenance is contributing to the value creation during each phase of the four product's life cycle steps and thus to the whole enterprise, we can therefore talk about a maintenance value chain. This value chain must be supported at each cycle step to ensure that assigned objectives have been fulfilled properly. If all objectives are reached, then the global chain is working correctly.

The value chain aims to keep the functional level of the product and to preserve all its characteristics as well as to be in line with business objectives.

Hence, e-maintenance is a philosophy striving to go from "fail and fix" operations to "predict and prevent" strategies [13, 22, 23]. In other words, B. Iung, E. Levrat, A. Crespo Marquez, H. Erbe [12] proposed to shift from considering MTBF [Mean Time Between Failure] to MTBD [Mean Time Between Degradation].

4. E-MAINTENANCE NEW TECHNOLOGIES IMPACT

E-maintenance has had different definitions. The web site www.mtonline.com [12] has considered it as a network that integrates the various maintenance and reliability applications to gather and collect, then deliver asset information when needed. On the other hand, Havard has defined the e of e-maintenance by "Excellent" or "Efficient". Whereas www.deicesword.net states that e-maintenance is a maintenance management concept whereby assets are monitored and managed over the internet.

… After these controversies what would be the real e-maintenance?

E-maintenance is rolling out the principles already defined by Tele-maintenance which are added to web and data services to achieve a true definition of pro-activity or the 'connected plant'.
E-maintenance relies on Intra-Net, Extranet and Internet to processes its IN and OUT. In order to fulfil its tasks, e-maintenance uses means of communication, processing and storage [12]. IT systems play a major role to make e-maintenance tasks successful.

In this section, some technology issues related to e-maintenance will be presented:

- Web services which allow universal access, connectivity and multimedia support for interactivity and interoperability [24],

- Database and its management is also considered as a mandatory tool used in digitalization, globally and in e-maintenance specifically
- Transducers with "built in" Internet modules allow users to connect to internet without PC connection,
- Wireless technology gives the right to flexibility on the floor. Remote data management facilitates transmitting, monitoring and controlling via a network [26],
- New communication pathways in industry allow for more collaboration possibilities…

More specifically, M. Ghouat [28] has studied the impact of new technologies over some indicators such as the availability. Availability is considered as the machines up time, here-below the studies result:

The impact could be characterized as follow:

Important impact
Elevated impact
Normal impact
No impact

Table 3. New technologies and their impact

Technologie	Impact
Enterprise resource Planning ERP	Medium
Manufacturing Execution Systems MES	Normal
Business intelligence BI	No impact
Cloud technology	Medium
Big data analytics	No impact
Machine to machine communication	Important
The Internet of things IoT	Normal
Automatic Identification and data collection	No impact
Radio frequency identification RFID	Normal
Virtual and augmented reality	Important
3D printing	No impact
Simulation	Normal
Cybersecurity	Normal
Miniaturization of electronics	Normal
Robotics, drones and nanotech	Normal

5. UPCOMING WORK

Future work will be a survey targeting different enterprises in France and Morocco categorized as follow:

- primary sector: also known as extractive industries [raw material extraction]. This type of company can be oil extraction companies, mining companies, forestry companies or maritime companies …
- Secondary sector: also known as manufacturing, which affects raw material processing companies into finished or semi-finished products including agri-food, textiles, steel and metallurgy, mechanical engineering and chemical industries

- Tertiary sector: referred to as the service sector, includes companies that are active in sales, trade, finance, real estate, etc. and other non-market activities including education, care and social.

It will also cover all cross-cutting classifications of enterprises, for-profit corporations[small and medium-sized businesses and large groups], private non-profit enterprises that are linked to the social economy and also public structures. To conclude all companies regardless of their sales figures is our target.

This questionnaire will refer to the organization of the maintenance department still in the context of reducing the probability of degradation or failure of operation. It will consider the techniques of maintenance, a dozen of which have caused devastation in the world of the industry for the fluidity of the industrial maintenance of the equipment that several experts have approved. It will deal with maintenance policy, companies are considering technical-economic objectives relating to the management of the equipment so that the actors and the related services have a base. It is necessary to distinguish two levels: the overall level of the company [basic maintenance policy], and the level of equipment [adjusted maintenance policy].

The preparation of the budget and the maintenance costs will also be highlighted given the complementarity and the obligatory nature of their presence in companies.

The means of digitalisation used within companies will also be discussed in order to know and analyse the techniques and digital solutions used. Modern industrial maintenance processes are essential for reliable production.

6. CONCLUSION

E-maintenance is a philosophy and not a technique nor a platform. All industry 4.0 tools and means could be used in e-maintenance. Nevertheless, some are definitely impactful, while others aren’t. Maintenance shouldn’t be seen as a necessary evil but should be considered a value stream that starts and takes place even before the product's manufacturing.

Our next step will be an empirical work based on market survey. The blocs of questions will be basically around company size, maintenance department organization and the industry 4.0 tools used in maintenance field. We will try to reach the highest number of companies with different activities in two different countries who coped successfully with COVID19 pandemic: France, one of the most developed and industrial European economies, with huge consumer market and Morocco which is considered as one of the fastest growing economies in Africa and in the world with ambitious objectives and a versatile economy encompassing local and international companies.

The survey result will come soon and will refer to the current paper to complete this prior work based on literature review.

ACKNOWLEDGEMENT

We would like to express our very great appreciation to our team members for their valuable and constructive suggestions.

REFERENCES

[1] SherifMostafaa*, JantaneeDumrakb and Hassan Soltan. Lean Maintenance Roadmap. PP 2-3Volume 51, Issue 30, 2018, Pages 800-802. https://doi.org/10.1016/j.ifacol.2018.11.192

[2] K. Fraser, 2014, Facilities management: the strategic selection of a maintenance system, Journal of Facilities Management. 12, 18-37.

[3] S.K. Pinjala, L. Pintelon, A. Vereecke, 2006, An empirical investigation on the relationship between business and maintenance strategies, International Journal of Production Economics. 104, 214-229

[4] M. Bevilacqua, M. Braglia, 2000, The analytic hierarchy process applied to maintenance strategy selection. Reliability Engineering & System Safety. 70, 71-83.

[5] B.S. Blanchard, 1997, An enhanced approach for implementing total productive maintenance in the manufacturing environment, Journal of Quality in Maintenance Engineering. 3, 69-80.

[6] T. Santos, F. J. G. Silva*, S. F. Ramos, R. D. S. G. Campilho, L. P. Ferreira. Asset Priority Setting for Maintenance Management in the Food Industry. Volume 38, 2019, Pages 1623-1633.https://doi.org/10.1016/j.promfg.2020.01.122

[7] P. Neves, F. J. G. Silva, L. P. Ferreira, T. Pereira, A. Gouveia, and C. Pimentel, 2018, Implementing Lean Tools in the Manufacturing Process of Trimmings Products, Procedia Manufacturing 17 696-704.

[8] Márquez, A.C., 2007, The maintenance management framework: models and methods for complex systems maintenance. Springer.

[9] M.M. Fouladgar, A. Yazdani-Chamzini, A. Lashgari, E. K. Zavadskas, Z. Turskis, 2012, Maintenance strategy selection using AHP and COPRAS under fuzzy environment, International Journal of Strategic Property Management. 16, 85-104.

[10] G.Waeyenbergh, L. Pintelon, 2004, Maintenance concept development: A case study, International Journal of Production Economics. 89, 395-405.

[11] Srinivas Kumar Pinjalaa, Liliane Pintelona,_, Ann Vereecke . An empirical investigation on the relationship betweenbusiness and maintenance strategies? Volume 104, Issue 1, November 2006, Pages 214-229. https://doi.org/10.1016/j.ijpe.2004.12.024

[12] B.Iung, E.Levrat, Crespo.Marquez, H.Erbe E-Maintenance: Principles, review and conceptual framework. Volume 40, Issue 19, 2007, Pages 18-29. https://doi.org/10.3182/20071002-MX-4-3906.00005

[13] Blann Dale R. (2003), Reliability as a Strategic Initiative: To Improve Manufacturing Capacity, Throughput and Profitability Asset Management &Maintenance Journal, 16(2).

[14] Pintelon, L., Gelders, L., Van Puyvelde, F., 2000. Maintenance Management, second ed. Acco Belgium, Leuven.

[15] T. Santos, F. J. G. Silva*, S. F. Ramos, R. D. S. G. Campilho, L. P. Ferreira. Asset Priority Setting for Maintenance Management in the Food Industry. Volume 38, 2019, Pages 1623-1633. https://doi.org/10.1016/j.promfg.2020.01.122

[16] Vicent Hernández-Chover∗, Lledó Castellet-Viciano, Francesc Hernández-Sancho. Preventive maintenance versus cost of repairs in asset management: An efficiency analysis in wastewater treatment plants. Volume 141, September 2020, Pages 215-221 https://doi.org/10.1016/j.psep.2020.04.035

[17] Tseko Mofokeng, Paul T Mativenga, Annlizé Marnewick. Analysis of aircraft maintenance processes and cost. Volume 90, 2020, Pages 467-472. https://doi.org/10.1016/j.procir.2020.01.115

[18] Xh Mehmeti, B Mehmeti, Rr Sejdiu . The equipment maintenance management in manufacturing enterprises. Volume 51, Issue 30, 2018, Pages 800-802. https://doi.org/10.1016/j.ifacol.2018.11.192

[19] Takata S., F. Kimura, F.J.A.M. van Houten, E. Westkämper, M. Shpitalni, D. Ceglarek, J. Lee(2004), Maintenance: Changing Role in Life Cycle Management, Annals of the CIRP, 53/2, pp 643 – 656

[20] Van Houten F.J.A.M., Tomiyama T., Salomons O.W., (1998), Product modelling for model-based maintenance, Annals of the CIRP, 47/1, pp123-129

[21] DeSimone, L. D., Popoff, F. with the WBCSD (1997), Eco-Efficiency, MIT Press.

[22] Lee J., J. Ni, D. Djurdjanovic, H. Qiu and H. Liao (2006), intelligent prognostics tools and emaintenance, Computers in Industry, Special issue on e-maintenance, 57(6), pp 476-489

[23] Iung B., Morel G., Léger J.B. (2003) Proactive maintenance strategy for harbor crane operation improvement, Robotica, Special issue on Cost Effective Automation, Eds H. Erbe, 21(3), pp.313-324.

[24] Lee J. (1998). Teleservice engineering in manufacturing: challenges and opportunities. Int. Journal of Machine Tools & Manufacture. 38, pp 901-910.

[25] Wang, J., Tse, P., He, L.S. and R. Yeung (2004). Remote sensing, diagnosis and collaborative maintenance with Web-enabled virtual instruments and mini-servers. International Journal of Advanced Manufacturing Technology, 24(9-10), pp. 764 – 772.

[26] Egea-Lopez E., Martinez-Sala A., Vales-Alonso J., Garcia-Haro J. and Malgosa-Sanahuja J-M. (2005). Wireless communications deployment in industry: a review of issues, options and technologies. Computers in Industry, 56 (1), January, pp. 29-53.

[27] M. Ghouat A. Haddout, M. Benhadou. Impact of industry 4.0 concept on the levers of Lean Manufacturing approach in manufacturing industries. International journal of automotive and mechanical engineering (IJAME). ISSN: 2229-8649 e-ISSN: 2180-1606 VOL. 18, ISSUE 1, 8523 – 8530 DOI: https://doi.org/10.15282/ijame.18.1.2021.11.0646

AUTHOR

Yassine MOUMEN, 28 November 1990, Engineer in maintenance

Lattice Based Group Key Exchange Protocol in the Standard Model

Parhat Abla

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing China,
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing China

Abstract. Group key exchange schemes allow group members to agree on a session key. Although there are many works on constructing group key exchange schemes, but most of them are based on algebraic problems which can be solved by quantum algorithms in polynomial time. Even if several works considered lattice based group key exchange schemes, believed to be post-quantum secure, but only in the random oracle model.
In this work, we propose a group key exchange scheme based on ring learning with errors problem. On contrast to existing schemes, our scheme is proved to be secure in the standard model. To achieve this, we define and instantiate multi-party key reconciliation mechanism. Furthermore, using known compiler with lattice based signature schemes, we can achieve authenticated group key exchange with post-quantum security.

Keywords: Group key exchange; Lattice; Ring LWE,

1 Introduction

Cryptographic key exchange protocols can establish a "secure channel" among the participants, connected by insecure communication networks, by enabling them agree on a session key. Through this channel, participants can transmit sensitive data or apply other higher-level cryptographic schemes. The confidentiality of this channel usually can be reduced to the security of the cryptographic protocols.

