Natarajan Meghanathan
David C. Wyld (Eds)

Computer Science & Information Technology

The Fifth International Conference on Advanced Computer Science and Information Technology (ICAIT 2016)
Sydney, Australia, May 28~29, 2016

AIRCC Publishing Corporation

Volume Editors

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

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

ISSN: 2231 - 5403
ISBN: 978-1-921987-54-0
DOI : 10.5121/csit.2016.60701 - 10.5121/csit.2016.60707

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

Preface

The Fifth International Conference on Advanced Computer Science and Information Technology (ICAIT 2016) was held in Sydney, Australia, during May 28~29, 2016. The Fifth International Conference on Cryptography and Information Security (CRYPIS 2016), The Fourth International Conference of Networks and Communications (NC 2016) and The Fifth International Conference on Information Technology Convergence and Services (ITCSE 2016) were collocated with the ICAIT-2016. 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 ICAIT-2016, CRYPIS-2016, NC-2016, ITCSE-2016 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. All these efforts undertaken by the Organizing and Technical Committees led to an exciting, rich and a high quality technical conference program, which featured high-impact presentations for all attendees to enjoy, appreciate and expand their expertise in the latest developments in computer network and communications research.

In closing, ICAIT-2016, CRYPIS-2016, NC-2016, ITCSE-2016 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 ICAIT-2016, CRYPIS-2016, NC-2016, ITCSE-2016.

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

Natarajan Meghanathan
David C. Wyld

Organization

General Chair

Jan Zizka	Mendel University in Brno, Czech Republic
Dhinaharan Nagamalai	Wireilla Net Solutions, Australia

Program Committee Members

A.K.M. Fazlul Haque	Daffodil International University, Bangladesh
Abd El-Aziz Ahmed	Cairo University, Egypt
Abdelhamid A. Mansor	University of Khartoum, Sudan
Abdelmadjid Allali	Ben Bouali University, Algeria
Abdelmounaim Abdali	Cadi Ayyad University, Morocco
Abdolreza Hatamlou	Islamic Azad University, Iran
Aftab Alam	King Khalid University, Saudi Arabia
Ahmed Hussein Aliwy	University of Kufa, Iraq
Akira Otsuki	Nihon University, Japan
Ali Abid D.Al-Zuky	Mustansiriyah University, Iraq
Ali Hussein	Alexandria University, Egypt
Andino Maseleno	STMIK Pringsewu, Indonesia
Ashraf A.Shahin	Cairo Univeristy, Egypt
Assem Abdel Hamied Moussa	E commerce Manager, Egypt
Atif Farid Mohammad	University of North Carolina, Charlotte
Ayad Ghany Ismaeel	Erbil Polytechnic University, Iraq
Ayad Salhieh	Australian College of Kuwait, Kuwait
Azween Bin Abdullah	Universiti Teknologi Petronas, Malaysia
Baghdad Atmani	University of Oran Ahmed Benbella, Algeria
Bouix Emmanuel	IKlax Media, France
Cherif Foudil	Biskra University, Algeria
Chin-Chih Chang	Chung-Hua University, Taiwan
Danda B. Rawat	Eastern Kentucky University, USA
David B. Bracewell	General Electric Global Research, USA
Dongchen Li	Peking University, China
Elashiry M.A	Beni Suef University, Egypt
Eric Renault	Telecom SudParis, France
Fatih Korkmaz	karatekin university, Turkey
Gongjun Yan	Indiana University Kokomo, USA
Grigorios N.Beligiannis	University of Patras, Greece
Hamid Reza Karimi	University of Agder, Norway
Hamza Zidoum	Sultan Qaboos University, Oman
Hao Shi	Victoria University, Australia
Hossein Jadidoleslamy	MUT University, Iran
Hou, Cheng-I	Chung Hua University, Taiwan
I.V.Narasimha	University of Houston, USA
Ioannis Karamitsos	University of Aegean, Greece

Technically Sponsored by

Networks & Communications Community (NCC)

Computer Science & Information Technology Community (CSITC)

Digital Signal & Image Processing Community (DSIPC)

Organized By

Academy & Industry Research Collaboration Center (AIRCC)

TABLE OF CONTENTS

The Fifth International Conference on Advanced Computer Science and Information Technology (ICAIT 2016)

The Fifth International Conference on Cryptography and Information Security (CRYPIS 2016)

The Fourth International Conference of Networks and Communications (NC 2016)

The Fifth International Conference on Information Technology Convergence and Services (ITCSE 2016)

"USABILITY TESTING IN MOBILE APPLICATIONS INVOLVING PEOPLE WITH DOWN SYNDROME: A LITERATURE REVIEW"

Doris Cáliz1, Loïc Martínez[1], Xavier Alamán[2], Carlos Terán[3], Richart Cáliz[3].

[1]Department ETSIINF, DLSIIS, Madrid Polytechnic University, Campus de Montegancedo 28660 , Boadilla del Monte , Madrid, Spain
doriscalizramos@outlook.com; loic@fi.upm.es;
[2]Department of Computer Engineering, Autonomous University, Madrid, C/ Francisco Tomás y Valiente, 11. 28049, Madrid, Spain.
Xavier.Alaman@uam.es
[3]Department of Computer Sciences FIS Group, National Polytechnic University, Ladrón de Guevara E11-25 y Andalucía Quito, Ecuador
carlos.teran@cobiscorp.com; richartharold@hotmail.com

ABSTRACT

We present a review of research related to the usability testing of mobile applications including participants with Down syndrome. The purpose is to identify good usability testing practices and possible guidelines for this process when participants are people with this cognitive disability. These practices and guidelines should account for their specific impairments. We applied document analysis techniques to searches of scientific databases. The results were filtered considering how well they matched the research topic. We processed and reported the classified and summarized results. The main findings of this literature review is that mobile applications usability testing including people with Down syndrome is an issue that has not be comprehensively investigated. While there is some related research, this is incomplete, and there is no single proposal that takes on board all the issues that could be taken into account. Consequently, we propose to develop guidelines on the usability testing process involving participants with Down syndrome.

KEYWORDS

Usability Testing, Mobile Applications, Cognitive Disability, Down Syndrome, Human Computer Interaction (HCI), Mobile Devices.

1. INTRODUCTION

Usability is a quality attribute of interactive systems defined by five attributes: learnability, efficiency, memorability, errors and satisfaction (Nielsen and Kaufmann). In ISO 9241-11

Natarajan Meghanathan et al. (Eds) : ICAIT, CRYPIS, NC, ITCSE-2016
pp. 01–11, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60701

(Abran et al.), the International Organization for Standardizations (ISO) bases usability on three quality attributes: effectiveness, efficiency and satisfaction. Usability is one of the key qualities of a product or system. Systems whose usability is good are easy to learn, efficient, not prone to errors and generate user satisfaction (Nielsen and Kaufmann), (Abran et al.).This paper focuses on one particular cognitive disability: Down syndrome (DS). Down syndrome is a genetic disorder with a worldwide incidence close to one in every 700 births (15/10,000), but the risk varies with the mother's age. In 2010 there were approximately 34,000 people with DS in Spain. People with DS have impaired cognitive processing, language learning and physical abilities, as well as different personal and social characteristics (Yussof and Badioze Zaman).

A usability testing methodology suitable for participants including people with DS needs to be well designed (Jones, Scanlon, and Clough). The article is structured as follows. First, it describes the nine usability testing process steps. It then describes the literature review process, including the applied methodology, searches and filters.

2. USABILITY TESTING PROCESS

A user-centred design process is applied to build products and systems with a satisfactory level of usability [1]. As part of this process, planning, context of use analysis, interactive system design and evaluation tasks are carried out iteratively. A key step is usability evaluation. There are several methods for evaluating how usable a product or system is: heuristic or guideline evaluation, usability testing and follow-up studies of installed systems [2]. The most common method is usability testing, which involves testing prototypes with real users [3]. Participating users are set a number of tasks that they have to perform using a prototype or a full system. Data on the effectiveness, efficiency and satisfaction of users are collected during testing. Generally, the usability process is divided into the following steps: 1.Recruit participants , 2. Establish the tasks, 3.Write the instructions, 4.Define the test plan , 5.Run the pilot test, 6. Refine the test plan , 7.Run the test session, 8.Analyse the collected objective, 9.Report results. The literature review process described in Section 3 focused on identifying papers that report a usability test with people with Down syndrome and on retrieving the key information that they provide on each of these nine steps

3. LITERATURE REVIEW PROCESS

We applied a review and document analysis (RAD) methodology with two protocols: one for searching for sources of information and the other for inspecting the sources of information [4]. Table 1 shows the search protocol and Table 2 illustrates the document analysis protocol.

The literature review process (Figure 1) was composed of two searches: one used the terms "usability evaluation" and "down syndrome" and the other employed the terms "cognitive disabilities" and "usability". The preliminary list of papers (621 + 415) was first pruned based on date of publication and the relevance of paper titles. This returned 58+57 papers. The list was further pruned based on the relevance of the content of the abstracts. The result was a list of 98 papers (43 + 55). These papers were read and analysed, and 11 papers were found to be of relevance to the topic of usability testing for people with DS.

Table 1: Information source search protocol

Information source search protocol		
Language:	Spanish and English	
Period:	2008 to 2014	
Term	**Individual**	Usability, evaluation, down syndrome, cognitive disabilities, hci, human computer interaction
	Combinations	*Search 1*: USABILITY EVALUATION DOWN SYNDROME *Search 2*: COGNITIVE DISABILITIES USABILITY
Information resources	WEB OF SCIENCE UAM, INGENIO UAM, COPUS UAM, GOOGLE ACADEMICO, MICROSOFT ACADEMIC SEARCH, ERIC, REFSEEK, SCIENCE RESEARCH, WORLD WIDE SCIENCE, SCIELO CERN, SCIENCE DIRECT, SCIENCE, ACM AND SPRINGER	
Search strategies	Two searches were run with combinations of different keywords: • Search 1:"usability evaluation" and "down syndrome" • Search 2: "cognitive disabilities" and "usability" The results were successively refined considering: 1. Year of publication: from 2008 to 2014 2. Relation of publications to technologies and computing 3. Relation of usability to computer systems usability (Human-Computer Interaction – HCI).	

The literature review process has consisted in two searches, one with terms "usability evaluation down syndrome" and the other with the terms "cognitive disabilities usability". The initial list of references was pruned in a first stage based on the relevance of their titles. Then a second pruning was made based on the relevance of the content of the abstracts. The result was a list of 98 papers. These papers have been read and analysed, then we had 11 articles.

These 11 papers were thoroughly analysed and sorted by priority (high, medium or low) depending on their contributions to the steps of the usability testing process (Table 3). The result was a list of five high-priority papers that are analysed in Section 4.