Since Diffie-Hellman's two party key exchange protocol [13], the work of [22, 24] are focus on designing two-party protocols based on various hard problems and improving their efficiency. There are many works [4, 8–11] on considering the multi-party scenario. However, aforementioned protocols's security are based on classically hard problems which can be solved in polynomial time by quantum algorithms [29].

Since the quantum resistance of lattice problems, especially the hardness of LWE problems [7, 23, 25, 27, 28], most of the recent works [1, 6, 14, 18, 19, 26, 30]

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 157-174, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111113

mainly focus on designing and improving the quality of lattice based two party protocols. On the other hand, only a few works [2, 14] focus on designing lattice based group key exchange(GKE) protocols, but they have their own drawbacks as we show next.

The work of [14] is the first try of constructing lattice based key exchange scheme, but it is lack of standard security proof. Even if the work of [2] proposed a constant round GKE protocols base on plain LWE problem. But, their protocols only proven secure in the random oracle model [3], which usually replaced by cryptographic hash functions in a real world applications. But there exist cryptographic schemes that are secure in the Random Oracle Model, but for which any implementation yields insecure schemes [12]. Therefore, security in the standard model is more plausible for the cryptographic schemes. To our knowledge, designing and modular analyzing of a group key exchange protocols in the standard model are not considered yet. Even if a GKE scheme can be obtained by a two-party key exchange scheme, but this approach believed to be very impractical, hence we consider the direct construction.

1.1 Our Contributions

In this work, we analyze and construct a multi-party group key exchange protocol. As shown in the work of [18], the key reconciliation mechanism(KRM) is necessary for a LWE based key exchange protocols. Therefore, we first introduce the concept of multi-party KRM and show it's concrete instantiation. Our definition of the multi-party KRM can be regarded as the generalization of the two-party KRM [14, 19, 26]. In a multi-party key reconciliation mechanism, each party should own predetermined informations to ensure that each party have a same element after running the multi-party KRM. Its not hard to see that multi-party KRM is not enough to get a group key exchange protocol because the correctness of KRM need the pre-determined value(input to the KRM) satisfy some proper constraints. Therefore, this is why we need other additional tools to get GKE. For the security, we require that KRM's output should random even if the transactions are exposed.

To instantiate, we designe a new multi-party key reconciliation mechanism. Compared to a naive generalization of the two-party case [14], our instantiation can be applied to both for odd and even modulus. Meanwhile, the previous key reconciliation mechanism of [14] only fits for the odd modulus. Furthermore, our design is as efficient as [14] in the two-party settings. Roughly, we have following result.

Theorem 1.1 (informal) *For the integers p, q, g such that $p < q$, $q > p(g + 1)$ and $gcd(q, g) = 1$, there exist a multi-party KRM that is secure and correct.*

Additionally, we introduce a weaker version of GKE. In contrast to GKE, a weak GKE only enables the participants to agree on some approximately the same

element. Obviously, any GKE protocol is also a weak GKE, but the reverse is not the case. Therefore, constructing this weak definition of GKE at most as hard as constructing a general GKE.

The correctness of a weak GKE is similar to the case of GKE except the final output of a weak GKE should belongs to some range with overwhelming probability. But the security of weak GKE is a crux. In a GKE protocol, there is no difference between the following two cases:(1) the adversary is given one key of the parties, and (2) the adversary is given all parties's keys. This is the case in a GKE, since the correctness of GKE guarantees that all parties's keys are equal. But this is not the case in the weak GKE. Because in a weak GKE, the participants will obtain an approximately the same keys. However, we define passive security of weak GKE and present the our instantiation of weak GKE for sake of such weak GKE's existence.

Finally, we construct a GKE in the standard model. Roughly speaking, we show that a secure multi-party KRM and a secure weak GKE implies passively secure GKE. Intuitively, the weak GKE ensures that each party have approximately the same element, and then applying the multi-party KRM, each party will agree on a same session key. The correctness of corresponding GKE can be reduced to the correctness of the KRM and the weak GKE. The security analysis is more subtle, and we elaborate it in section 5. Additionally, combining the previous instantiations, we show the instantiation of the GKE.

1.2 Related Works and Comparison

There are sequence of works [1, 6, 14, 19, 26, 30] are working on designing and improving the two-party KRM and authenticated key exchange schemes from lattices.

Even if the works of [14, 19, 26] designed KRM, but they only focused on two-party case. Our KRM design is applicable for both two party and multi-party case. Variants of above designs are submitted to the NIST post-quantum cryptography competition. But they mainly focused on designing KEMs, and then designed two-party key exchange protocols through this KEMs. Obviously, this approach seem to be more centralized and heavily rely on one party. Hence we didn't consider this research line in designing multi-party case.

Apon et.al [2] proposed constant round lattice based GKE, but their scheme only proven secure in the random oracle model. In contrast, our GKE protocol is proven secure in standard model which is a more plausible security for a cryptographic scheme.

Organizations In section 2 we present basic notations, definitions and some useful results from literatures. In section 3 we introduce multi-party KRM and its concrete instantiation. We define and instantiate a waker version of group key exchange protocol in section 4. finally we construct a secure group key exchange protocol in the standard model.

2 Preliminaries

Notations For a real $x \in \mathbb{R}$, denote the largest integer which smaller than x by $\lfloor x \rfloor$. For any natural integer $n \in \mathbb{N}$, the symbol $[n]$ denotes the index set $\{0, 1, \cdots, n-1\}$. For any positive integer q, let $\mathbb{Z}_q$ be the cyclic group $\{0, 1, 2, ..., q-1\}$ with addition modulo q. For any reals a, b, c such that $a \leq b$, the shifted set $c + (a, b)$ denotes the interval $(a + c, b + c)$. We abuse the notions for the half closed and closed intervals in $\mathbb{Z}_q$ in a similar way. For any two elements $x, y \in \mathbb{Z}_q$, we let $|x - y|$ be the value of $\min_{k \in \mathbb{Z}} |x - y + kq|$. Vectors are denoted with bold lower-case letters(e.g., $\boldsymbol{a}$). For any set S and $n \in \mathbb{N}$, the set of n-dimensional vectors with entries in S is denoted by S^n, and the set of n-by-m matrices with entries in S is denoted by $S^{n \times m}$. For any probability distribution χ with probability space Ω, the notion $x \xleftarrow{\chi} \Omega$ mean that x is sampled from Ω according to χ. If the probability space is clear from the context, we simplify the notion as $x \leftarrow \chi$. If χ is uniform distribution, we omit it for the sake of simplicity, e.g., $x \leftarrow \Omega$. We say a function $\epsilon(\lambda)$ is negligible if $\frac{1}{\epsilon(\lambda)}$ is larger than all polynomial $\mathsf{poly}(\lambda)$ from some point λ_0.

2.1 Group Key Exchange Protocol

In this section, we recall the concepts relevant to group key exchange and key reconciliation mechanisms.

GKE: A Group key exchange protocol enables the participated parties agree on a random session key. During the process, participants may run different scripts, but after all interaction and calculation processes, they will agree on a same session key. The security of GKE require that the agreed session key is indistinguishable from an equal-length random string. Here we recall the definition, correctness, and security of GKE as follow:

Definition 2.1 *A Group key exchange protocol* GKE *consists of three algorithms* $(\mathsf{GKE.Setup}, \mathsf{Interact}, \mathsf{KeyGen})$ *as follow:*

- $\mathsf{GKE.Setup}(1^\lambda, 1^N) \rightarrow \mathsf{pp}$: *On input the security parameter* λ *and number of participants* N*, it outputs a general public parameter* pp*.*
- $\mathsf{Interact}(P_i, \mathsf{pp})_{i \in [N]} \rightarrow \{\mathsf{trans}_i, \mathsf{st}_i\}_{i \in [N]}$: *After receiving the public parameter* pp*, each party* P_i *run its own script which calculate, receive, and broadcast data transmitted through public tunnel. Use* trans_i *to denote the data sets received and sent by* P_i*, and denote the after all state of* P_i *by* st_i*.*
- $\mathsf{KeyGen}(\mathsf{pp}, P_i, \{\mathsf{trans}_i, \mathsf{st}_i\})_{i \in [N]} = \{K_i\}_{i \in [N]}$: *On input public parameter* pp*, transaction* trans_i*, party* P_i *computes its own session key* K_i*.*

Definition 2.2 (Correctness.) *We say a* GKE *is correct if for some random string K, the probability*

$$\mathsf{Pr}\left[\bigwedge_{i\in[N]} K_i = K \middle| \begin{array}{l} \mathsf{pp} \leftarrow \mathsf{GKE.Setup}(1^\lambda, 1^N) \\ \{\mathsf{trans}_i, \mathsf{st}_i\}_{i\in[N]} \leftarrow \mathsf{Interact}(P_i, \mathsf{pp})_{i\in[N]} \\ \{K_i\}_{i\in[N]} := \mathsf{KeyGen}\left(\mathsf{pp}, P_i, \{\mathsf{trans}_i, \mathsf{st}_i\}\right)_{i\in[N]} \end{array}\right]$$

is $\mathsf{negl}(\lambda)$*, where probability is taken over the randomness of* KeyGen *algorithm and randomness of* Interact *algorithm.*

For a probabilistic polynomial time algorithm $\mathcal{A}$ and key space $\mathcal{K}$ of GKE, we define the advantage of $\mathcal{A}$ against GKE, denoted $\mathsf{Adv}^{\mathsf{GKE}}_{\mathcal{A}}$, as

$$\mathsf{Pr}\left[b' = b \middle| \begin{array}{l} \mathsf{pp} \leftarrow \mathsf{GKE.Setup}(1^\lambda, 1^N) \\ \{\mathsf{trans}_i, \mathsf{st}_i\}_{i\in[N]} \leftarrow \mathsf{Interact}(P_i, \mathsf{pp})_{i\in[N]} \\ \{K_i\}_{i\in[N]} := \mathsf{KeyGen}(\mathsf{pp}, P_i, \{\mathsf{trans}_i, \mathsf{st}_i\})_{i\in[N]} \\ b \xleftarrow{\$} \{0,1\},\ \text{if } b = 0, K^* \xleftarrow{\$} \mathcal{K},\ \text{else } K^* := K_0 \\ b' \leftarrow \mathcal{A}(\{\mathsf{trans}_i\}_{i\in[N]}, \mathsf{pp}, K^*) \end{array}\right] - \frac{1}{2},$$

where the probability is taken over the randomness of KeyGen algorithm, randomness of Interact algorithm and random coin toss of b. we define the eavesdropper(passive) security of a GKE as follows.

Definition 2.3 (Security.) *We say protocol* GKE *is passively secure if the advantage* Adv *of any* PPT *algorithm $\mathcal{A}$(eavesdropper) is negligible in the security parameter λ, i.e.,* $\mathsf{Adv}^{\mathsf{GKE}}_{\mathcal{A}}(\lambda) \leq \mathsf{negl}(\lambda)$.

If a GKE protocol remain secure in a case where the adversary capable of completely controlling over all the communications in the network, We say GKE is adaptively secure. Fortunately, there is a compiler [21] transforms a passively secure GKE into an adaptive one. Note that this compiler need a secure signature scheme. Fortunately, there are lattice based signature schemes [15–17] which are strongly unforgeable under adaptive chosen message attack (EUF-CMA), and it's enough for the compiler. In other words, if there is a lattice based GKE, then we have a lattice based athenticated GKE. Hence in this work, we mainly focus on constructing GKE.

2.2 Gaussians and Ring LWE

Here, we recall definitions and some useful results of gaussian distributions and ring Learning With Errors(LWE) problems.

Lattice and Gaussian. A n-dimensional lattice L is the discrete subgroup of $\mathbb{R}^n$. A lattice can be generated by n linearly independent basis $B = \{\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_n\}$ as $L = L(\mathbf{B}) := \{\sum_{i=1}^n k_i \mathbf{b}_i | k_i \in \mathbb{Z}\}$. For a real $s > 0$, the gaussian distribution function on a real $x \in \mathbb{R}$ is defined as $\rho_s(x) = e^{-\pi \frac{x^2}{s^2}}$. For a positive matrix Σ, we extend

the definition over a n-dimensional vector $\boldsymbol{x} \in \mathbb{R}^n$ by letting $\rho_\Sigma(\boldsymbol{x}) = e^{-\pi\|\boldsymbol{x}\Sigma\boldsymbol{x}\|^2}$. For a probability distribution ρ and a S subset of ρ's support, we let $\rho(S) := \sum_{x\in S}\rho(x)$. For a natural number n and a discrete set $S \subset \mathbb{Z}^n$, the discrete gaussian distribution $D_s : S^n \to [0,1]$ is defined as $D_{S,s}(\boldsymbol{x}) := \frac{\rho_s(\boldsymbol{x})}{\rho_s(S^n)}$. For a polynomial $\boldsymbol{a} = \sum_{i\in[n]} a_i x^i$, we say $\boldsymbol{a}$ is sampled from $D_{\mathbb{Z},s}^{\mathsf{Coeffs}}$, if the coefficient vector $\boldsymbol{a} = (a_0, a_1, \cdots, a_{n-1})$ is sampled from $D_{\mathbb{Z},s}$.

ring-LWE. Before recalling the definitions of ring LWE, we first define the rings that we work on in this paper. One thing need to be noticed that our construction of GKE and instantiation of key reconciliation mechanisms are independent of concrete instantiations. The reason of using ring LWE is because of its compactness and commutativity. One can instantiate the scheme with plain LWE or any version of learning with rounding problems following the constraints of GKE.

Let n be a power of 2, we define the polynomial ring $R := \mathbb{Z}[x]/(x^n+1)$ and let R_q be the quotient R/qR for some positive integer q. For a $s \in R_q$ and gaussian parameter s, we say a pair (a,b) is sampled from the R-LWE distribution, denoted $A_{n,q,s}$, if a is uniformly sampled from R_q and $b = as + e$ for some error term e sampled from $D_{\mathbb{Z},s}^{\mathsf{Coeffs}}$. The goal of R-LWE problem is to distinguish the samples of $A_{n,q,s}$ from the same number of samples of $\mathcal{U}(R_q) \times \mathcal{U}(R_q)$.

Definition 2.4 (ring-LWE) *For any positive integers n, q and gaussian parameter s, we say R-$\mathsf{LWE}_{n,k,q,s}$ is hard if for all* PPT *adversary $\mathcal{A}$, the following holds :*

$$\mathsf{Pr}\left[b' = b \;\middle|\; \begin{array}{l} b \xleftarrow{\$} \{0,1\}; \\ \textit{if } b = 1, (a_i,b_i)_{i\in[k]} \leftarrow A_{n,q,s}^k; \\ \textit{else }, (a_i,b_i)_{i\in[k]} \xleftarrow{\$} R_q^k \times R_q^k; \\ b' \leftarrow \mathcal{A}((a_i,b_i)_{i\in[k]}); \end{array}\right] - \frac{1}{2} \leq \mathsf{negl}(\lambda),$$

where the probability is over the randomness of all the coin tosses.

Theorem 2.5 [20] *Let α be a positive real, m be a power of 2, l be an integer, $\Phi_m(X) = X^n + 1$ be the m-th cyclotomic polynomial where $m = 2n$, and $R = Z[X]/(\Phi_m(X))$. Let $q \equiv 3 \mod 8$ be a (polynomial size) prime such that there is another prime $p \equiv 1 \mod m$ satisfying $p \leq q \leq 2p$. Let also $\alpha q \geq n^{1.5}k^{0.25}\omega(\log^{2.25}(n))$. Then, there is a probabilistic polynomial-time quantum reduction from $O(n/\alpha)$-approximate SIVP (or SVP) to $RLWE_{n,k,q,\alpha q}$.*

Above theorem shows that for the parameters satisfying the constraints in above theorem, $RLWE_{n,k,q,\alpha q}$ problem is hard if assuming the $O(n/\alpha)$-approximate SIVP is hard. Furthermore, its believed that SIVP remains hard even if the large scale quantum computers are available. Therefore, it is reasonable to assume that the $RLWE_{n,k,q,\alpha q}$ based cryptographic schemes are post-quantum.

3 Multi-Party Key Reconciliation

3.1 Definition

KRM: A key reconciliation mechanism enables participated parties to obtain a key from roughly the same elements. A significant difference between KRM and GKE is that KRM requires all the parties should have some approximately the same elements beforehand. But a GKE not need this requirement at all. Here in what follows, we define the multi-party KRM with its correctness and security.

Definition 3.1 *A N-party key reconciliation mechanism* KeyRek *consist of tuples* $(\mathsf{KeyRek.Hint}, \mathsf{KeyRek.KeyGen})$*, described as follow:*

- $\mathsf{KeyRek.Hint}(b_i)_{i\in[N]} \to \{h_i\}_{i\in[N]}$: *On input b_i, each party P_i for $i \in [N]$ runs this algorithm to obtain a hint message h_i and broadcast it to other parties.*
- $\mathsf{KeyRek.KeyGen}(b_i, \{h_i\}_{i\in[N]})_{i\in[N]} :\to \{K_i\}_{i\in[N]}$: *On input b_i and $\{h_i\}_{i\in[N]}$, each party P_i runs this algorithm to obtain a key K_i.*

where the b_is are the predetermined approximately same elements.

Correctness. For a KRM, we require all the agreed keys are equal except with negligible probability. The formal definition is as follow.

Definition 3.2 *We say multi-party* KeyRek *is correct with respect to β if $\|b_i - b_j\| \leq \beta$ for all $i, j \in [N]$ and for some random string K, the probability*

$$\mathsf{Pr}\left[\bigwedge_{i\in[N]} K_i = K \middle| \begin{matrix}\{h_i\}_{i\in[N]} \leftarrow \mathsf{KeyRek.Hint}(b_i)_{i\in[N]};\\ \{K_i\}_{i\in[N]} := \mathsf{KeyRek.KeyGen}(b_i, \{h_i\}_{i\in[N]})\end{matrix}\right]$$

is at least $1 - \mathsf{negl}(\lambda)$, where the probability is taken over the randomness of b_i.

Security. For any PPT algorithm $\mathcal{A}$ and key space $\mathcal{K}$ of KeyRek, the advantage of $\mathcal{A}$ against the protocol KeyRek, denoted $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{KeyRek}}$, is defined as

$$\mathsf{Pr}\left[b' = b \middle| \begin{matrix}\{h_i\}_{i\in[N]} \leftarrow \mathsf{KeyRek.Hint}(b_i)_{i\in[N]};\\ \{K_i\}_{i\in[N]} := \mathsf{KeyRek.KeyGen}(b_i, \{h_i\}_{i\in[N]});\\ b \xleftarrow{\$} \{0,1\},\ \text{if } b = 0, K^* :\xleftarrow{\$} \mathcal{K},\ \text{else } K^* := K_0;\\ b' \leftarrow \mathcal{A}(\{h_i\}_{i\in[N]}, K^*)\end{matrix}\right] - \frac{1}{2},$$

where the probability is taken over the randomness of b_is and the random coin toss of b. We say KeyRek is secure if the above advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{KeyRek}}$ is negligible in the security parameter λ. Note that b_is are approximately the same elements, but it's unknown and random to the adversary. A secure KeyRek should reveals nothing about K_i to the adversary except the public message h_i derived from b_i.

3.2 Instantiation

Here, we instantiate the KRM in Definition3.1 with more special case in which only one participant's hint message is suffice for all the participants to agree on the same session key. In below, we generalized the KRM of [14]. Our description of $\mathsf{KeyRek} = (\mathsf{Hint}, \mathsf{KeyGen})$ is as below where we omit the input integers q, p, g as they are implicitly contained in both algorithms.

Construction 3.3 *For the integers q, p, g such that $2 \leq p$, $p(g+1) < q$ and $gcd(q, g) = 1$, the construction of $\mathsf{KeyRek} = (\mathsf{Hint}, \mathsf{KeyGen})$ as follows:*

$\mathsf{Hint}(K') \to h$ *: On input $K' \in \mathbb{Z}$, it runs as follow:*

- *(1)* $i \xleftarrow{\$} \mathbb{Z} \cap (-\frac{g}{2}, \frac{g}{2}]$
- *(2)* $h = \lfloor p - \frac{p}{q}K' + \frac{1}{2} + \frac{p}{q}i \rfloor \mod p$
- *(3) Outputs h*

$\mathsf{KeyGen}(K, h) = k$ *: On input $K \in \mathbb{Z}$ and $h \in \mathbb{Z}_p$, it runs:*

- *(1)* $k = (K + \lfloor h\frac{q}{p} \rfloor \mod^{\pm} q) \mod g$
- *(2) Outputs k*

For any integer $x \in \mathbb{Z}$, we let $(x \mod^{\pm} q)$ be an integer in $(\frac{-q}{2}, \frac{q}{2}]$. In what follows, we prove the correctness and security of above KeyRek.

Theorem 3.4 *For the integer parameters as in Construction3.3, if for any $K', K \in \mathbb{Z}_q$, there is an integer d such that $K - K' = dg$ and $|dg| \leq q\frac{p-1}{2p} - \frac{g+1}{2}$, then we have*

$$\mathsf{KeyGen}(K', h) = \mathsf{KeyGen}(K, h),$$

where $h = \mathsf{Hint}(K')$.

Proof. Since $K = dg + K'$, we re-write $\mathsf{KeyGen}(K, h)$ as

$$\begin{aligned}
&\mathsf{KeyGen}(K, h) = \mathsf{KeyGen}(K' + dg, h) \\
=&\left(K' + \left\lfloor h\frac{q}{p} \right\rfloor + dg \mod^{\pm} q\right) \mod g \\
=&\left(\underbrace{((K' + \left\lfloor h\frac{q}{p} \right\rfloor \mod^{\pm} q)}_{\leq \frac{q}{2p} + \frac{g+1}{2} \leq \frac{q}{2} - |dg|} + \underbrace{dg}_{\leq |dg|}) \mod^{\pm} q\right) \mod g.
\end{aligned}$$

Since $|dg| \leq q\frac{p-1}{2p} - \frac{g+1}{2} < \frac{q}{2}$, we have $\frac{q}{2} - |dg| \geq \frac{q}{2p} + \frac{g+1}{2}$. So if $|(K' + \lfloor h\frac{q}{p} \rfloor \mod^{\pm} q)| \leq \frac{q}{2p} + \frac{g+1}{2}$, then we can remove the second $\mod^{\pm} q$ operation from the

representation of $\mathsf{KeyGen}(K,h)$. That is to say, $\mathsf{KeyGen}(K,h)$ can be re-written as

$$\begin{aligned}\mathsf{KeyGen}(K,h) &= \left(K' + \lfloor h\frac{q}{p}\rfloor \mod {}^{\pm}q\right) + dg \mod g \\ &= \left(K' + \lfloor h\frac{q}{p}\rfloor \mod {}^{\pm}q\right) \mod g \\ &= \mathsf{KeyGen}(K',h)\end{aligned}$$

Therefore, to compete the proof, we need to show: $|(K'+\lfloor h\frac{q}{p}\rfloor \mod {}^{\pm}q)| \leq \frac{q}{2p}+\frac{g+1}{2}$.

Replacing the h in $(K' + \lfloor h\frac{q}{p}\rfloor \mod {}^{\pm}q)$ with explicit representation of h in Hint, it's easy to see the following

$$\begin{aligned}&|(K' + \lfloor h\frac{q}{p}\rfloor \mod {}^{\pm}q)| \\ =\ &|\lfloor \underbrace{K' + \frac{q}{p}(\lfloor p - \frac{p}{q}K' + \frac{1}{2} + \frac{p}{q}i\rfloor \mod p)}_{\in\left(\kappa\cdot q-\frac{q}{2p}+i,\kappa\cdot q+\frac{q}{2p}+i\right]}\rfloor \mod {}^{\pm}q|,\end{aligned}$$

where κ is some integer. In addition, we have that $(K'+\lfloor h\frac{q}{p}\rfloor \mod {}^{\pm}q) \in \left(\frac{-q}{2p}+i, \frac{q}{2p}+i\right]$, and thus $|(K' + \lfloor h\frac{q}{p}\rfloor \mod {}^{\pm}q)| \leq \frac{q}{2p} + \frac{g+1}{2}$. This completes the proof. □

The following theorem shows the uniformity of our KeyRek.

Theorem 3.5 *For the parameters as in Construction3.3, and a uniform K, the $\mathsf{KeyGen}(K,h)$ is uniformly distributed conditioned on $h = \mathsf{Hint}(K)$, i.e.,*

$$\Pr_{K\leftarrow\mathbb{Z}_q}[\mathsf{KeyGen}(K,h) = k|\mathsf{Hint}(K) = h] = \frac{1}{g},$$

where $k \in \mathbb{Z}_g$.