We applied the parameters in table 2 to determinate the level priority

Table 2: Information source inspection protocol

Information source inspection protocol	
Inspection rules:	The order of inspection is as follows: 1. Inspection of title 2. Inspection of abstract 3. If the information is relevant to the research topic, the content is inspected.
Exclusion criteria:	1. Duplicate information 2. Information unrelated to the research topic 3. Outdated information.
Inclusion criteria:	1. Information relevant and related to the research topic

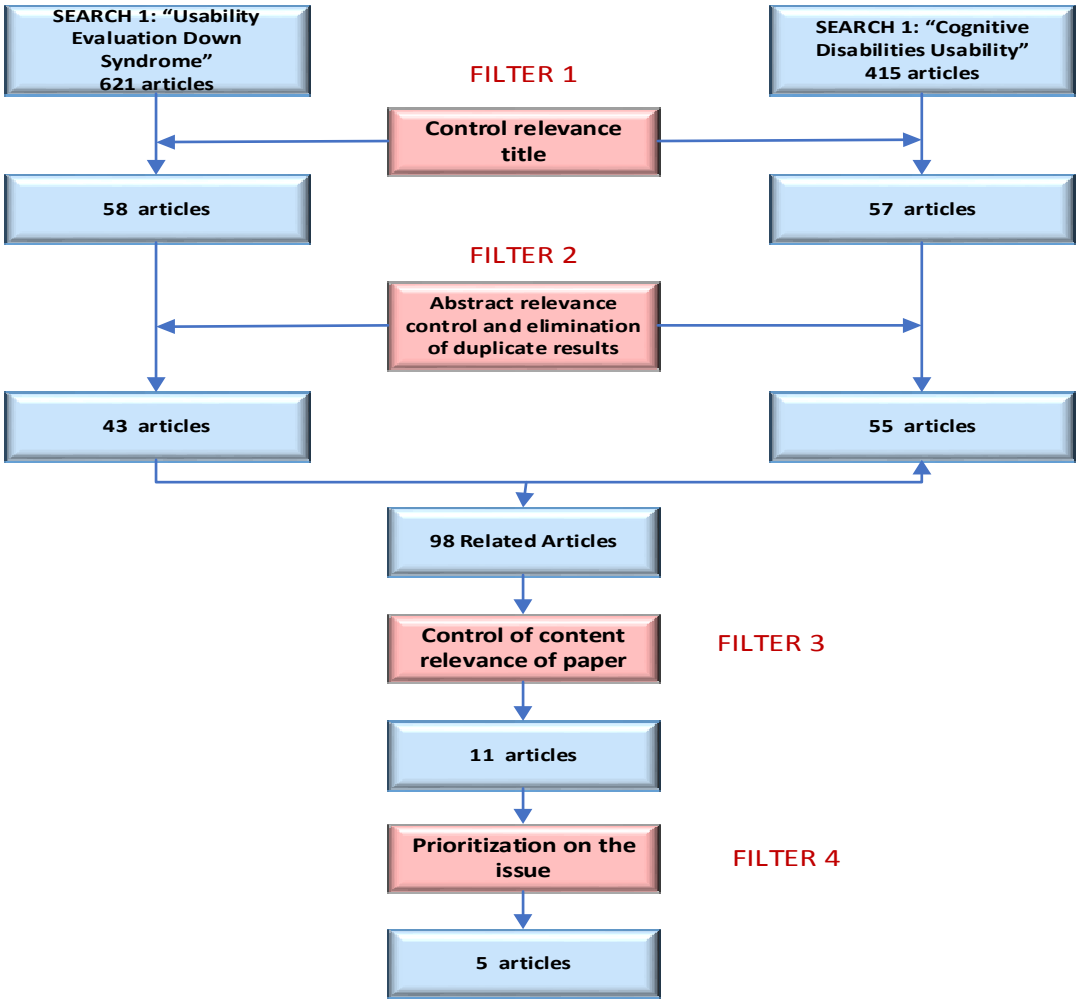

Figure 1 : Search refinement strategy flow diagram

We applied a new filter giving a priority and an important level to the contribution research taking in count the approach of the investigation to the actual research. Finally we obtained result 5 papers have been useful to extract information about usability testing with participants.

Table 3 : Summary and classification of preselected papers

DOCUMENT	PRIORITY	SUMMARY
A method to evaluate disabled user interaction: a case study with Down syndrome children [5]. 2013.	High	This study designed by [5] evaluated four children aged between 6 and 12 years with DS and analyses the development of the coding scheme based on the detailed video analysis method (DEVAN) to observe the interaction of the children with DS. Also applies IQ evaluation and use JECRIPE tool. The test plan is to deliver the application to the children, observe and film. No pilot test was run. Finally, the workshop was held and the results for each child evaluated on average for 45 minutes for all process were analysed.

A Usability Evaluation of Workplace-Related Tasks on a Multi-Touch Tablet Computer by Adults with Down Syndrome [6]. 2012.	High	Two pilot sessions are run: administer demographic questionnaire to participants and validate participant recruitment criteria. Participants were asked to perform five different categories of tasks on an iPad (social networking, electronic mail, scheduling / planning, price comparison and basic text input / note taking). No formal data collection or methodology was applied. Use patterns were observed. They were then used to write a list of tasks and develop a methodology. Participants were reevaluated during the second session, and this information was used to rewrite the list of tasks.
Designing Usability Evaluation Methodology Framework of Augmented Reality Basic Reading Courseware (AR BACA SindD) for Down Syndrome Learner [7]. 2011.	High	This paper proposes a usability evaluation framework for an augmented reality framework for learners with DS. To do this, three to five expert interface design and learning content evaluators were recruited. They analysed 10 adults with DS to evaluate how proficient they were at using multi-touch tablets for job-related tasks. The evaluation was divided into two phases: an acceptance testing phase including formative assessment and a usability phase including either a formative phase with an iterative development cycle or a summative phase where testing is conducted with a large number of users. The goal was to identify strengths and weaknesses [7].
The complementary role of two evaluation methods in the usability and accessibility evaluation of a non-standard system [8]. 2010.	High	[8] worked with five usability and accessibility experts and six learners to evaluate a literacy system in Africa. It was evaluated using the heuristic method and a usability field study. First a pilot study was run to gain an idea of how the applications work. The pilot study activities were: run the evaluation and draft a report of the compiled evaluation for submission to the immediate evaluator.
Usability Evaluation of Multimedia Courseware (MEL-SindD) [9]. 2009.	High	This paper discusses the usability assessment of the courseware, the methods used for the evaluation, as well as suitable approaches that can be deployed to evaluate the courseware effectiveness for disabled children. The evaluation was divided into three phases: PHASE 1. Identify user needs, PHASE 2. Evaluate usability with the participation of 11 students with DS, and PHASE 3. Send the data collected by the researcher to the specialist teachers and parents of the recruited children with DS.
Usability of the SAFEWAY2SCHOOL system in children with cognitive disabilities]. [10]	Low	Fourteen children with DS and a control group of 23 children without disabilities participated in the study conducted by (Falkmer et al., 2014) which involved evaluating a system for improving safe school transport for children.
Validating WCAG versions 1.0 and 2.0 through usability testing with disabled users [11]. 2012.	Low	This paper reports a study that empirically validated the usefulness of using WCAG as a heuristic for website accessibility.
Usability remote evaluation: METBA system [12]. 2012.	Low	This paper reports a solution (METBA) for managing the information related to the evaluation of human behavioural observation . The system is used to register and manage the information derived from remote usability evaluation and complements the methodology commonly used in this research area.
Computer Usage by Children with Down Syndrome: Challenges and Future Research [13]. 2010	Low	This paper reports the text responses collected in the survey and is intended as a step towards understanding the difficulties experienced by children with DS when using computers.

A multi-method, user-centered evaluation of accessibility for persons with disabilities [14]. 2009.	Low	The Study have assessed the accessibility of web site from federal e-government. The conclusion is that web sites should be accessible to persons with disabilities.
Computer Usage by Young Individuals with Down Syndrome: An Exploratory Study [15]. 2008.	Low	This paper discusses the results of an online survey that investigates how children and young adults with DS use computers and computer-related devices.

4. LITERATURE REVIEW RESULTS

We analysed the five selected papers with regard to their contributions to each of the usability testing process Figure 2. A user-centred design process is applied to build products and systems with a satisfactory level of usability (Standard). As part of this process, planning, context of use analysis, interactive system design and evaluation tasks are carried out iteratively. A key step is usability evaluation. There are several methods for evaluating how usable a product or system is: heuristic or guideline evaluation, usability testing and follow-up studies of installed systems (Adebesin and Gelderblom). The most common method is usability testing, which involves testing prototypes with real users (Diah et al.). Participating users are set a number of tasks that they have to perform using a prototype or a full system. Data on the effectiveness, efficiency and satisfaction of users are collected during testing. Generally, the usability process is divided into the following steps:

1. Recruit participants after determining the population group of interest and the required number of participants.

2. Establish the tasks that are to be used in the usability tests.

3. Write the instructions that participants will be given to perform the usability test.

4. Define the test plan, which is a protocol stating activities like welcome, pre-test interview, observed task performance by user, satisfaction questionnaire, personal interview to gather qualitative information, etc.

5. Run the pilot test to analyse whether the process works to plan.

6. Refine the test plan after analysing the results of the pilot tests.

7. Run the test session.

8. Analyse the collected objective (times, number of errors, etc.) and subjective (satisfaction questionnaires) data.

9. Report results to the development team or management.

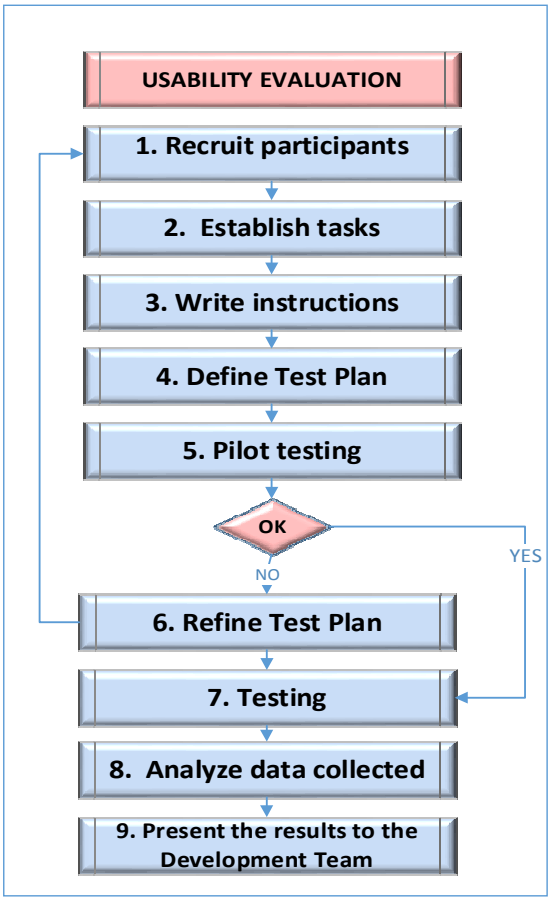

Figure 2: Usability Testing Process

The literature review process described in Section 3 focused on identifying papers that report a usability test with people with Down syndrome and on retrieving the key information that they provide on each of these nine steps. The Table:4 , show the detailed contribution of each author in each phase of the usability process.

Table 4: Part of the analysis of the research on usability testing for people with DS

1. Recruit participants	From the analysis of the research with regard to the recruitment of participants, we find that [5] take four children aged from 6 to 12 years with DS, [8] use five usability experts and six learners, [7] use from three to five interface design and learning content experts, and [16] work with two paediatricians, primary school teachers and 11 children with DS. This illustrates the importance of working with on average 10 paediatricians, interface and learning content evaluators and people with DS.
2. Establish tasks	[5] holds a 30-minute training session, takes 20-minute videos per child and uses the DEVAN method to work directly with children with DS. On the other hand, [8] evaluate a literacy portal in Africa using the following tasks: submission of evaluation criteria, submission of document stating procedure to be followed, submission of document on interfaces and applications for evaluation, signature of anonymity and confidentiality forms. In the research by [8], the experts identify critical usability problems in the early stages of the development cycle and divide the evaluation into two phases: acceptance testing and usability. [9] divide the tasks used in the evaluation into several phases: PHASE 1. Identify user needs, iteratively engage students in

	testing, and collect data from teachers and parents of students with DS, PHASE 2. Conduct the usability evaluation, and PHASE 3. Collect the data from specialist teachers and parents and hold the scheduled interviews. The activities specified by [6] are validate the criteria for recruiting participants, like computer experience.
3. Write instructions	[9] describe the instructions for identifying the needs of users, which are collect data, interview students' paediatrician and primary school teachers, interact socially with students; identify the learning needs. Understand the problems through conversations with parents; interview specialists, teachers and parents as informers on the background of students and the research.
5. Pilot testing	[8] conduct a pilot test aimed at understanding how applications work. [6] believe formal data collection to be important for the pilot test. This should be followed by a second session during which they suggest modifying the list of tasks, adding a warm-up task, giving tips on how to move forward and encouraging thinking aloud.
6. Testing	[9] collect the data iteratively from people with DS in Phase 1. Another aim is identify the suitability of the teaching material for the learning problems that students are set. [8] describe the testing steps: execute evaluation, write report, submit report to immediate evaluator, okay report, and compile evaluation reports.

After the exhaustive analysis we wrote the contributions of each paper Table 5 sets out the information regarding which papers provide key information for each of the steps.

Table 5: Contributions of usability testing papers

Paper	**1. Recruit participants**	**2.Establish tasks**	**3. Write instructions**	**5. Pilot testing**	**7.Testing**
[5] 2013.	X	X			
[8] 2010.	X	X		X.	X
[7] 2011.	X	X			
[6] 2012.		X		X	
[9]. 2009.	X	X	X		X

Note that there are contributions regarding five of the nine usability testing steps: recruit participants (1), establish tasks (2), write instructions (3), pilot testing (5) and testing (7). Table 5 contains the key contributions regarding each of the steps.

Briefly, the retrieved information is as follows. As regards the instructions on tasks, there is very little information. Additionally, the test plan that can be enacted for the population group of interest is not clearly defined. Even though pilot testing greatly improves the second round of testing, pilot tests are seldom used, and the papers fail to establish the format or steps to be taken. As regards testing, they only describe the activities performed without any specific specifications for participants with DS. Therefore, we can conclude that the different papers contain no recommendations as regards the addressed research topic. Table 5 details the activities to be performed to achieve the specific goal of each piece of research but not a general-purpose method proposed by the authors that is applicable across the board.

5. CONCLUSION AND FUTURE WORK

The document analysis reveals that usability has been well researched. As regards usability evaluation, there are many proposals and methodologies. However, we have not found any

significant efforts considering mobile applications and people with DS. On this ground, there is a patent need to state guidelines on all the steps to be taken to test the usability of applications for mobile devices for people with DS.

We have started to work on this line of research. To do this, we will take into account some of the interesting contributions identified in the analysed papers. Specifically, children with DS find it hard to express their feelings and thoughts. On this ground, it is recommended that they should not be asked to verbalize their suggestions [5]. A pre-test demographic questionnaire is recommended [7]. Different methods, including heuristic evaluation, pluralistic walkthrough, cognitive walkthrough, and graphical jog through, can be used, which should, additionally, be rounded out with a field study. Adults with DS are able to effectively use multi-touch devices for job-related tasks, although password use is still a usability challenge for people with DS. A five-point Likert scale can be used if users are required to rate task difficulty. People with DS have strong visual motor, visual processing and visual memory learning skills, whereas auditory processing and auditory memory are found to be relatively weaker learning channels. The key problems identified were text input using virtual keyboards, problems with passwords and problems with pull-down menus [6]. Researchers should make sure that they gain the trust of and get acquainted with users before the evaluation session [9].

On the other hand, as the identified information is incomplete, we are conducting experimental studies in order to round out the guidelines using the knowledge acquired directly from contact with people with DS. For example, we are holding workshops for both children and adults with DS in order to identify their needs with respect to the use of mobile devices with a basic gesture-based application, including touch, double touch, drag, rotation, press, scale down and scale up. We have found that the 108 participants have special needs and the general usability testing procedures do not work well.

Mobile computing has a very promising future with a view to improving the life of people with DS, provided that the developed solutions meet the needs of these people. Accordingly, the proposed research on usability testing with people with DS is an opportunity to improve the inclusion of this population group which is at risk of exclusion from technological development.

ACKNOWLEDGEMENTS

This work was also supported by a pre-doctoral scholarship given by the SENESCYT (Secretaria Nacional de Educación Superior, Ciencia y Tecnología e Innovación) of the government of Ecuador (N0. 381 -2012) to Doris Cáliz.

REFERENCES

[1] I. Standard, “DRAFT INTERNATIONAL STANDARD ISO / FDIS,” vol. 2009, 2010.

[2] F. Adebesin and P. H. Gelderblom, “Technical Report Usability and Accessibility Evaluation of the Digital Doorway.”

[3] N. M. Diah, M. Ismail, S. Ahmad, and M. K. M. Dahari, “Usability testing for educational computer game using observation method,” Proc. - 2010 Int. Conf. Inf. Retr. Knowl. Manag. Explor. Invis. World, CAMP’10, pp. 157–161, 2010.

[4] J. W. Barbosa Chacón, J. C. Barbosa Herrera, and M. Rodrígue Villabona, "Revisión y análisis documental para estado del arte: Una propuesta metodológica desde el contexto de la sistematización de experiencias educativas," Investig. Bibl., vol. 27, no. 61, pp. 83–105, 2013.

[5] I. Macedo and D. G. Trevisan, "A Method to Evaluate Disabled User Interaction : A Case Study with Down Syndrome Children," Univers. Access Human-Computer Interact. Des. Methods, Tools, Interact. Tech. eInclusion, pp. 50–58, 2013.

[6] L. Kumin and J. Lazar, "A Usability Evaluation of Workplace-Related Tasks on a Multi-Touch Tablet Computer by Adults with Down Syndrome," J. Usability …, vol. 7, no. 4, pp. 118–142, 2012.

[7] R. Ramli and H. B. Zaman, "Designing usability evaluation methodology framework of Augmented Reality basic reading courseware (AR BACA SindD) for Down Syndrome learner," Proc. 2011 Int. Conf. Electr. Eng. Informatics, ICEEI 2011, no. July, 2011.

[8] F. Adebesin, P. Kotzé, and H. Gelderblom, "The complementary role of two evaluation methods in the usability and accessibility evaluation of a non-standard system," Proc. 2010 Annu. Res. Conf. South African Inst. Comput. Sci. Inf. Technol. - SAICSIT '10, pp. 1–11, 2010.

[9] R. L. Yussof and H. Badioze Zaman, "Usability evaluation of multimedia courseware (MEL-SindD)," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5857 LNCS, pp. 337–343, 2009.

[10] S. K. D. Mello, S. D. Craig, B. Gholson, S. Franklin, R. Picard, and A. C. Graesser, "Integrating Affect Sensors in an Intelligent Tutoring System," Affect. Interact. Comput. Affect. Loop Work. 2005 Int. Conf. Intell. User Interfaces, pp. 7–13, 2005.

[11] D. Rømen and D. Svanæs, "Validating WCAG versions 1.0 and 2.0 through usability testing with disabled users," Univers. Access Inf. Soc., vol. 11, no. 4, pp. 375–385, 2012.

[12] F. Alcantud, J. Coret, E. Jiménez, S. Márquez, F. Moreno, and J. Pérez, "Usability remote evaluation: METBA system," 2012 15th Int. Conf. Interact. Collab. Learn. ICL 2012, 2012.

[13] J. Feng, J. Lazar, and L. Kumin, "Computer Usage by Children with Down Syndrome : Challenges and Future Research," Computer (Long. Beach. Calif)., vol. 2, no. 3, p. 13, 2010.

[14] P. T. Jaeger, "Assessing Section 508 compliance on federal e-government Web sites: A multi-method, user-centered evaluation of accessibility for persons with disabilities," Gov. Inf. Q., vol. 23, no. 2, pp. 169–190, 2006.

[15] J. Feng, J. Lazar, L. Kumin, and a Ozok, "Computer Usage by Young Individuals with Down Syndrome: An Exploratory Study," Proc. 10th Int. ACM SIGACCESS Conf. Comput. Access., pp. 35–42, 2008.

[16] R. L. Yussof and T. N. S. T. Paris, "Reading Activities Using the Scaffolding in MEL-SindD for Down Syndrome Children," Procedia - Soc. Behav. Sci., vol. 35, no. December 2011, pp. 121–128, 2012.

AUTHORS

Ing. MSc. Doris Cruz Caliz Ramos.

- Computer Sciences Engineering
- Master in Management of Information Technology and Communications National Polytechnic School Ecuador. 2008 - 2012
- International Leadership Training. Germany. 2011 - 2012
- PHD Student in Polytechnic School Madrid. 2013- 2017
- Academic Visitor in Middlesex University London. 2015 - 2016

Ing.MSc. Richarth Harold Caliz Ramos.