Proof. Let $\mathsf{Hint}(K,i)$ be the deterministic version of $\mathsf{Hint}(K)$(making the implicit randomness $i \in \mathbb{Z}_g$ as an explicit input), proving following two statements is suffice to complete the proof.

(1) For any $i \in \mathbb{Z}_g$, we have

$$\Pr_{K\leftarrow\mathbb{Z}_q}[\mathsf{Hint}(K,i) = h] = \frac{|T_h^i|}{q}, \text{ and}$$

$$\Pr_{K\leftarrow\mathbb{Z}_q}[\mathsf{KeyGen}(K,h) = k \wedge \mathsf{Hint}(K,i) = h] = \frac{|T_{h,k}^i|}{q},$$

where T_h^i and $T_{h,k}^i$ are defined as

$$T_h^i := \left(\frac{q}{p}(p-h-\frac{1}{2})+i, \frac{q}{p}(p-h+\frac{1}{2})+i\right],$$
$$T_{h,\kappa}^i := \{x \in T_h^i | \mathsf{KeyGen}(x,h) = \kappa\}.$$

(2) For any $i \in \mathbb{Z}_g$ and $T_h^i, T_{h,\kappa}^i$ defined above, we have

$$T_h^i := \bigcup_{\kappa \in \mathbb{Z}_g} T_{h,\kappa}^i, |T_h^i| = |T_h^0|, \text{ and}$$

$$|T_h^0| = \sum_{\kappa \in \mathbb{Z}_g} |T_{h,\kappa}^i| = \sum_{i \in \mathbb{Z}_g} |T_{h,k}^i|.$$

This is the case, since we have

$$\begin{aligned}
&\Pr_{K \leftarrow \mathbb{Z}_q} [\mathsf{KeyGen}(K,h) = k | \mathsf{Hint}(K) = h] \\
&= \frac{1}{g} \sum_{i \leftarrow \mathbb{Z}_g} \Pr_{K \leftarrow \mathbb{Z}_q} [\mathsf{KeyGen}(K,h) = k | \mathsf{Hint}(K,i) = h] \\
&= \frac{1}{g} \sum_{i \leftarrow \mathbb{Z}_g} \frac{\Pr_{K \leftarrow \mathbb{Z}_q} [\mathsf{KeyGen}(K,h) = k \wedge \mathsf{Hint}(K,i) = h]}{\Pr_{K \leftarrow \mathbb{Z}_q} [\mathsf{Hint}(K,i) = h]} \\
&= \frac{1}{g} \sum_{i \leftarrow \mathbb{Z}_g} \frac{\frac{|T_{h,k}^i|}{q}}{\frac{|T_h^i|}{q}} = \frac{1}{g}
\end{aligned}$$

where the first and second equality is by property of probability; the third equality is by statement (1); the last equality is by the statement (2). In what follows, we prove (1) and (2)

Now, we prove (1). We first show $\Pr_{K \leftarrow \mathbb{Z}_q} [\mathsf{Hint}(K,i) = h] = \frac{|T_h^i|}{q}$ as follow: From the definition of T_h^i, it is easy to verify that, for any $x \in T_h^i$ we have $\mathsf{Hint}(x,i) = h$; Furthermore, T_h^is are disjoint and $\mathbb{Z}_q = \cup_{\bar{h} \in \mathbb{Z}_p} T_{\bar{h}}^i$, and thus for any $x \notin T_h^i$, there is some $h' \neq h$ such that $x \in T_{h'}^i$ and $\mathsf{Hint}(x,i) = h' \neq h$. It is obvious from the definition of $T_{h,k}^i$ that $\Pr_{K \leftarrow \mathbb{Z}_q} [\mathsf{KeyGen}(K,h) = k \wedge \mathsf{Hint}(K,i) = h] = \frac{|T_{h,k}^i|}{q}$.

Next, we prove (2). Since KeyGen is deterministic algorithm of K and h, $T_{h,k}^i$s are the partitioning of T_h^i, that is $T_h^i = \cup_{\kappa \in \mathbb{Z}_g} T_{h,\kappa}^i$. Observing the definition of T_h^i, it's not hard to find that T_h^i is the shift of T_h^0(e.g., $T_h^i = T_h^0 + i$), and thus $|T_h^i| = |T_h^0|$. To show $\sum_{\kappa \in \mathbb{Z}_g} |T_{h,\kappa}^i| = \sum_{i \in \mathbb{Z}_g} |T_{h,k}^i|$, verifying the existence of a bijection between

$T^i_{h,k}$ and $T^{i-1}_{h,k-1}$ is suffice. This is the case, because we have $|T^i_{h,k}| = |T^{i-1}_{h,k-1}|$ in this case, and

$$\sum_{i\in\mathbb{Z}_g} |T^i_{h,k}| = \sum_{i\in\mathbb{Z}_g} |T^0_{h,k-i}| = \sum_{\kappa\in\mathbb{Z}_g} |T^0_{h,\kappa}| = |T^0_h|.$$

Here, we define the map $f : T^i_{h,k} \longrightarrow T^{i-1}_{h,k-1}$ as $f(x) = x - 1$ and prove this is a bijective map. We first show that for any $x \in T^i_{h,k}$, $f(x) \in T^{i-1}_{h,k-1}$. From the definition of the algorithms Hint and KeyGen, we have $\mathsf{Hint}(x-1, i-1) = \mathsf{Hint}(x, i) = h$ and $\mathsf{KeyGen}(x-1, h) = k-1 \mod g$, and thus $f(x) \in T^{i-1}_{h,k}$. It's straight that f is bijective map. This completes the proof. □

The following is a multi-party KRM using the Construction3.3 as a building block.

Construction 3.6 *A N-party key reconciliation mechanism* KeyRek *is consist of algorithm tuples* $(\mathsf{KeyRek.Hint}, \mathsf{KeyRek.KeyGen})$ *as follow:*

- $\mathsf{KeyRek.Hint}(b_i)_{i\in[N]} \to \{h_i\}_{i\in[N]}$: *On input b_0, party P_0 computes $h_0 = \mathsf{Hint}(b_0)$ and broadcast h_0 to other parties, then each party P_i set $h_i = h_0$.*
- $\mathsf{KeyRek.KeyGen}(b_i, \{h_i\}_{i\in[N]})_{i\in[N]} :\to \{K_i\}_{i\in[N]}$: *On input b_i and $\{h_i\}_{i\in[N]}$, each party P_i runs $\mathsf{KeyGen}(b_i, \{h_i\}_{i\in[N]})$ to obtain a key k_i.*

where the b_is are the predetermined approximately same elements.

As described in above Construction3.6, this KeyRek is a special case of Definition3.1. In general, we have following result.

Theorem 3.7 *For the integers p, q, g such that $p < q$, $q > p(g+1)$ and $gcd(q, g) = 1$, there exist a multi-party KRM that is secure and correct respect to $q\frac{p-1}{2pg} - \frac{g+1}{2g}$.*

Proof. The Construction3.6 is the witness to the existence of such multi-party KRM. The security and correctness are simply followed from the Theorem3.5 and the Theorem3.4. □

4 A Weaker Version of GKE

In this section, we define a weak version of GKE, and then we show the RLWE based instantiation.

4.1 Weak GKE

The correctness of a GKE protocol guarantees that the participated parties can have the same session key. But, in this section, we degrade the correctness of the GKE protocol, and we call this new degraded protocol as *weak* GKE. More specifically,

at the end of a *weak* GKE, the correctness of the *weak* GKE requires that the participants agree on an approximately the same element rather than an exactly the same element. The definition of a *weak* GKE is identical to the definition GKE(Definition 2.1), and thus we omit the formal definition here. We define the correctness of a *weak* GKE protocol as follows.

Definition 4.1 (Correctness.) *For a real $\gamma > 0$, we say a* weak-GKE *is correct respect to γ[3] if the probability*

$$\mathsf{Pr}\left[\bigwedge_{i,j\in[N]} \|K_i - K_j\| \leq \gamma \middle| \begin{array}{c} \mathsf{pp} \leftarrow w\mathsf{GKE.Setup}(1^\lambda, 1^N) \\ \{\mathsf{trans}_i, \mathsf{st}_i\}_{i\in[N]} \leftarrow w\mathsf{Interact}(P_i, \mathsf{pp})_{i\in[N]} \\ \{K_i\}_{i\in[N]} := \underset{i\in[N]}{w\mathsf{KeyGen}}(\mathsf{pp}, P_i, \{\mathsf{trans}_i, \mathsf{st}_i\}) \end{array}\right]$$

is negligible, where the probability is taken over the randomness of weak-KeyGen *algorithm and randomness of* weak-Interact *algorithm.*

The above correctness definition of a *weak*-GKE shows that all the agreed keys from a *weak*-GKE protocol should be near each other instead of requiring them to be equal. Intuitively, this relaxed version seems to be easily reached, and we will show an explicit instantiation in next section.

security Here we define the security of *weak* GKE which is slightly different from the security definition of GKE. Recall the security definition of a GKE protocol, all the keys should be exactly equal, and thus there is no difference either of the following two cases: (1) the adversary is only given a single key, or (2) the adversary has all the keys. But in the case of *weak* GKE, the approximate-equality is needed, and thus above two cases are different. Here, the adversary is asked to distinguish the derived keys of a *weak* GKE from the same number of random dense keys.

For a probabilistic polynomial time(PPT) algorithm $\mathcal{A}$ and the key space $\mathcal{K}$ of a $w\mathsf{GKE}$, we define the advantage of $\mathcal{A}$ against the protocol $w\mathsf{GKE}$, denoted $\mathsf{Adv}_{\mathcal{A}}^{w\mathsf{GKE}}$, as follow:

$$\mathsf{Pr}\left[b' = b \middle| \begin{array}{l} \mathsf{pp} \leftarrow w\mathsf{GKE.Setup}(1^\lambda, 1^N) \\ \{\mathsf{trans}_i, \mathsf{st}_i\}_{i\in[N]} \leftarrow w\mathsf{GKE.Interact}(P_i, \mathsf{pp})_{i\in[N]} \\ \{K_i\}_{i\in[N]} := \underset{i\in[N]}{w\mathsf{GKE.KeyGen}}(\mathsf{pp}, P_i, \{w\mathsf{trans}_i, \mathsf{st}_i\}) \\ b \xleftarrow{\$} \{0,1\},\ \text{if } b = 1, K_i^* := K_i \text{ for all } i \in [N], \\ \quad \text{else } K_0^* :\xleftarrow{\$} \mathcal{K}, \{K_i^*\}_{i\in 1,\ldots,N-1} := K_0^* + \chi_{\gamma/2}, \\ b' \leftarrow \mathcal{A}(\{\mathsf{trans}_i\}_{i\in[N]}, \mathsf{pp}, \{K_i^*\}_{i\in[N]}) \end{array}\right] - \frac{1}{2},$$

where $\chi_{\gamma/2}$ is a distribution bounded by $\gamma/2$, the probability is taken over the randomness of $w\mathsf{GKE.KeyGen}$, $w\mathsf{GKE.Interact}$, χ and random coin toss of b. Our security definition of a *weak* GKE is as follows.

[3] We use the notion *correct respect to* γ rather than γ-correct due to the fact that the latter usually used to imply the correctness not holds with probability γ.

Definition 4.2 *We call a protocol* $w\mathsf{GKE}$ *is passively secure if the advantage of any* PPT *algorithm* $\mathcal{A}$*(eavesdropper) against the protocol* $w\mathsf{GKE}$ *is negligible in the security parameter* λ*, i.e.,* $\mathsf{Adv}_{\mathcal{A}}^{w\mathsf{GKE}}(\lambda) \leq \mathsf{negl}(\lambda)$.

Note that a GKE protocol is obviously a weak GKE. We instantiate this weaker version of GKE in the following section.

4.2 Instantiation of Weak GKE

In this section, instead of presenting a concrete instantiation of $w\mathsf{GKE}$, we give a high level description of its existence. In particular, we construct a $w\mathsf{GKE}$ using a similar way as in [5, 18].