- Master in Management of Information Technology and Communications MSc, final mark: cum laude. National Polytechnic School (EPN), Quito, Ecuador (Fall 2008-Winter 2010)
- Telecommunications and Electronics Engineering, final mark: cum laude. National Polytechnic School (EPN), Quito, Ecuador (Fall 1995-Winter 2002)

Doctor. Loic Antonio Martinez Normand

- Professor Department ETSIINF, DLSIIS, Madrid Polytechnic University. 2008 – Today.
- Researcher in Group Investigation on Technology Informatics and Communications: CETTICO.
- President Sidar Foundation. 2002 – Today

Ing. MSc. Carlos Miguel Terán Villamarín

- Computer Sciences Engineering
- Master in Management of Information Technology and Communications National Polytechnic School Ecuador. 2008 – 2012
- Vice-president Technology Department in COBISCORP. S.A

Xavier Alamán Roldán

- Professor Autonomous University Madrid Computer Sciences and Artificial Intelligence.
  1993 – Today
- Doctor CC. Physics UCM in 1993
- M.Sc. on Artificial Intelligence (UCLA

INTENTIONAL BLANK

AVOIDING DUPLICATED COMPUTATION TO IMPROVE THE PERFORMANCE OF PFSP ON CUDA GPUS

Chao-Chin Wu[1*], Kai-Cheng Wei[1], Wei-Shen Lai[2], Yun-Ju Li[1]

[1]Department of Computer Science and Information Engineering, National Changhua University of Education, Changhua 500, Taiwan
ccwu@cc.ncue.edu.tw, kcwei@cc.ncue.edu.tw, icecloud6666@gmail.com
[2]Department of Information Management,
Chienkuo Technology University, Changhua 500, Taiwan
weishenlai@gmail.com

ABSTRACT

Graphics Processing Units (GPUs) have been emerged as powerful parallel compute platforms for various application domains. A GPU consists of hundreds or even thousands processor cores and adopts Single Instruction Multiple Threading (SIMT) architecture. Previously, we have proposed an approach that optimizes the Tabu Search algorithm for solving the Permutation Flowshop Scheduling Problem (PFSP) on a GPU by using a math function to generate all different permutations, avoiding the need of placing all the permutations in the global memory. Based on the research result, this paper proposes another approach that further improves the performance by avoiding duplicated computation among threads, which is incurred when any two permutations have the same prefix. Experimental results show that the GPU implementation of our proposed Tabu Search for PFSP runs up to 1.5 times faster than another GPU implementation proposed by Czapiński and Barnes.

KEYWORDS

GPU, CUDA, Parallel algorithm, Tabu Search, Permutation Flowshop Scheduling Problem

1. INTRODUCTION

GPUs (Graphics Processing Units) have been emerged as powerful parallel compute platforms for various application domains. A GPU consists of hundreds, even more than one thousand, of processing elements, making it very suitable for executing applications with big data and data-level parallelism [1, 2]. Compute Unified Device Architecture (CUDA) [3-5] is proposed by nVIDIA for easier programming on nVIDIA GPUs. Due to the low cost and the popular GPU-inside desktops and laptops, more and more researchers focus on how to parallelize various algorithms on GPU architecture. On the other hand, computational intelligence has been successfully applied to solve many kinds of applications [6-9]. Researchers have investigated how to use GPU computing to accelerate computational intelligence. For example, *Janiak et al.* [10] proposed the GPU implementations of the Tabu Search algorithm for the Travelling Salesman Problem and the Permutation Flowshop Scheduling Problem. Lots of research has

Natarajan Meghanathan et al. (Eds) : ICAIT, CRYPIS, NC, ITCSE-2016
pp. 13–23, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60702

reported that the optimized GPU implementations can run tens of times, or even more than one hundred times, faster than their sequential CPU counterparts.

The Tabu Search algorithm is a neighbourhood-based and deterministic metaheuristic, which is proposed to solve many discrete optimisation problems by *Glover* [11, 12]. This algorithm is similar to the function of human's memory. If the solution has been chosen by the previous generation, then it cannot be chosen again until a specified time interval has passed. This way can avoid choosing the local optimal solution to the problems. While computing the flowtime of the permutations, we use the Tabu list to record which permutations have been chosen to produce local optimal solutions during the previous several generations. In addition, users can set an initial value for the so called Tabu value, which determines how many generations the corresponding permutation cannot be used again since the permutation is selected. Whenever a permutation is selected, it is added into the Tabu list and its corresponding Tabu value is set to the user specified input value. Each Tabu value in the Tabu list will be decreased by one whenever proceeding to the next generation. The permutations in the Tabu list cannot be used until its corresponding Tabu value becomes zero. How to optimizing Tabu search on GPUs has been discussed on several projects [13-15].

The Permutation Flowshop Scheduling Problem (PFSP) has been first proposed by Johnson [16] in 1954. The PFSP is to find the best way to schedule many jobs to be processed on several ordered machines, which minimizes the flowtime that is equal to the total processing time of a permutation of the jobs. PFSP can be applied to the manufacturing and resources management in factories and companies. Due to the large number of jobs, the sequential program for PFSP is too slow to be adopted. GPUs have been adopted to solving the PFSP by using the Tabu search [14, 17]. To compute the flowtime of all permutations on GPUs, the previous work proposed placing all the permutations in the global memory initially to avoid branch divergence [14]. These permutations are produced by CPU sequentially. In each generation, each thread will read a permutation from the global memory. For efficient global memory access, the authors of Reference [10] proposed a data placement method that enables coalesced global memory accesses. They arrange all the permutations in an interleaving way. In other words, all the *i*-th elements of C^N_2 permutations are stored in the global memory contiguously. Following the i-th elements are the contiguous C^N_2 (*i*+1)-th elements. Nevertheless, it takes time to read the permutations from the global memory in each generation. The latency of global memory access is about 300 to 400 cycles. Previously, we have address this problem about how to create the appropriate numbers of threads and blocks and efficiently manage the shared memory [17]. Moreover, we propose using a math function to generate all the permutations on the fly, without the need of generating all the permutations by CPU and placing them on the global memory.

To solve the PFSP, in each generation of Tabu search, every thread will exchange two positions of the parent permutation to generate its child permutation. In the previous work [14,17], every thread has to compute the flowtime by constructing the whole completion time table. However, we have observed the following feature. If two child the two corresponding permutations share the same prefix, completion time tables contain several identical column data between them. More precisely, the number of identical columns equals to the legth of the same prefix .Therefore , there is much duplicated computation between threads in the previous work[14.17]. We will address this issue in this paper. Compared with the sequential CPU version, our new approach can run up to 1.5 times faster.

This paper is organized as follows. Section 2 introduces the CUDA architecture, the Permutation Flowshop Scheduling Problem, and related parallel methods. In Section 3, our proposed approach for implementing the PFSP on a CUDA GPU is described in detail. Section 4 demonstrates the experimental results and analyse the performance. Finally, conclusions are given in Section 5.

2. RELATED WORK

2.1. Compute unified device architecture

The CUDA (Compute Unified Device Architecture) development environment is mainly based on a sequential programming language, such as C/C++, and extended with some special functions that hide most issues of GPUs [3-5]. A GPU consists of several streaming multiprocessors (SMs) and each SM has multiple streaming processor cores [1-2]. From the software perspective, a CUDA's device program is organized as a hierarchy of grids, blocks and threads. To design a CUDA device program, programmers must define a C/C++ function, called kernel. While a CPU invokes a kernel to execute the kernel on GPU, the programmer must specify the number of blocks and the number of threads to be created. A block will be allocated to a SM and the threads within a block are able to communicate each other through the shared memory in the SM. Each thread is executed on a streaming processor. One or more blocks can be executed concurrently on a streaming multiprocessor at a time. There are hundreds or even thousands of threads within a block on CUDA. These threads can be organized as a 1-, 2- or 3-dimensional array, as shown in Figure 1. However, blocks can be organized as only a 1-, or 2-dimensional array.

There are many types of memory on GPU. They have different size, access time, and whether they can be written or read by blocks and threads. The description of each memory type is as below. Global memory is the main memory on a GPU, it can be allocated and deallocated explicitly through invoking the CUDA APIs in the kernel to communicate the CPU with the GPU. It has the largest memory space on the GPU, but it requires 400-600 clock cycles to complete a read or write operation. Blocks can communicate with each other via the global memory.

Constant memory is accessible as global memory except it is cached. A read operation takes the same time as that for the global memory in the case of a cache miss, otherwise it is much faster. The CPU can write and read the constant memory. It is read-only for GPU threads. Shared memory is a very fast memory on the GPU, it is used to communicate between threads in the same block. Data in the shared memory of a block cannot be directly accessed by other blocks. Accessing shared memory requires only 2-4 clock cycles. Unfortunately, the memory space of shared memory is limited. The maximum space is 16384 bytes per block for Tesla C1060. When a thread needs more space than the shared memory, the thread has to swap out and in the data in shared memory explicitly. Registers are the fastest memory that can only be used in the thread scope. They are for automatic variables. The number of 32-bit register is limited up to 16384 on each streaming multiprocessor on Tesla C1060. Local memory is used for large automatic variables per-thread, such as arrays. Both read and write operations take the same time as that for the global memory.

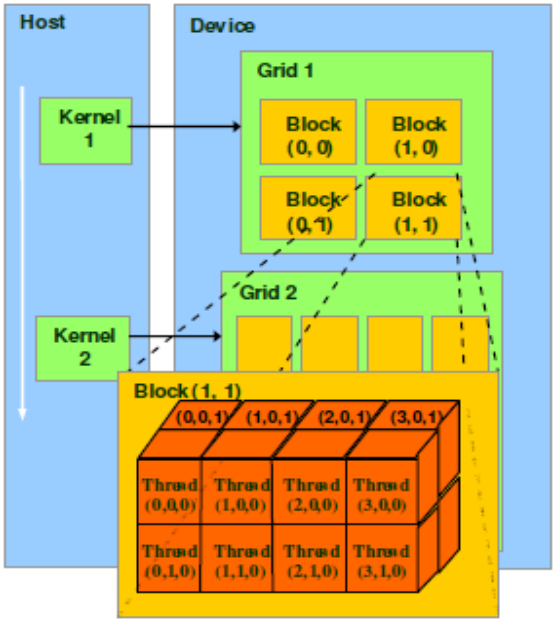

Figure 1. The relations between threads, blocks, and grids

2.2. Permutation Flowshop Scheduling Problem

In the PFSP, a set of N jobs is to be processed on a set of R machines. Each job will be divided into R parts and go through the R machines in a predefined order. Assume M_i is Machine i, and J_k is Job k. Let $P_{i,j}$ denote the processing time of Job k on Machine i. Compute the flowtime, denoted as $C_{i,k}$, for processing J_k on machine M_i, which is defined as the following formula. Each permutation has its own flowtime $C_{m,n}$.

$$C_{0,0} = p_{0,0},$$
$$C_{i,0} = p_{i,0} + C_{i-1,0},$$
$$C_{0,k} = p_{0,k} + C_{0,k-1},$$
$$C_{i,k} = p_{i,k} + \max\{C_{i,k-1}, C_{i-1,k}\},$$
$$\text{where} \quad i \in \{1,2,\ldots, m\}, \quad \text{and} \quad k \in \{1,2,\ldots, n\}$$

To solve the PFSP is to find the minimum of all flowtimes from all permutations. Let ω_i is a permutation, then $C_{m,n}(\omega_i)$ denotes the flowtime of the permutation ω_i. Ω_x denotes the set of all permutations of length x.

$$\forall \omega \in \Omega_x, C_{\max} = \max\{C_{m,n}(\omega_1), C_{m,n}(\omega_2),\ldots, C_{m,n}(\omega_x)\}$$

Because the PFSP is a NP problem, it has been parallelized to shorten its execution time. For instance, *Chakroun et al.* [10] used the branch-and-bound algorithm and the inter-task parallel method to improve the performance of the flowshop problem on GPUs. In the inter-task method, each thread calculates the flowtime for a permutation. Each thread is responsible for sequentially computing the flowtime for a permutation. The advantage is that the threads have no data dependency between each other in the block, so they do not need to synchronize with each other

or wait for another. The disadvantage is that each thread needs a large amount of the shared memory space for processing a permutation. It has low performance when more jobs and machines have to be processed because threads in the same block contend for the use of the shared memory. Due to the limitation of available shared memory space, the maximum number of threads per block cannot be very large.

On the other hand, the intra-task method let all the threads in a block process a permutation together. *Michael et al.* [11] used the intra-task method by well utilizing the characteristic of the GPU memory, such as memory coalescing for accessing the global memory, and avoiding bank conflict on the shared memory. They let each block be responsible for computing the flowtime of a permutation, where multiple threads in a block work together to compute the flowtime for a permutation. The advantage of the method is that a larger number of threads can execute the PFSP concurrently because of using less shared memory when the flowtime of a permutation is processed by a block. In other words, it means the elements in an anti-diagonal have no data dependency between each other. Unfortunately, this method has two drawbasks. First, the number of threads in each phase is not equivalent. It causes the waste of thread resources, due to the idle threads in some phases. Second, the elements in each anti-diagonal have to wait for the results produced by the elements in the previous anti-diagonal. It needs synchronization between threads and blocks, making it necessary to invoke one kernel for each phase.

3. AVOIDING DUPLICATED COMPUTATION

In this section, we describe the proposed approach of avoiding duplicated computation. Section 3.1 presents the relation between the completion tables of the parent permutation and the child permutation. Section 3.2 explains how we can use the above important observation to design an algorithm to accelerate the execution of the completion time tables for child permutations.

3.1. Observation

For the Tabu search for PFSP, in each generation, the permutations to be processed are generated based on the best processing order of jobs produced in the previous generation. If there are N jobs, there will be C^N_2 permutations at most to be processed in each generation, where any permutation leading to a job processing order the same as one in the Tabu list will be prohibited in the generation.

In each generation of the Tabu search, each thread will be assigned on permutation to calculate the flow time of the permutation. To accelerate the computation of the flow time, each thread will be allocated with M words on shared memory if there are M machines in the PFSP. Shared memory is fast memory for the scope of a CUDA block. The number of threads is limited by the available space of shared memory if each thread requires shared memory space. In other words, if each thread uses less shared memory space to process and compute the flowtime of a permutation, the block can have more threads. For PFSP, the number of machines is less than that of jobs in general. To keep the required shared memory as much as possible, the number of shared memory words per thread is equal to the number of machines. As shown in Figure 2, if there are 3 machines and 4 jobs, we allocate 3 shared memory words for a thread. Then, it computes sequentially according to the order of the permutation.

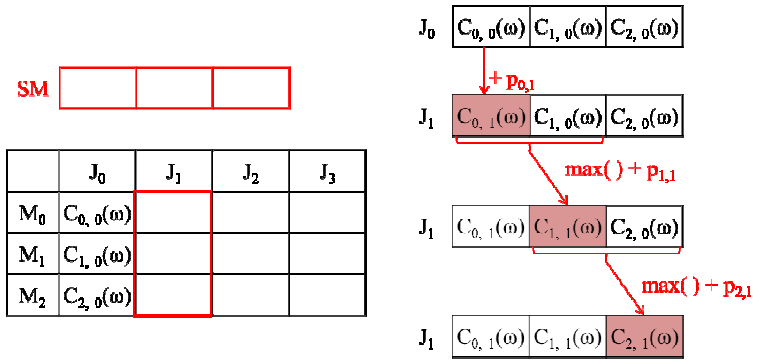

Fig. 2. The space allocation of shared memory, the completion time table, and the register reutilization for calculating completion time within the same column

For the thread to process the permutation, J_0, J_1, J_2, J_3, as show in Figure 2, it will calculate the completion time for J_0 on each machine, from M_0 to M_2 one by one, as show in Figure 2. Next, it continues the computations for the subsequent jobs, J_1, J_2, J_3, one by one, and finally obtain the flow time for the permutation. If we exchange the positions of J_2 and J_3 on the above permutation, new permutation, J_0, J_1, J_3, J_2, is generated. To compute the flow time, a thread will be assigned to perform the same procedures as that illustrated in Figure 2, except the job ordering. We depict two tables in Figure 3 to show the completion times for each job on different machines for the above two permutations. Note that each call of any table contains one completion time and all the completion time in one table are calculated one by one from top to bottom and from left to night. As a result, the first two columns in both tables have the same contents, respectively because the first two jobs in the two permutations are both J_0 and J_1. However, the two third columns in the tables are different because the third job in the original permutation is J_3 but the third Job in the new permutation is J_2. Since the calculation of i-th column depends in the results in *(i-1)-th* column, the results in the two third columns are different. Furthermore, for the following columns, the same columns on both tables have different values.

In general, assume there are a parent permutation, π_0, π_1, π_2, … …, π_n and a child permutation is derived from the parent permutation by exchanging two positions, π_i and π_j , where i<j and $0 \leqq i \leqq n$, $0 \leqq j \leqq n$, The first (i-1) columns in the two corresponding tables of completion time will have the same contents. For the subsequent columns in the two tables any pair of two columns with the same column number must have different completion times. As a result, if we have the completion time table of the parent permutation, we can calculate the flowtime of the child permutation from the *i-th* column after copying the *(i-1)-th* column in the completion table for the parent permutation. In fact the computation of the first *(i-1)* columns in the completion time table for the child permutation is redundant if we are given the completion time table for the parent permutation.

To solve the PFSP, at most C^N_2 child permutations will be generated in each generation of Tabu search based on the parent permutation, where each child permutation is obtained by exchanging two positions in the parent permutation. In previous world [14, 17], at most C^N_2 threads will be forked in each generation and each thread is assigned with one child permutation. All threads compute the flowtimes in parallel for their permutations because each flowtime computation depends on only the parent permutation. Since each thread constructs all the table of completion time for its assigned permutation from the scratch based on mainly the parent permutation, too

much redundant computation is performed, resulting in worse performance. Therefore, we propose an approach in the following subsection to accelerate the execution of solving the PFSP by using Tabu search on GPU.

	J_0	J_1	J_2	J_3
M_0	$C_{0,0}(\omega)$	$C_{0,1}(\omega)$	$C_{0,2}(\omega)$	$C_{0,3}(\omega)$
M_1	$C_{1,0}(\omega)$	$C_{1,1}(\omega)$	$C_{1,2}(\omega)$	$C_{1,3}(\omega)$
M_2	$C_{2,0}(\omega)$	$C_{2,1}(\omega)$	$C_{2,2}(\omega)$	$C_{2,3}(\omega)$

(a) The completion time table of the permutation: J_0, J_1, J_2, J_3

	J_0	J_1	J_3	J_2
M_0	$C_{0,0}(\omega)$	$C_{0,1}(\omega)$	$C_{0,3}(\omega)$	$C_{0,2}(\omega)$
M_1	$C_{1,0}(\omega)$	$C_{1,1}(\omega)$	$C_{1,3}(\omega)$	$C_{1,2}(\omega)$
M_2	$C_{2,0}(\omega)$	$C_{2,1}(\omega)$	$C_{2,3}(\omega)$	$C_{2,2}(\omega)$

(b) The completion time table of the permutation: J_0, J_1, J_3, J_2

Fig. 3. Comparison between completion time tables of two permutations, where two positions are different in the permutations

3.2. Our Proposed Approach

Instead of computing the flowtime from the empty completion time table as that adopted in the previous for each child permutation work [14, 17], we start the computation from the *i-th* column after copying the *(i-1)-th* column from the parent's completion time table. To achieve the goal, we have to store all the completion time table for the parent permutation in the global memory, which is not necessary in the previous work [14, 17]. Figure 4 demonstrates an example of our proposed approach. The completion time table for the parent permutation, (1, 2, 3, 4, 5, 6), is calculated and stored in the global memory. Assume the thread T_1, will exchange Jobs 3 and 6 in the parent permutation to produce his child permutation, (1, 2, 6, 4, 5, 3). T_1 has to fetch the whole second column in the completion time table of the parent permutation in the global memory and save the column data into shared memory. Following the similar computation procedures shown in Figure 2, T_1 can calculate the flowtime for its child permutation. In this way, T_1 can avoid the computation of the first two columns, resulting in a shorter execution time. Similarly, if T_2 will exchange Jobs 4 and 6 in the parent permutation, it has to fetch the third column from the global memory, which is used to calculate the completion times for the following columns and derive the flowtime. Totally, the computation of three columns are avoided for T_2. After the flowtimes for all possible child permutation are produced, we will select the permutation with the minimum flowtime to become the parent permutation for the next generation. However, in fact, the completion time table of the newly selected parent permutation does not exist because all column data are stored in the same shared memory of one-table-column size, as shown in Figure 4. At the end, only the last column data are stored in shared memory.

Note that it is impossible to store all the information about the whole completion time table in shared memory for every thread because of the limited shared memory space. Also it is impossible to know which child permutation will become the parent permutation for the next generation before the flowtimes of all possible child permutations are calculated. One possible solution to address the above problem is that every thread writes all its column data to the global memory. However, this solution will result in high overhead due to a large amount of long-latency global memory access.