Construction 4.3 *The construction of* $w\mathsf{GKE}$ *is consist of three algorithm triples* $(w\mathsf{GKE.Setup}, w\mathsf{GKE.Interact}, w\mathsf{GKE.KeyGen})$ *as follows:*
$w\mathsf{GKE.Setup}(\lambda)$ *: On input the security parameter* λ *and number of participants* N*, it first choose a random ring element* a*, a PRF, and an obfuscated circuit* C*(described in Construction 4.4),*
$w\mathsf{GKE.Interact}(\mathsf{pp}, P_i)_{i\in[N]}$*: On input public parameter* pp*, party* P_i *choose a pair* $(s_i, e_i) \xleftarrow{\chi} R$*, and comput* $b_i = a \cdot s_i + e_i$*, then broadcast* b_i*.*
$w\mathsf{GKE.KeyGen}(\mathsf{pp}, P_i, \{b_i,\}_{i\in[N]}, (s_i, e_i))_{i\in[N]}$*: Party* P_i *evaluate the obfuscated circuit* C *on input* $\{b_j, s_j, e_j\}_{j\in[N]}$*, and let the sum of a random bounded value and the evaluation of* C *as it's session key.*

Construction 4.4 *Input : a,* $(b_i, s_i, e_i)_{i\in[N]}$*, PRF:*
For i *=0 to* n *:*
if $b_i = a \cdot s_i + e_i$*, output* $PRF(b_1, \cdots, b_N)$.
Otherwise output $\perp$.

Hardness result of RLWE shows that b_i only leaks negligible information about the pair (s_i, e_i). Since the ith party has exact values of (s_i, e_i), $\{b_j\}_{j\in[N]}$, and incorrect values of s_j, e_j's for $j \neq i$, the statement $b_k = a \cdot s_k + e_k$ holds for $k = i$, and thus it will correctly have the value $PRF(b_1, \cdots, b_N)$. But those who hasn't any exact pair of (s_i, e_i) unable to have $PRF(b_1, \cdots, b_N)$.

5 Group Key Exchange Protocol from Ring LWE

In this section, we firstly construct a GKE protocol from a weak GKE and key reconciliation mechanism. Then, we will show its correctness and security. After all, we will instantiate the GKE protocol.

5.1 construction

In this section, we present the construction of group key exchange scheme $\mathsf{GKE} = (\mathsf{GKE.Setup}, \mathsf{GKE.Interact}, \mathsf{GKE.KeyGen})$ from a combination of weak group key exchange scheme $w\mathsf{GKE} = (w\mathsf{GKE.Setup}, w\mathsf{GKE.Interact}, w\mathsf{GKE.KeyGen})$ and a multi-party key reconciliation mechanism $\mathsf{KeyRek} = (\mathsf{KeyRek.Hint}, \mathsf{KeyRek.KeyGen})$. let λ be the security parameter and N be the number of participants, the construction if GKE is as follows.

Construction 5.1 *The description of* GKE *as follows:*

$\mathsf{GKE.Setup}(1^\lambda, N) \to \mathsf{pp}$**:** *On input the security parameter* λ *and number of participants* N*, it obtains* pp *by running* $w\mathsf{GKE.Setup}(1^\lambda, N)$*.*

$\mathsf{GKE.Interact}(\mathsf{pp}, P_i)_{i\in[N]} \to \{\mathsf{trans}_i, h_i, \mathsf{st}_i\}_{i\in[N]}$**:** *On input the public parameter* pp*, each party* P_i *do the followings :*

1. $(\mathsf{trans}_i, \mathsf{st}_i) \leftarrow w\mathsf{GKE.Interact}(\mathsf{pp}, P_i)$*, and brodcast* trans_i
2. $(K_i) \leftarrow w\mathsf{GKE.KeyGen}(\mathsf{trans}_i, \mathsf{st}_i, P_i)$
3. $(h_i) \leftarrow \mathsf{KeyRek.Hint}(K_i)$*, and brodcast it.*

$\mathsf{GKE.KeyGen}(\mathsf{pp}, (\mathsf{trans}_i, h_i, \mathsf{st}_i)_{i\in[N]}) = \{k_i\}_{i\in[N]}$**:** *On inputs* $\mathsf{pp}, (\mathsf{trans}_i, h_i, \mathsf{st}_i)_{i\in[N]}$ *generated from previous algorithms, it first generate* K_i *by running the algorithm* $w\mathsf{GKE.KeyGen}(\mathsf{trans}_i, \mathsf{st}_i, P_i)$*. Then it runs* $\mathsf{KeyRek.KeyGen}(K_i, \{h_i\}_{i\in[N]})$ *to get* k_i*.*

Correctness. Following theorem shows the correctness of above GKE.

Theorem 5.2 *The GKE protocol* GKE *presented in Construction5.1 is correct if the* $w\mathsf{GKE}$ *and* KeyRek *are correct respect to* γ*.*

Proof. From the correctness definition of GKE, we have following by union bound

$$\begin{aligned}\mathsf{Pr}\left[\bigwedge_{i,j\in[N]} k_i = k_j\right] &= 1 - \mathsf{Pr}\left[\bigwedge_{i,j\in[N]} k_i \neq k_j\right] \\ &\leq 1 - N^2 \max_{i,j\in[N]} \mathsf{Pr}\left[k_i \neq k_j\right].\end{aligned}$$

Hence, for any $i, j \in [N]$, showing $\mathsf{Pr}[k_i \neq k_j] \leq \mathsf{negl}(\lambda)$ is suffice to show the theorem. To show this, we rewrite the probability $\mathsf{Pr}[k_i \neq k_j]$ as

$$\begin{aligned}&\mathsf{Pr}[k_i \neq k_j \wedge \|K_i - K_j\| \leq \gamma] + \mathsf{Pr}[k_i \neq k_j \wedge \|K_i - K_j\| > \gamma] \\ &\quad\leq \mathsf{Pr}[k_i \neq k_j | \|K_i - K_j\| \leq \gamma] + \mathsf{Pr}[\|K_i - K_j\| > \gamma]\end{aligned}$$

Since $w\mathsf{GKE}$ is correct respect to γ, thus $\|K_i - K_j\| \leq \gamma$ holds except with $\mathsf{negl}(\lambda)$ probability. In addition, the conditional probability of $k_i = k_j$ on $\|K_i - K_j\| \leq \gamma$ is at least $1 - \mathsf{negl}(\lambda)$ by the correctness of KeyRek. Therefore we have $\mathsf{Pr}[k_i \neq k_j] \leq \mathsf{negl}(\lambda)$. This completes the proof

□

5.2 Security and Instantioation

Let $\chi_{\gamma/2}$ be some bounded distribution, the following theorem shows the security of the GKE in Construction 5.1.

Theorem 5.3 *The GKE protocol* GKE *presented in Construction5.1 is(passively) secure assuming the(passive) security of* KeyRek *and security of* $w\mathsf{GKE}$ *respect to* $\chi_{\gamma/2}$.

Proof. We prove the theorem by contradiction. We start by assuming the theorem is false, that is there exists an adversary $\mathcal{A}$ which can break the protocol GKE, then we will show that at least one of the following two statements holds: (1) There is a simulator $\mathsf{Sim1}$ which breaks the security of $w\mathsf{GKE}$. (2) There is a simulator $\mathsf{Sim2}$ which breaks the security of KeyRek. This contradict with the theorem assumption that $w\mathsf{GKE}$ and KeyRek are secure, and thus the theorem holds.

To show the existence of an adversary $\mathcal{A}$ which can break the protocol GKE implies one of the above two statements is true, we need following sequence of games.

Game_0 This is the ordinary GKE security game between the $\mathcal{A}$ and the challenger.

Game_1 In this game, we modify the game so that challenger chooses K_0 from uniform distribution instead of generating it by running $w\mathsf{GKE.KeyGen}$, and then let $K_i = K_0 + \chi_\gamma$. Here we also require χ be some distribution bounded by $\gamma/2$ except with negligible probability.

Game_2 In this game, we change the way that the challenger compute the challenge key k^*. Here the challenge key k^* is chosen randomly instead of generating it by using $\mathsf{KeyRek.KeyGen}$.

In what follows, we show the advantage of $\mathcal{A}$ in the Game_0, denoted $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_0}$, is upper bounded by the advantage of corresponding algorithms($\mathsf{Adv}_{\mathsf{Sim1}}^{w\mathsf{GKE}}$ and $\mathsf{Adv}_{\mathsf{Sim2}}^{\mathsf{KeyRek}}$) plus a negligible function in security parameter λ. By our assumption, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_0}$ is noticeable, therefore $\mathsf{Adv}_{\mathsf{Sim1}}^{w\mathsf{GKE}}$ or $\mathsf{Adv}_{\mathsf{Sim2}}^{\mathsf{KeyRek}}$ is non-negligible, and this is what we want to prove. Now, we show it by following lemmas.

Lemma 5.4 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_0} \leq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_1} + \mathsf{Adv}_{\mathsf{Sim1}}^{w\mathsf{GKE}}$.

Proof. The algorithm $\mathsf{Sim1}$ works as follows:

At the beginning of the game, algorithm $\mathsf{Sim1}$ is given $(\mathsf{pp}, \{\mathsf{trans}_i, K_i^*\}_{i\in[N]})$ from its challenger, where pp is the public parameter of $w\mathsf{GKE}$, trans_is are the transactions and K_i^*s are derived keys of the $w\mathsf{GKE}$ if the challenger's coin toss $b = 1$, and $K_0^* \xleftarrow{\$} \mathcal{K}, \{K_i^*\}_{i\in 1,\ldots,N-1} := K_0^* + \chi_{\gamma/2}$ otherwise. Then, $\mathsf{Sim1}$ computes $h_i := \mathsf{KeyRek.Hint}(K_i^*)$ for all $i \in [N]$, $k^* := \mathsf{KeyRek.KeyGen}(K_0, \{h_i\}_{i\in[N]})$, and send $(\mathsf{pp}, \{\mathsf{trans}_i, h_i\}_{i\in[N]}, k^*)$ to the adversary $\mathcal{A}$. At the end of the game, after receiving the $\mathcal{A}$'s guessing bit $b' \in \{0, 1\}$, $\mathsf{Sim1}$ outputs b' as its guess of b.

If the challenger's coin toss $b = 1$, then $\mathsf{Sim1}$ perfectly simulate the view of $\mathcal{A}$ as in Game_0. Otherwise, $\mathsf{Sim1}$ simulates the view of $\mathcal{A}$ as in Game_1. Therefore, the lemma follows.

□

Lemma 5.5 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_1} \leq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_2} + \mathsf{Adv}_{\mathsf{Sim}}^{\mathsf{KeyRek}}$.

Proof. The algorithm $\mathsf{Sim2}$ runs as follows:

At the beginning of the game, algorithm $\mathsf{Sim2}$ is given $(\{h_i\}_{i\in[N]}, K^*)$ from its challenger, where $h_i = \mathsf{KeyRek.KeyGen}(U_i)$ for uniformly distributed U_is such that $\|U_i - U_j\| \leq \gamma, \forall i, j \in [N]$. The key K^* is generated by the algorithm $\mathsf{KeyRek.KeyGen}(U_0, \{h_i\}_{i\in[N]})$ if the challenger's coin toss $b = 1$ and generated by randomly if $b = 0$. Then, $\mathsf{Sim2}$ obtain $(\mathsf{pp}, \{\mathsf{trans}_i\}_{i\in[N]})$ by running $w\mathsf{GKE.Setup}$ and $w\mathsf{GKE.Interact}$. Next, $\mathsf{Sim2}$ let $k^* := K^*$ and sends $(\mathsf{pp}, \{\mathsf{trans}_i, h_i\}_{i\in[N]}, k^*)$ to the adversary $\mathcal{A}$. At the end of the game, after receiving the $\mathcal{A}$'s guessing bit $b' \in \{0, 1\}$, $\mathsf{Sim2}$ outputs b' as its guess of b.

If the challenger's coin toss $b = 1$, then $\mathsf{Sim2}$ perfectly simulate the view of $\mathcal{A}$ as in Game_1. Otherwise, $\mathsf{Sim2}$ simulates the view of $\mathcal{A}$ as in Game_2. Therefore, the lemma follows. □

Complete the proof. Since the key k^* in Game_2 is uniformly selected, then the adversary's advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_2}$ is zero. Furthermore, combining the above lemmas, we have

$$\begin{aligned}\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_0} &\leq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_1} + \mathsf{Adv}_{\mathsf{Sim1}}^{w\mathsf{GKE}} \\ &\leq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_2} + \mathsf{Adv}_{\mathsf{Sim2}}^{\mathsf{KeyRek}} + \mathsf{Adv}_{\mathsf{Sim1}}^{w\mathsf{GKE}} \\ &\leq \mathsf{Adv}_{\mathsf{Sim2}}^{\mathsf{KeyRek}} + \mathsf{Adv}_{\mathsf{Sim1}}^{w\mathsf{GKE}}.\end{aligned}$$

Since $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Game}_0}$ is noticeable, at least on of $\mathsf{Adv}_{\mathsf{Sim1}}^{\mathsf{KeyRek}}$ and $\mathsf{Adv}_{\mathsf{Sim2}}^{w\mathsf{GKE}}$ is noticiable. This completes the proof.

□

Instantiation. Concrete Instantiation of GKE straightly obtained by combining the instantiations of multi-party KeyRek and $w\mathsf{GKE}$ from the previous sections. Therefore, we omit the concrete description here.

References

1. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - A new hope. In T. Holz and S. Savage, editors, *USENIX Security 2016*, pages 327–343. USENIX Association, Aug. 2016.

2. D. Apon, D. Dachman-Soled, H. Gong, and J. Katz. Constant-round group key exchange from the ring-LWE assumption. In J. Ding and R. Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019*, pages 189–205. Springer, Heidelberg, 2019.
3. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In D. E. Denning, R. Pyle, R. Ganesan, R. S. Sandhu, and V. Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, Nov. 1993.
4. M. Bellare and P. Rogaway. Provably secure session key distribution: The three party case. In *27th ACM STOC*, pages 57–66. ACM Press, May / June 1995.
5. D. Boneh and M. Zhandry. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. *Algorithmica*, 79(4):1233–1285, 2017.
6. J. W. Bos, C. Costello, M. Naehrig, and D. Stebila. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In *2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015*, pages 553–570. IEEE Computer Society, 2015.
7. Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. Classical hardness of learning with errors. In D. Boneh, T. Roughgarden, and J. Feigenbaum, editors, *45th ACM STOC*, pages 575–584. ACM Press, June 2013.
8. E. Bresson and D. Catalano. Constant round authenticated group key agreement via distributed computation. In F. Bao, R. Deng, and J. Zhou, editors, *PKC 2004*, volume 2947 of *LNCS*, pages 115–129. Springer, Heidelberg, Mar. 2004.
9. E. Bresson, O. Chevassut, and D. Pointcheval. Provably authenticated group Diffie-Hellman key exchange – the dynamic case. In C. Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 290–309. Springer, Heidelberg, Dec. 2001.
10. E. Bresson, O. Chevassut, and D. Pointcheval. Dynamic group Diffie-Hellman key exchange under standard assumptions. In L. R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 321–336. Springer, Heidelberg, Apr. / May 2002.
11. E. Bresson, O. Chevassut, D. Pointcheval, and J. Quisquater. Provably authenticated group diffie-hellman key exchange. In M. K. Reiter and P. Samarati, editors, *CCS 2001, Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, USA, November 6-8, 2001*, pages 255–264. ACM, 2001.
12. R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited (preliminary version). In *30th ACM STOC*, pages 209–218. ACM Press, May 1998.
13. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6):644–654, 1976.
14. J. Ding. New cryptographic constructions using generalized learning with errors problem. Cryptology ePrint Archive, Report 2012/387, 2012. `http://eprint.iacr.org/2012/387`.
15. L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. Lattice signatures and bimodal Gaussians. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 40–56. Springer, Heidelberg, Aug. 2013.
16. L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(1):238–268, 2018.
17. L. Ducas and D. Micciancio. Improved short lattice signatures in the standard model. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 335–352. Springer, Heidelberg, Aug. 2014.
18. S. Guo, P. Kamath, A. Rosen, and K. Sotiraki. Limits on the efficiency of (ring) LWE based non-interactive key exchange. In A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 374–395. Springer, Heidelberg, May 2020.
19. Z. Jin and Y. Zhao. Optimal key consensus in presence of noise. Cryptology ePrint Archive, Report 2017/1058, 2017. `http://eprint.iacr.org/2017/1058`.
20. S. Katsumata and S. Yamada. Partitioning via non-linear polynomial functions: More compact IBEs from ideal lattices and bilinear maps. In J. H. Cheon and T. Takagi, editors,

ASIACRYPT 2016, Part II, volume 10032 of *LNCS*, pages 682–712. Springer, Heidelberg, Dec. 2016.
21. J. Katz and M. Yung. Scalable protocols for authenticated group key exchange. *Journal of Cryptology*, 20(1):85–113, Jan. 2007.
22. H. Krawczyk. HMQV: A high-performance secure Diffie-Hellman protocol. In V. Shoup, editor, *CRYPTO 2005*, volume 3621 of *LNCS*, pages 546–566. Springer, Heidelberg, Aug. 2005.
23. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Heidelberg, May / June 2010.
24. A. Menezes, M. Qu, and S. Vanstone. Some key agreement protocols providing implicit authentication. 01 1995.
25. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In M. Mitzenmacher, editor, *41st ACM STOC*, pages 333–342. ACM Press, May / June 2009.
26. C. Peikert. Lattice cryptography for the internet. In M. Mosca, editor, *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014*, pages 197–219. Springer, Heidelberg, Oct. 2014.
27. C. Peikert, O. Regev, and N. Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. In H. Hatami, P. McKenzie, and V. King, editors, *49th ACM STOC*, pages 461–473. ACM Press, June 2017.
28. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In H. N. Gabow and R. Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.
29. P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, Nov. 1994.
30. J. Zhang, Z. Zhang, J. Ding, M. Snook, and Ö. Dagdelen. Authenticated key exchange from ideal lattices. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 719–751. Springer, Heidelberg, Apr. 2015.

THE 5 DIMENSIONS OF PROBLEM SOLVING USING DINNA DIAGRAM: DOUBLE ISHIKAWA AND NAZE NAZE ANALYSIS

Mohammed Hamoumi[1], Abdellah Haddout[2] and Mariam Benhadou[2]

[1]PHD Student, Laboratory of Industrial Management, Energy and Technology of Plastic and Composites Materials
Hassan II University – ENSEM Casablanca, Morocco
[2]Professor, Laboratory of Industrial Management, Energy and Technology of Plastic and Composites Materials
Hassan II University – ENSEM Casablanca, Morocco

ABSTRACT

Based on the principle that perfection is a divine criterion, process management exists on the one hand to achieve excellence (near perfection) and on the other hand to avoid imperfection. In other words, Operational Excellence (EO) is one of the approaches, when used rigorously, aims to maximize performance. Therefore, the mastery of problem solving remains necessary to achieve such performance level.

There are many tools that we can use whether in continuous improvement for the resolution of chronic problems (KAIZEN, DMAIC, Lean six sigma…) or in resolution of sporadic defects (8D, PDCA, QRQC ...). However, these methodologies often use the same basic tools (Ishikawa diagram, 5 why, tree of causes…) to identify potential causes and root causes. This results in three levels of causes: occurrence, no detection and system.

The research presents the development of DINNA diagram [1] as an effective and efficient process that links the Ishikawa diagram and the 5 why method to identify the root causes and avoid recurrence. The ultimate objective is to achieve the same result if two working groups with similar skills analyse the same problem separately, to achieve this, the consistent application of a robust methodology is required. Therefore, we are talking about 5 dimensions; occurrence, non-detection, system, effectiveness and efficiency.

As such, the paper offers a solution that is both effective and efficient to help practitioners of industrial problem solving avoid missing the real root cause and save costs following a wrong decision.

KEYWORDS

Operational Excellence, DINNA Diagram, Double Ishikawa and Naze Naze Analysis, Ishikawa, 5 Way analysis, Morocco.

1. INTRODUCTION

Previous research has identified methodologies using a set of methods that we can use to improve the results of each of the phases that continuous improvement projects must go through [2]. As

David C. Wyld et al. (Eds): CMC, NCO, SOFT, CDKP, MLT, ICAITA - 2021
pp. 175-183, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111114

problems become more complex, more structured tools are needed to support these steps, from characterizing the problem to put in place an action plan. These tools use divergent techniques, which help generate multiple alternatives, and convergent techniques that help analyze and filter the generated options [3] [4]. Some of the most cited methodologies are 8D [5] [6] [7] [8], PDCA[9] [10] [11] [12] [13] [14] [15] [16], DMAIC [17] [18] [19] [20] [21] [22] [11] and KAIZEN [23] [24] [25] [26] [27] [28]. However, Ishikawa [29] and 5 Way analysis [30] remain the most basic tools used in all those methodologies.

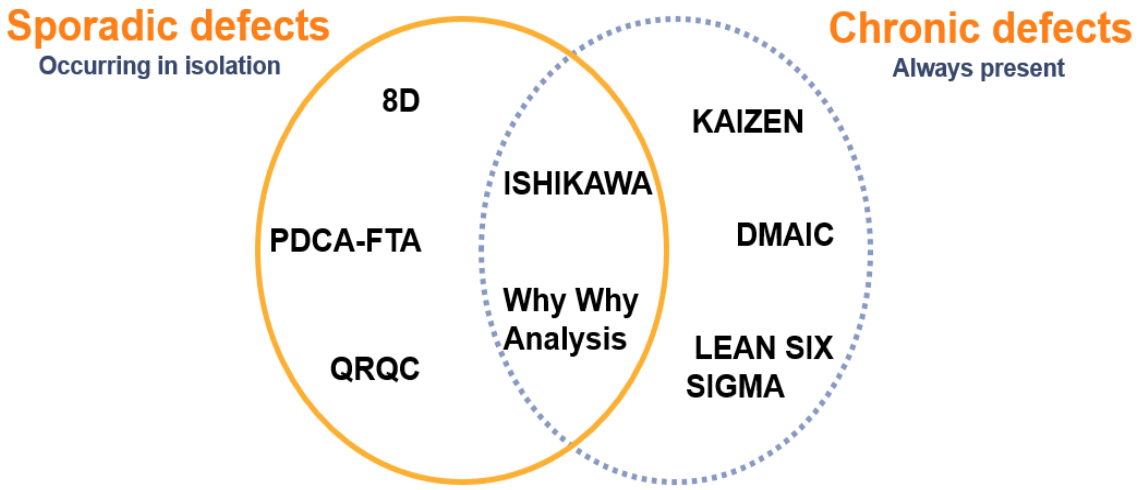


Figure 1. Common tools to all problem-solving methodologies

2. MOTIVATION & PHILOSOPHY

2.1. Motivation

The research is the result of several years of 8D methodology practitioner (more than 1200 reports over 15 years) on semiconductor, wiring systems and automotive industries. I hope that will be helpful and by the way, one cogitates (think deeply) item to develop in the future. I present the 5 dimensions experimental design of problem solving using DINNA Diagram : Double Ishikawa and Naze Naze Analysis, discussing the novel approach we have taken to defect and root cause classification and the mechanisms we have used to connect between the different diagrams. We then present the results of our analyses and describe the best way to get it. We conclude with lessons learned from the methodology and resulting ongoing improvement activities.

2.2. Philosophy

If we assume that we have two teamwork groups with similar skills both looking for the root cause of the same problem separately, how can we be sure that the two groups will achieve the desired result using the same methodology?

3. DINNA DIAGRAM

3.1. Double Ishikawa diagram

The Ishikawa diagram [29] is one of Seven Basic Tools of Quality, (also called fishbone diagrams, herringbone diagrams, cause-and-effect diagrams, or Fishikawa) are causal diagrams created by Kaoru Ishikawa (1968) that show the causes of a specific event. This diagram illustrates the cause and effect diagram or 5ME (Material, Man, Machine, Method, Measure and Environment). For each branch all potential causes are described. Indeed, the purpose is to break down (in successive layers of detail) causes that potentially contribute to a particular effect.

Mostly if not always, we treat only the occurrence (why it happened) and we forget the non-detection (why it wasn't detected) root causes. That's why, double Ishikawa diagram is very important to complete the analysis. And, we keep the "Man" for the last, to not be influenced.

I chose the double Ishikawa form like "Figure. 2" to facilitate the connection with the why why analysis.