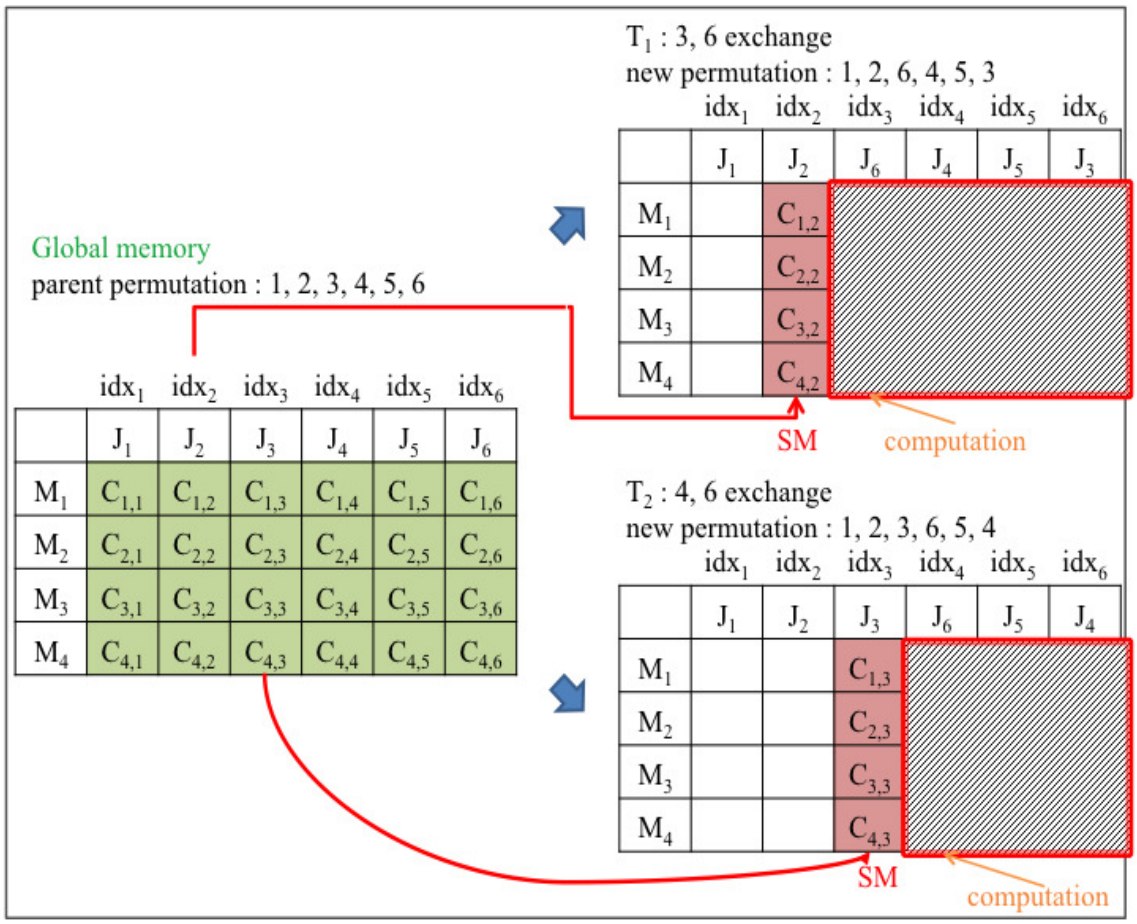

Fig. 4 Avoiding duplicated computation when calculating the completion time table of child permutations from the one of the parent permutation.

We adopt another solution to address the above problem. After the new parent permutation is selected, we use one thread block to calculate the completion time table of the new parent permutation and store the table in global memory. In our proposed approach, we need to construct the completion time table for the next parent permutation, which is the unique overhead for our approach comparing the previous work [14, 17]. Therefore, minimizing the execution time of constructing the table is the key issue of the success of our proposed approach. We parallelize the above table construction with a single thread block [11], as shown in Figure 5. Because of the data dependency, the completion time table construction, is parallelized diagonally. In the example shown in Figure 5, there are 4 machines and 4 jobs. The table construction consists of 7 phases, indicated by dash lines with numbers. The maximum number of threads required is 4. Between any two consecutive phases, we need to insert a synchronization to enforce data consistency between threads.

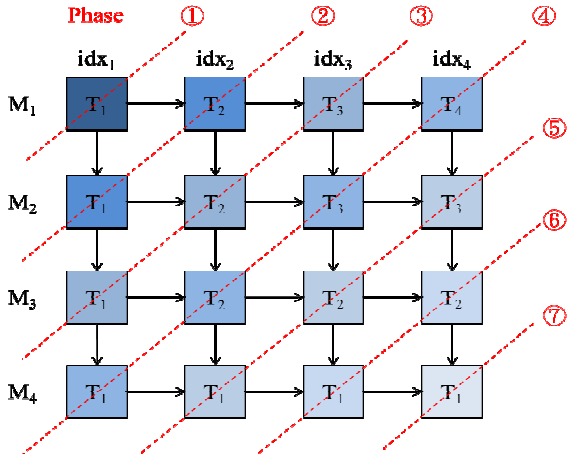

Fig. 5. The parallelization of building the completion time table of the next parent permutation by one thread block.

4. EXPERIMENT RESULTS

The Tabu Search for PFSP is written in C and evaluated on an Intel Pentium 2.5 GHz CPU with 2 GB memory and NVIDIA Tesla C2050 with 448 CUDA cores and 2.6 GB memory. Detailed configurations are shown in Table 1. We use CUDA version 4.2 to implement both the approaches of ours and Czapiński and Barnes', for the Permutation Flowshop Scheduling Problem using the Tabu Search algorithm. The operating system installed is Linux and its version is Ubuntu 11.10, 32-bit.

Table 1. The specifications of the Intel Pentium CPU and the NVIDIA Tesla C2050.

Intel® Pentium® D		NVIDIA Tesla C2050	
# of Cores	2	# of GPUs	1
# of Threads	2	Processor cores	448
Clock Speed	3GHz	Clock Speed	1.15GHz
Memory Size	2GB	Memory Size	2.6GB
Memory Types	DDR2 667	Memory Types	GDDR5
Cache	2MB	Memory Clock	800MHz

We show the speedups of our approach over the Czapiński and Barnes' method in Table 2, where we vary the numbers of the machines, jobs and generations. The speedup is derived from dividing the execution time of our approach by the execution time of Czapiński and Barnes' method. Also, the shared memory size (SMs) is either 16 MB or 48 MB. When the product of (# of machines) and (# of jobs) is smaller than or equal to 3000, our approach would degrade the performance. The reason is as follows. (1) The number of columns that we have no need to re-calculate is rather limited. (2) The computation time of constructing the next parent permutation the completion time table of significantly increases the critical path of the whole execution. On the other hand, when the product is bigger than or equal to 5000, our approach outperforms the previous work. The larger the product, the higher the speedup. The reason is because we can avoid more duplicated computation for larger problem sizes.

Table 2. Speedups of Tabu Search for PFSP, compared with the Czapiński and Barnes' method

# of generations			10		100		1000	
# of ma-chines	# of jobs	SMs m * j	16 MB	48 MB	16 MB	48 MB	16 MB	48 MB
15	100	1500	0.82	0.83	0.65	0.64	0.61	0.61
20	150	3000	0.94	0.95	0.87	0.87	0.85	0.85
25	200	5000	1.01	1.01	1.03	1.03	1.03	1.03
25	350	8750	1.11	1.12	1.28	1.28	1.33	1.33
30	500	15000	1.15	1.14	1.3	1.3	1.34	1.34
30	650	19500	1.15	1.14	1.32	1.32	1.36	1.36
35	800	28000	1.2	1.2	1.35	1.34	1.37	1.37
40	900	36000	1.31	1.31	1.47	1.47	1.5	1.5

5. CONCLUSION

In this paper, an approach of avoiding duplicated computation was presented for the Tabu Search algorithm to solve PFSP on a CUDA GPU. In the previous work, each thread has to calculate the whole completion time table for its assigned child permutation in every iteration. However, we have observed that most child permutations has the same prefix as the parent permutation. Using this observation, we have proposed a new approach. One thread block builds the completion time table of the next parent permutation in parallel and stores the table in the global memory. Each thread fetches the table data of the column, from the global memory, corresponding to the last job in the same prefix. Next, each thread calculates the flowtime according to the column data, without the need of constructing the whole completion time table for its child permutation. Experimental results demonstrated our approach has the best speedup up to 1.5, comparing with the previous work.

In further work, we will apply more optimization techniques of CUDA and utilize the features of a GPU workstation to optimize the Tabu search algorithm, such as how to efficiently manage device memories, synchronize blocks, and reduce the number of computing subtasks.

ACKNOWLEDGMENT

The authors would like to thank the Ministry of Science and Technology, Taiwan, for financially supporting this research under Contract No. MOST104-2221-E-018-007.

REFERENCES

[1] Owens, J.D., Luebke, D., Govindaraju, N., Harris, M., Kruger, J., Lefohn, A.E., Purcell, T.J.: A survey of general-purpose computation on graphics hardware. Computer Graphics Forum 26, pp. 80–113, (2007)

[2] NVIDIA GPU, http://www.nvidia.com/object/cuda_home_new.html.

[3] NVIDIA GPU Programming Guide, http://docs.nvidia.com/cuda/cuda-c-programming-guide/index.html.

[4] Kirk, D.B., Hwu, W.W.: Programming Massively Parallel Processors. NVIDIA.

[5] Oster, Brent: Programming the CUDA Architecture: A Look at GPU Computing. Electronic Design, Vol. 57, Issue 7. (2009)

[6] Ge, M., Wang, Q.-G., Chiu, M.-S., Lee, T.-H., Hang, C.-C., Teo, K.-H.: An effective technique for batch process optimization with application to crystallization. Chemical Engineering Research and Design, Vol. 78, No. 1, pp. 99-106. (2000)

[7] Precup, R.-E., David, R.-C., Petriu, E. M., Preitl, S. Radac, M.-B.: Novel adaptive gravitational search algorithm for fuzzy controlled servo systems. IEEE Transactions on Industrial Informatics, Vol. 8, No. 4, pp. 791–800. (2012)

[8] Saha, S. K., Ghoshal, S. P., Kar, R. Mandal, D. Cat swarm optimization algorithm for optimal linear phase FIR filter design. ISA Transactions, Vol. 52, No. 6, pp. 781-794. (2013)

[9] Yazdani, D., Nasiri, B., Azizi, R. Sepas-Moghaddam, A., Meybodi, M. R.: Optimization in dynamic environments utilizing a novel method based on particle swarm optimization. International Journal of Artificial Intelligence, Vol. 11, No. A13, pp. 170-192. (2013)

[10] Bożejko, W., Wodecki, M.: Parallel genetic algorithm for the flow shop scheduling problem. Lecture Notes in Computer Science, Vol.3019, pp.566–571. (2004)

[11] Glover, F.: Tabu search—part I. ORSA Journal on Computing 1, Vol.3, pp.190-206. (1989)

[12] Glover, F.: Tabu search—part II. ORSA Journal on Computing 2, Vol.1, pp.4-32. (1990)

[13] Janiak, A., Janiak, W., Lichtenstein, M.: Tabu search on GPU. Journal of Universal Computer Science 14, Vol.14, pp.2416–2427. (2008)

[14] Czapiński, M., Barnes, S.: Tabu Search with two approaches to parallel flowshop evaluation on CUDA platform. J. Parallel Distrib. Comput., Vol.71, pp.802-811. (2011)

[15] Chakroun, I. Bendjoudi, A. Melab, N. Reducing Thread Divergence in GPU-Based B&B Applied to the Flow-Shop Problem. PPAM. (2011)

[16] Johnson, S.M.: Optimal two- and three-stage production schedules with setup times included. Naval Research Logistics Quarterly 1, Vol.1, pp.61-68. (1954)

[17] Liang-Tsung Huang, Syun-Sheng Jhan, Yun-Ju Li, Chao-Chin Wu, “Solving the Permutation Problem Efficiently for Tabu Search on CUDA GPUs,” 6th International Conference on Computational Collective Intelligence Technologies and Applications, LNAI 8733, pp. 342-352, 24th-26th September 2014, Seoul, Korea.

INTENTIONAL BLANK

A PROXY SIGNATURE SCHEME BASED ON NEW SECURE AUTHENTICATED KEY AGREEMENT PROTOCOL

H. Elkamchouchi[1], Heba G. Mohamed[2], Fatma Ahmed[3] and Dalia H. ElKamchouchi[4]

[1]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, helkamchouchi@ieee.org
[2]Dept. of Electrical engineering, Arab Academy for Science and Technology (AAST), heba.g.mohamed@gmail.com
[3]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, moonyally@yahoo.com
[4]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, Daliakamsh@yahoo.com

ABSTRACT

Proxy signature scheme permits an original signer to delegate his/her signing capability to a proxy signer and then the proxy signer generates a signing message on behalf of the original signer. So far, the proxy signature scheme is only applied in a special duration, when the original signer is not in his office or when he travels outside. The two parties must be able to authenticate one another and agree on a secret encryption key, in order to communicate securely over an unreliable public network. Authenticated key agreement protocols have an important role in building a secure communications network between the two parties. In this paper, we propose a secure proxy signature scheme over an efficient and secure authenticated key agreement protocol based on RSA cryptosystem.

KEYWORDS

Digital Signature, Proxy Signature, RSA, Key Agreement

1. INTRODUCTION

The cryptographic treatment of proxy signature scheme was first introduced by Mambo et Al.in 1996 [1]. Proxy signature is an important inquiry in the field of a digital signature. It permits an original signer to delegate his signing rights to a proxy signer, and then the proxy signer performs message signing on behalf of the original signer. For example, a director of a company wants to survive for a long trip. He would require a proxy agent, to whom he would delegate his signing capability, and thereafter the proxy agent would sign the documents on behalf of the director. The classification of the proxy signature is dependent on the basis of delegation, namely full delegation, partial delegation and delegation by warrant, and presents a well-organized strategy.

Natarajan Meghanathan et al. (Eds) : ICAIT, CRYPIS, NC, ITCSE-2016
pp. 25–33, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60703

In full delegation, the proxy signer signs document using the same secret key of the original signer given by the original signer. The drawback of proxy signature with full delegation is the difficulty to distinct/differentiate between original signer and proxy signer. In partial delegation, the proxy key is derived from the secret key of the original signer and hands it over to the proxy signer as a delegation capability. Due to partial delegation cannot restrict the proxy signer's signing capability, he can misuse the delegation capability. The weaknesses of full delegation and partial delegation are eliminated by partial delegation with warrant. A warrant, explicitly states the signer's identity, delegation period and the qualification of messages on which the proxy signer can sign.

In 1997, Kim, et al., [2] proposed a scheme using the concept of partial delegation with a warrant to restrict proxy signer signing capability. In 1999, Okamoto, et al., [3], for the first time, proposed proxy unprotected signature scheme based on RSA scheme. A proxy-protected signature scheme based on the RSA assumption was proposed by Lee, et al., in 2001 [4, 5]. In 2002, Shum and Wei [6] proposed another proxy protected signature scheme. Shao proposed the first proxy signature scheme based on the factoring integer problem in 2003 [7]. In 2005, Zhou, et al., [8] proposed two efficient proxy-protected signature schemes. Their first system is based on RSA assumption and the second strategy was based on the integer factorization problem. Park, et al., [9] observed the defect of Zhou, et al., systems. The normal proxy signature scheme and multi-proxy signature scheme based on the difficulty of factoring of large integers was proposed by Xue, et al. in 2006. In 2009, Shao [10] proposed proxy-protected signature scheme based on RSA. Yong, et al., [11] pointed out provably secure proxy signature scheme from the factorization in 2012. Several variants of RSA-based proxy signature scheme were pointed in the sequel [12, 13, 14].

Key establishment protocols are applied at the beginning of a communication session in order to verify the parties' identities and build a common session key to communicate together securely over an unreliable public network. Authenticated key agreement protocols have an important role in establishing secure communications between any two parties over the open network. The most famous protocol for key agreement was proposed by Diffie and Hellman which is based on the concept of public-key cryptography (DL) [15]. There are two types of the Diffie-Hellman protocol namely static and ephemeral. In the first one, the parities exchange static public keys, and in the second, they exchange ephemeral public keys [16]. The important feature of the designed protocol is the established session key is formed as a combination of static and ephemeral private keys of two parties.

In this paper, we propose a secure proxy signature scheme over an efficient and secure authenticated key agreement protocol based on RSA cryptosystem. The designed protocol depends on the relation between two assumptions (RSA factoring and DLP). Moreover, it is efficient and provides authentication between original signer and proxy signer before exchanging the session keys. The remaining parts of this paper are organized as follows. In Section 2, we elaborate security properties of the proxy signature scheme. Next, we discuss the designed protocol in Section 3. In Section 4, we proposed our proxy signature scheme. We analyze the security properties and common attacks of our proposed scheme in Section 5. We analyze the performance analysis of our proposed scheme in Section 6. Finally, in Section 7, we give our conclusion.

2. SECURITY REQUIREMENTS OF PROXY SIGNATURE

Due to the security features of proxy signature scheme, it's become popular and widely. So, any proxy signature should satisfy several requirements. Therefore, a secure proxy signature scheme satisfies the following five requirements [17]:

1. Verifiability: A verifier can be confident of the original signer's agreement on the signed message from a proxy signature.
2. Strong unforgeability: Only the designated proxy signer can generate a valid proxy signature.
3. Strong identifiability: The identity of the proxy signer can be determined by any verifier from a proxy signature.
4. Strong undeniability: The proxy signer cannot repudiate the signature creation against anyone else, once he creates a valid proxy signature on behalf of an original signer.
5. Prevention of misuse: The responsibility of the proxy signer should be determined explicitly if he misuses the proxy key for the purposes other than generating a valid proxy signature.

3. THE NEW SECURE KEY AGREEMENT PROTOCOL

The used protocol for authenticated key agreement [18] provides authentication between the two parties A and B before exchanging the session keys. The protocol consists of three phases; The Registration Phase, The Transfer and Substantiation Phase, and The Key Generation Phase. Figure1 shows the overall operation of the new protocol.The system picks short-term private key r_A, r_B, they are random integers $2 \leq r_A, r_B < n1$ and $GCD(r, n1) = 1$ $n1 = (p-1)(q-1)$ where p, q are large safe prime numbers normally at least 512 bits. t_A, t_B are short-term public keys where $t_A = g^{r_A} \bmod n$ and $t_B = g^{r_B} \bmod n$, g is a generator of Z_p^* and $n = pq$ long term public key at least 1024 bits. Then the system picks long-term private keys x_A, x_B they are random integer where $2 \leq x_A, x_B < n1$ and $GCD(x, n1) = 1$ and compute long-term public key y_A , y_B where $y_A = g^{x_B} \bmod n$ and $y_B = g^{x_A} \bmod n$. K_{AB} is the shared secret key calculated by the new secure protocol between the two parties A and B.

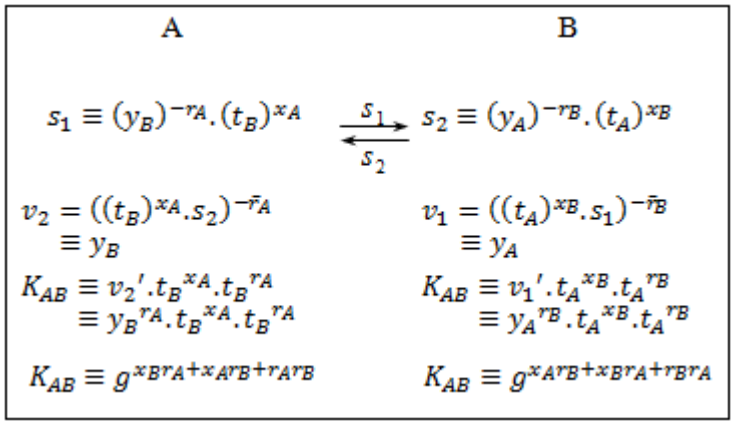

Fig. 1. Overall operation of the proposed protocol

4. PROPOSED PROXY SIGNATURE SCHEME

The proposed scheme is based on a proxy signature scheme with the new secure key agreement protocol and is divided into five phases: Initialization, Proxy key generation, Proxy key verification, Proxy signature generation and Proxy signature verification.

4.1 Initialization

The notation used in our scheme is included as follows:

A:	Original signer
B:	Proxy signer
p, q	Two large prime numbers
$(e_A; d_A)$:	Secret key of original signer
$(e_A; n_A)$:	Public key of original signer
$(e_B; d_B)$:	Secret key of proxy signer
$(e_B; n_B)$:	Public key of proxy signer
n_A , n_B:	The product of two large safe primes
$h(\ )$:	A secure one-way hash function
K_{AB} :	Shared secret key between A and B
m_w:	A warrant.

4.2 Proxy Key Generation

The original signer A does the following:

1. Computes $S_A = h(m_w \| e_B \| K_{AB})^{d_A} \ mod\ n_A$.
2. Sends (S_A, m_w) to the proxy signer over a public channel.

4.3 Proxy Key Verification

The proxy signer B checks whether $h(m_w \| e_B \| K_{AB}) = {S_A}^{e_A} \ mod \ n_A$. If it holds, the proxy signer accepts it as a valid proxy key; otherwise, rejects it.