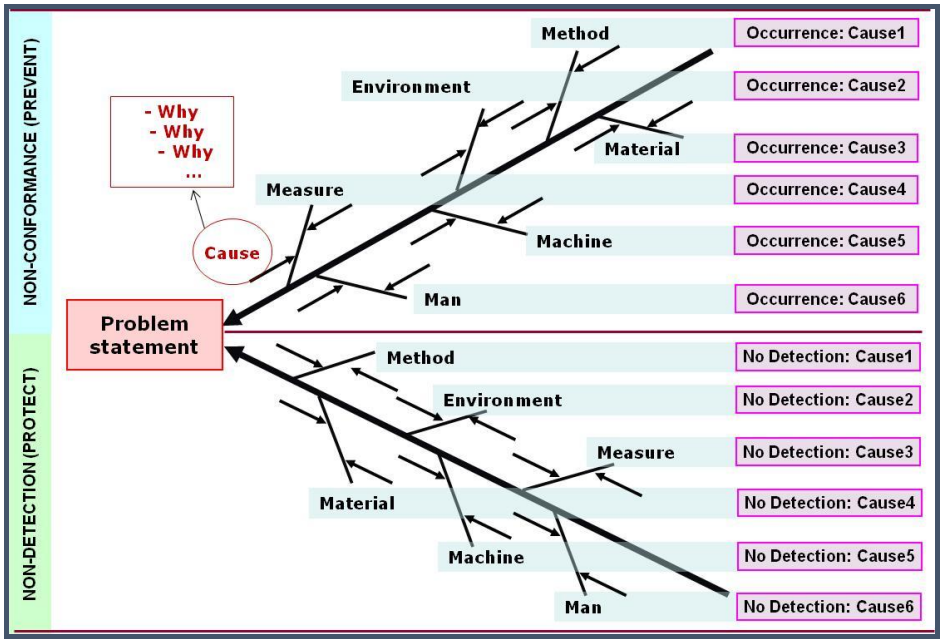


Figure 2. Double Ishikawa Diagram

There are two ways to verify the causes, by reproducing the defect or by team voting.

***By reproducing the defect*:** We try to reproduce the defect based on hypotheses given by team members, but this method is limited by time allocate to the analysis and also if there is combination of several causes.

***By team voting*:** Sometimes it is very difficult to verify the causes by reproducing the defect. In this case, the team formulates hypotheses that can be objectively tested. The approach is that each team member gives a causes weight (3P, 2P, 1P) based on their feedback and expertise, and in the end we sum the points which giving a final number as shown in the example below "Figure. 3".

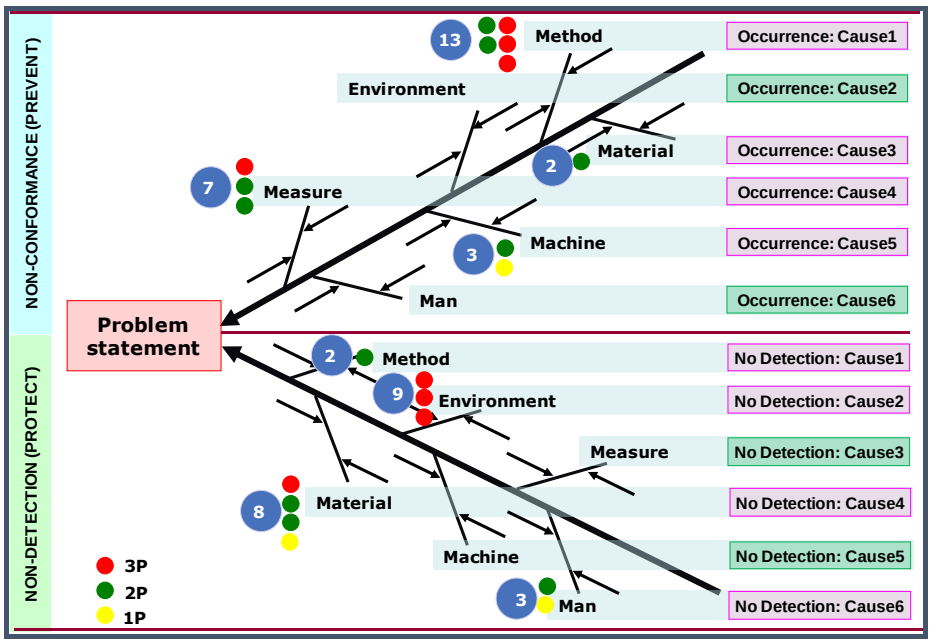


Figure 3. Double Ishikawa and the vote

3.2. Naze Naze Analysis

5 Why's are widely used to find the real root cause, invented by Taiichi Ohno [30] which was the great quality guru working for Toyota, 5 Why's are also called Naze Naze in Japanese (Naze=Why). The principal is to ask several times the question Why until you hit the real root cause.

And for sure, the question Why can be asked less or more than 5 times. Also, make sure the root cause is connected to the initial problem with a logical link.

Which is the Reel Root Cause?

• The reel root cause must be well described: need to be accurate, measurable, specific and without interpretation.
• The reel root cause is the one identified that satisfies the requirement of completely explaining the effect. It is the single verified reason that accounts for the problem.
• The reel root cause is supported by the facts without contradiction.
• The reel root cause is the one whose removal should make the effect stop permanently.
The Double Ishikawa (or the list of initial causes) is the starting point. That could be the problem itself but that will be less accurate.

Methodology:

Step 1: select one initial cause from the Double Ishikawa. For each branch all potential causes are described: Advantage of this in description of a problem: you will not forget anything.

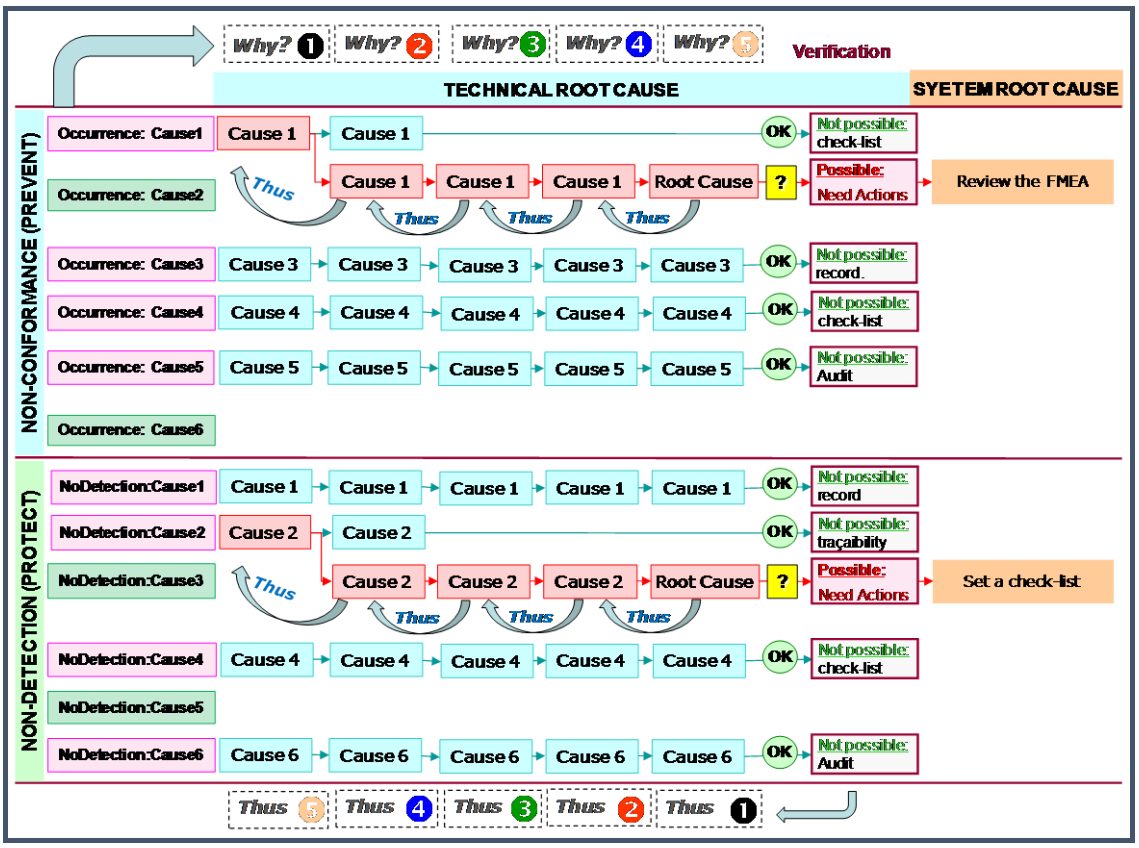


Figure 4. Naze Naze Analysis

Step 2: repeat "why" until the answer can trigger a countermeasure. It's important to note that the "5 Whys" technique can break into multiple chains when a particular "why?" has multiple answers. This is the time to apply the Pareto method and determine which pathway has the greatest effect in causing the performance gap. When choosing between two courses of action, it's better to address the causes with an 80% impact on the problem first, before dealing with causes that have a lesser impact. See below (Occurrence: cause 1, in the first why, we get two causes, one was verified as not possible the second one, guide us to the reel root cause).

Step 3: Ask « thus » at every cause to verify the root cause. In fact, to verify that the analysis is correct, you should be able to propose a countermeasure to the root cause and apply the word "thus" or "therefore" to verify that the countermeasure addresses each cause in the chain. This is what we call the "reversible" aspect of the 5 Why's to verify the reel root cause.

Good example:

"I was late" ➔ why ➔ because "my car did not start"
Do you mean "your car did not start so you were late"? Yes! so the cause is confirmed.

Bad example:

"I was late" ➔ why ➔ because "I had a party yesterday evening"
Do you mean "you had a party yesterday, so you were late"?
Cannot be Yes because you may have a party and be just in time. Being late is due to something else ➔ this cause is not confirmed.

3.3. Three dimensions of Naze Naze Analysis

The Naze Naze Analysis splits into 3 dimensions:

1) The Occurrence (non-conformity)

Why do we have the problem?

2) The Escape (non-detection)

Why did we not detect the problem?

3) The System (preventive & predictive)

Why did the system allow this problem to happen?
Why did the system allow this problem to not be detected?

3.4. Double Ishikawa and Naze Naze Analysis Diagram

DINNA Diagram is a powerful problem-solving methodology which is an iterative effort that requires strong leadership, good teamwork, and relentless follow-through. If it were easy, you wouldn't need to spend time diving deep to understand the real root causes and solutions. You'd simply solve the problem.

In lean manufacturing, real root cause countermeasure tools are often used to help perform the necessary discovery and analysis, and to provide the insight needed to develop an effective and permanent solution. This approach is exactly what we found when we use DINNA Diagram, it will help you to gain time, to effectively determine the real root cause(s), and to avoid the recurrence.

The DINNA Diagram is complete resolving problem methodology if it is used correctly, we should not stop until ALL real root causes have been identified: Occurrence and Escape, Technical and System.

Remind that when the real root cause is identified is provides an opportunity to prevent it happening again thus reducing the possible recurrence, increasing customer satisfaction, etc…Finally, customers often require a 5 Why's from their supplier because they think that it is a key tool to find the real root cause and then to prevent recurrence. That's why; DINNA Diagram is well designed to force us to go down to the real root causes using fact-based links between the cause and the effect.

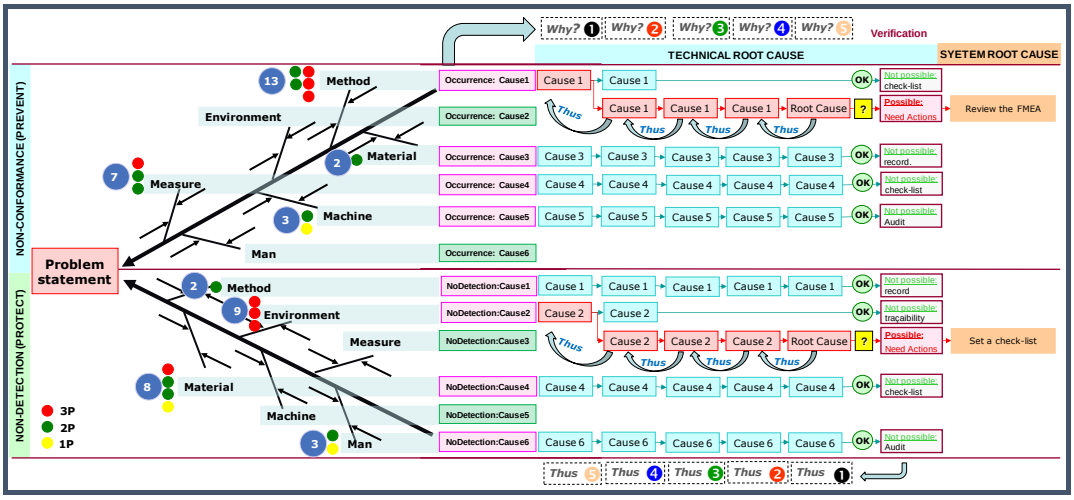


Figure 5. Double Ishikawa and Naze Naze Analysis Diagram

3.5. The 5 dimensions of problem-solving using DINNA Diagram:

The robustness of any problem-solving tool cannot be achieved if it does not address the effectiveness and efficiency dimensions. Using the Dinna diagram rigorously, we identify the true root cause or the combination of several root causes. At this stage, an action plan is required, and the choice of appropriate actions is made based on a decision matrix which should consider the cost criterion alongside the quality and the deadline. Therefore, the efficiency remains mandatory for Operational Excellence mindset and this is the 4th dimension.

Finally, the 5th dimension is the effectiveness of the actions put in place to eradicate the problem, which can be verified by compliance audits and perfectly if no recurrence recorded.

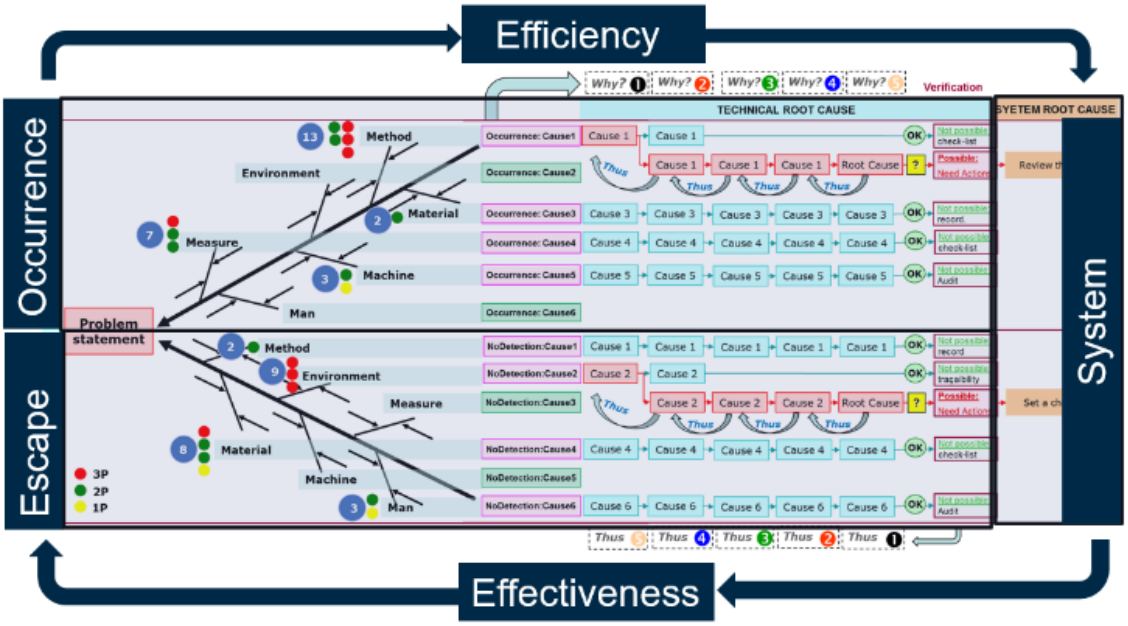


Figure 6. The 5 dimensions of problem-solving using DINNA Diagram

4. CONCLUSIONS

DINNA diagram has been tested for different problems in three sectors of the automotive industry: Semiconductor (80% machine Vs. 20% Human), Automotive suppliers (20% machine Vs. 80% Human), and Car Maker (50% machine Vs. 50% Human). We will publish practical cases in the future using the 5 dimensions of problem solving with DINNA diagram.

REFERENCES

[1] Hamoumi, M. (2017) Made in Morocco: DINNA Diagram (Double Ishikawa and Naze Naze Analysis). Proceedings of the International Conference on Industrial Engineering and Operations Management, 2017, :2180-2185 Language: English. IEOM Society.

[2] Tschimmel, K. (2012). Design thinking as an effective toolkit for innovation. Paper presented at the Proceedings of the XXIII ISPIM Conference: Action for Innovation: Innovating from Experience, Barcelona.

[3] Clune, S. J., & Lockrey, S. (2014). Developing environmental sustainability strategies, the double diamond method of lca and design thinking: A case study from aged care. Journal of Cleaner Production, 85, 67-82. doi:https://doi.org/10.1016/j.jclepro.2014.02.003

[4] Smalley, A. (2018). Four types of problem solving. Cambridge: Lean Enterpdise Institute.

[5] Al-Mashari, M., Zairi, M., & Ginn, D. (2005). Key enablers for the effective implementation of qfd: A critical analysis. Industrial Management & Data Systems, 105(9), 1245-1260. doi:10.1108/02635570510633284

[6] Camarillo, A., Rios, J., & Althoff, K. D. (2018). Knowledge-based multi-agent system for manufacturing problem solving process in production plants. Journal of Manufacturing Systems, 47, 115-127. doi:10.1016/j.jmsy.2018.04.002

[7] Gangidi, P. (2019). A systematic approach to root cause analysis using 3 x 5 why's technique. International Journal of Lean Six Sigma, 10(1), 295-310. doi:10.1108/ijlss-10-2017-0114

[8] Realyvasquez-Vargas, A., Arredondo-Soto, K. C., Garcia-Alcaraz, J. L., & Macias, E. J. (2020). Improving a manufacturing process using the 8ds method. A case study in a manufacturing company. Applied Sciences-Basel, 10(7). doi:10.3390/app10072433

[9] Alsyouf, I., Al-Aomar, R., Al-Hamed, H., & Qiu, X. J. (2011). A framework for assessing the cost effectiveness of lean tools. European Journal of Industrial Engineering, 5(2), 170-197.

[10] Matsuo, M., & Nakahara, J. (2013). The effects of the pdca cycle and ojt on workplace learning. International Journal of Human Resource Management, 24(1), 195-207. doi:10.1080/09585192.2012.674961

[11] Nascimento, D. L. D., Quelhas, O. L. G., Caiado, R. G. G., Tortorella, G. L., Garza-Reyes, J. A., & Rocha-Lona, L. (2019). A lean six sigma framework for continuous and incremental improvement in the oil and gas sector. International Journal of Lean Six Sigma, 11(3), 577-595. doi:10.1108/ijlss-02-2019-0011

[12] Nedra, A., Nejib, S., Yassine, C., & Morched, C. (2019). A new lean six sigma hybrid method based on the combination of pdca and the dmaic to improve process performance: Application to clothing sme. Industria Textila, 70(5), 447-456. doi:10.35530/it.070.05.1595

[13] Pinto, M. J. A., & Mendes, J. V. (2017). Operational practices of lean manufacturing: Potentiating environmental improvements. Journal of Industrial Engineering and Management, 10(4 Special Issue), 550-580. doi:10.3926/jiem.2268

[14] Rafferty, B. (2009). Understanding a3 thinking: A critical component of toyota's pdca management system. Journal of Product Innovation Management, 26(2), 243-244. doi:10.1111/j.1540-5885.2009.00348_1.x

[15] Song, M. H., & Fischer, M. (2020). Daily plan-do-check-act (pdca) cycles with level of development (lod) 400 objects for foremen. Advanced Engineering Informatics, 44, 12. doi:10.1016/j.aei.2020.101091

[16] Wei, W. J., Wang, S. C., Wang, H. L., & Quan, H. J. (2020). The application of 6s and pdca management strategies in the nursing of covid-19 patients. Critical Care, 24(1), 4. doi:10.1186/s13054-020- 03124-w

[17] Anderson-Cook, C. M., Patterson, A., & Hoerl, R. (2005). A structured problem-solving course for graduate students: Exposing students to six sigma as part of their university training. Quality and Reliability Engineering International, 21(3), 249-256. doi:10.1002/qre.666
[18] de Mast, J., & Lokkerbol, J. (2012). An analysis of the six sigma dmaic method from the perspective of problem solving. International Journal of Production Economics, 139(2), 604-614. doi:10.1016/j.ijpe.2012.05.035
[19] Easton, G. S., & Rosenzweig, E. D. (2012). The role of experience in six sigma project success: An empirical analysis of improvement projects. Journal of Operations Management, 30(7-8), 481- 493. doi:10.1016/j.jom.2012.08.002
[20] Garza-Reyes, J. A. (2015). Green lean and the need for six sigma. International Journal of Lean Six Sigma, 6(3), 226-248. doi:10.1108/ijlss-04-2014-0010
[21] Guo, W., Jiang, P. Y., Xu, L., & Peng, G. Z. (2019). Integration of value stream mapping with dmaic for concurrent lean-kaizen: A case study on an air-conditioner assembly line. Advances in Mechanical Engineering, 11(2), 17. doi:10.1177/1687814019827115
[22] Marques, P. A. D., & Matthe, R. (2017). Six sigma dmaic project to improve the performance of an aluminum die casting operation in portugal. International Journal of Quality & Reliability Management, 34(2), 307-330. doi:10.1108/ijqrm-05-2015-0086
[23] Delavari, S., Forghani, M., & Mollahoseini, A. (2009). Operational Kaizen in a manufacturing company.
[24] Singh, H., Gupta, N.K. (2010) Kaizen Improvement in a Process Organization. Lambert Academic Publishing.
[25] Rahmanian, F., & Rahmatinejad, Z. (2014). Impact of Kaizen implementation on performance of manufacturing companies' staff. European Online Journal of Natural and Social Sciences, 2(3s), 1094-1103.
[26] Abdulmouti, H. Benefits of Kaizen to business excellence: evidence from a case study (2018) Indus. Eng. Manage., 7 (2). https://proxy.univh2c.ma:2094/10.4172/2169-0316.1000251
[27] Kalva R. S., Kumar, A. P., & Srinivasu, V. (2018). Continuous Improvement through Kaizen in a Manufacturing Organisation. Patel, V. (2017). Review on Implementation of Kaizen Technique for Productivity Improvement in Manufacturing Organization (Vol. V).
[28] Rahmanian, F., & Rahmatinejad, Z. (2014). Impact of Kaizen implementation on performance of manufacturing companies' staff. European Online Journal of Natural and Social Sciences, 2(3s), 1094-1103.
[29] Ishikawa, K. (1984) la gestion de la qualité. Outils et applications pratiques. Paris: Dunod.
[30] Ohno T (1978) Toyota production system. Diamond-Press, Tokyo

AUTHORS

Mohammed HAMOUMI (40 years old)
2001/2005 Lille Polytechnic University Graduate Engineering School, France
2011/2013 EHTP/ENPC MBA- School of International Management Paris
7 years at STMicroelectronics as Quality Assurance and Customer Quality Support Manager
3 years at LEONI Wiring Systems as Plant Quality Manager
3 years at CIF (Plastic Industry. Leader in the manufacture of woven polypropylene (PP) bags and kraft paper bags) as Quality Director
2 years at PSA Morocco as Quality and Engineering Director
Since June 2018 Lead Auditor BUREAU VERITAS and trainer certified resolutions problems
Certified Lead Auditor IRCA ISO 9001, ISO 14001, ISO 45001, IATF 16949 V2016

AUTHOR INDEX

Abdellah HADDOUT *149*
Abdellah Haddout *175*
Armando Antonio M. Lagana *109*
Carlos Sauer Ayala *123*
Diego P. Pinto-Roa *123*
Edson C. Kitani *109*
Federico Daumas *123*
Federico Divina *123*
Federico Román *123*
Félix Morales *123*
Francisco Gómez-Vela *123*
Gabriela Robiolo *55*
Gustavo Velázquez *123*
Haluk Altay *01*
Hernán Medina *123*
Hoda Nematy *21*
José L. VázquezNoguera *123*
Leopoldo R. Yoshioka *109*
M. Furkan Solmazgül *01*
Malika Smail-Tabbone *81*
Mariam BENHADOU *149*
Mariam Benhadou *175*
Mariana Falco *55*
Md Kamrul Islam *81*
Michel Andre L .Vinagreiro *109*
Michele Staiano *73*
Miguel García-Torres *123*
Minh-Van Nguyen *101*
Mohammed Hamoumi *175*
Parhat Abla *157*
Pedro E. Gardel-Sotomayor *123*
Quoc-Huy Trinh *101*
Roberto Maranca *73*
Sabeur Aridhi *81*
Samah Mohammed S ALhusayni *35*
Vikas Thammanna Gowda *93, 139*
Wael Ali Alosaimiv *35*
Yassine MOUMEN *149*