4.4 Proxy Signature Generation

To sign message *m* on behalf of the original signer A, the proxy signer does the following:

1. Computes $S_B = (S_A \oplus h(m \| m_w \| e_B))^{\ d_B} \ mod\ n_B$ where $\oplus$ is an exclusive OR operation.
2. The proxy signature of message m is $(m, m_w, S_B, e_A, e_B, K_{AB})$.

4.5 Proxy Signature Verification

The verifier verifies whether $h(m_w \| e_B \| K_{AB}) = ({s_B}^{e_B} mod\ n_B \oplus h(m \| m_w \| e_B))^{e_A} \ mod\ n_A$. If it holds, he accepts it as a valid proxy signature; otherwise, rejects it.

5. SECURITY ANALYSIS

In the following, we show that the proposed schemes satisfy the security features, namely, verifiability, strong unforgeability, strong, undeniability, strong identifiability and prevention of misuse**.**

5.1 Verifiability

The verifier of proxy signature, can check whether verification equation $h(m_w \| e_B \| K_{AB}) = (s_B{}^{e_B} mod\ n_B \oplus h(m \| m_w \| e_B))^{e_A} mod\ n_A$ holds or not. We prove this as follows:

$$
\begin{aligned}
&(s_B{}^{e_B} mod\ n_B \oplus h(m \| m_w \| e_B))^{e_A} mod\ n_A \\
&\quad = \{(S_A \oplus h(m \| m_w \| e_B) mod n_B \oplus h(m \| m_w \| e_B)\}^{e_A} mod\ n_A \\
&\quad = \{(h(m_w \| e_B \| K_{AB})^{d_A} mod\ n_A mod\ n_B \oplus h(m \| m_w \| e_B) \oplus h(m \| m_w \| e_B)\}^{e_A} mod\ n_A \\
&= \ h(m_w \| e_B \| K_{AB}) \oplus h(m \| m_w \| e_B)^{e_A} mod\ n_B \oplus h(m \| m_w \| e_B)^{e_A} mod\ n_B \\
&= h(m_w \| e_B \| K_{AB})
\end{aligned}
$$

5.2 Strong Unforgeability

In this scheme, the proxy signature is created with the proxy signer's secret key d_B and delegated proxy key S_A. The proxy key is binding with the original signer's secret keyd_A and the session key K_{AB} where, $S_B = (S_A \oplus h(m \| m_w \| e_B))^{d_B} \ mod\ n_B$ and $S_A = h(m_w \| e_B \| K_{AB})^{d_A} mod\ n_A$. No one (including the original signer) can construct the proxy signature without having the knowledge of the secret keys d_B and d_A. Obtaining these secret keys by any other party is as difficult as breaking RSA. Moreover, the verification of $h(m_w \| e_B \| K_{AB})$ with the signed message prevents the dishonest party from the creation of forged proxy signatures. Therefore, any party, including the original signer cannot forge a valid proxy signature and thus the proposed scheme satisfies the unforgeability property.

5.3 Strong Identifiability

Any verifier can determine the identity of the proxy signer from the proxy signatures created by the proxy signer. Therefore, in the proposed scheme, any verifier can identify the identity of the proxy signer from the proxy signature generated by him, because the signed message is $S_B = (S_A \oplus h(m \| m_w \| e_B))^{d_B} mod n_B$, where S_A is the signed warrant by the original signer. Therefore, in the verification process any verifier can determine the identity of the proxy signer from m_w.

5.4 Strong Undeniability:

From the proposed scheme, the proxy signer and the original signer cannot deny their involvement in a valid proxy signature. In the proposed scheme, their involvements are determined by the warrant m_w , the connection of the public keys e_B and e_A and the common session key K_{AB} in the verification process.So the scheme satisfies the undeniability property.

5.5 Prevention of Misuse

In the proposed scheme, the proxy signer cannot forge the delegated rights. The responsibility of the proxy signer is determined from the warrant m_w in the case of the proxy signer's misuse. Therefore, the original signer's misuse is also prevented because he cannot compute a valid proxy signature against the proxy signer.

Next, we show that our scheme is heuristically secured by considering the following five most common attacks.

Known-Key Security (K-KS): In the proposed scheme, if an established session key between original signer and proxy signer is disclosed, the adversary is unable to learn other established session keys. In each run of the proposed scheme between the two parties should produce a unique session key K_{AB}which depends on r_A and r_B. Therefore, the opponent can't compute K_{AB} and the proposed scheme still achieves its goal in the face of the opponent.

(Perfect) Forward Secrecy: The secrecy of previous session keys established by honest entities is not affected if long-term private keys of one or more entities are compromised.The used protocol possesses a forward secrecy. Suppose that static private keys x_A and x_B of two parties are compromised. Even so, the secrecy of previous session keys established by honest parties is not affected, because an opponent who captured their private keys keys x_A or x_B should extract the ephemeral keys r_A or r_B from the exchanged values to know the previous or next session keys between them. However, this is RSA factorization problem and DLP (Discrete Logarithm Problem).

Key-Compromise Impersonation (K-CI): When A's static private key is compromised, it may be desirable that this event does not enable an adversary to impersonate other entities to A. Suppose A's long-term private key x_A , is disclosed. Now an opponent who knows this value can clearly impersonate A. But he can't impersonates B to A without knowing the B's long-term private keyx_B. For the success of the impersonation, the opponent must know A's ephemeral key r_A .So, in this case, the opponent should extract the value r_A from $t_A = g^{r_A} \ mod \ n$, then compute $r_A{}'$ from $r_A{}'r_A = 1 \ mod \ n1$ which is RSA factorization problem.

Unknown Key-Share (UK-S): Entity B cannot be coerced into sharing a key with entity A without B's knowledge, i.e., when B believes the key is shared with some entity C ≠ A, and A correctly believes the key is shared with B. The designed protocol prevents unknown key-share. Consequent to the assumption of this protocol that s_1 has verified that A possesses the private key x_A corresponding to his static public key y_A , an opponent can't register A's public key y_A as its own and subsequently deceive B into believing that A's messages are originated from the opponent. Therefore B cannot be coerced into sharing a key with entity A without B's knowledge

Subgroup Confinement Attack: Also small subgroup attack [9], the generator g is a primitive root of the prime p. If the selected prime p is such that p-1 has several small prime factors, then some values between 1 and p-1 do not generate groups of order p-1, but of subgroups of smaller orders. If the public parameter of either A or B lies within one of these small subgroups, so the shared secret key would be confined to that subgroup. The intruder may launch a brute force attack to determine the exact value of the shared secret key. The Solution to counter this kind of an attack is to choose a Safe Prime and use g that generates a large prime order subgroup or at the

very least make sure that composite order subgroup are not vulnerable for instance the order's prime number factorization contains only large primes, which we provided in our protocol, we choose two safe prime numbers and use generator of order p'q'

6. PERFORMANCE ANALYSIS

In order to analyze the performance of our scheme, we compare the computational complexity of our scheme with the existing RSA-based proxy signature schemes Lee, *et al.*, [2], Shao [11] and Sawati, *et al.* [17]. Our scheme and the existing schemes do not provide the proxy revocation mechanism. From this comparison, we show that our scheme and Sawati, *et al.* have the same performance analysis and they are efficient than the existing schemes; but our scheme provides extra security than the existing schemes by using new key agreement protocol to protect system fron any intruder . For simplicity, we neglect exclusive-OR operation ($\oplus$) time of the scheme.

Table1. Comparison of Computational Time with Previous Schemes

Phases	LKK schemes (2001)	Shao's scheme (2003)	Swati scheme (2013)	Our Scheme
Setup parameters	2Te + 2Tm + 2To	Te + Tm + To	2Te + 2Tm + 2To	2Te + 2Tm + 2To
Proxy key generation	Te + To + H	Te + To + H	Te + To + H	Te + To + H
Proxy key verification	Te + To + H	Te + To + Tm + H	Te + To + H	Te + To + H
Signature generation	3Te + 3To + 2H	2Te + 2Tm + 2To + H	Te + To + H	Te + To + H
Signature verification	3Te + 3To + 2H	2Te + Tm + To + 2H	2Te + 2Tm + 2To	2Te + 2Tm + 2To

The notations used in the Table 1 are as follows:

Te: computation time for an exponentiation operation
Tm: computation time for a multiplication operation
To: computation time for a modular operation
H: computation time for a hash operation.

The computation time of different phases of the schemes is given in Table 1. It is important to note that the computation time for a valid proxy signature falls into two parts. The first part consists of the time taken for the setup parameters, proxy key generation and proxy key verification process, which are a one-time computation and remain fixed for the entire delegation period. It is observed from Table 1 that for a proxy signature without revocation our scheme has the same performance as [17] in saving at least **Te** or **To** time unit in comparisons to others but it is more secure than the others.

7. CONCLUSION

In this paper, we proposed a new secure proxy signature scheme with a secure and efficient authentication key agreement protocol based on RSA cryptosystem. The used protocol depends

on the relation between two assumption (RSA factoring and DLP). Our scheme does not consider proxy revocation mechanism. The proposed scheme satisfies the necessary security requirements of proxy signature and has a secure channel to deliver the proxy key, through the designed new protocol. The system meets the security attributes and strong against most of potential attacks. So our system can be used to improve the security in an open Internet network.

REFERENCES

[1] M. Mambo, K. Usuda, E. Okamoto, Proxy signature: delegation of the power to sign the message, IEICE Trans. Fundamentals E79-A (9) (1996) PP. 1338 - 1353.

[2] S. Kim, S. Park and D. Won, "Proxy signatures", In: ICICS97, LNCS 1334, Springer-Verlag, (1997), pp. 223-232.

[3] T. Okamoto, M. Tada and E. Okamoto, "Extended proxy signatures for smart card", In: Proceedings of Information Security Workshop 99, LNCS 1729, Springer-Verlag, (1999), pp. 247-258.

[4] B. Lee, H. Kim and K. Kim, "Secure mobile agent using strong non-designated proxy signature", In: Information security and private (ACISP01), LNCS 2119, Springer-Verlag, (2001), pp. 474-486.

[5] B. Lee, H. Kim and K. Kim, "Strong proxy signature and its applications", In: Proceeding of the 2001 symposium on cryptography and information security (SCIS01), vol. 2, no. 2, (2001), pp. 603-608.

[6] K. Shum and V. K. Wei, "A strong proxy signature scheme with proxy signer privacy protection", In: Proceedings of IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE02), (2002).

[7] Z. Shao, "Proxy signature schemes based on factoring", Inform Process Lett., no. 85, (2003), pp. 137 143.

[8] Y. Zhou, Z. Cao and R. Lu, "Provably secure proxy-protected signature schemes based on factoring", Appl Math Comput., vol. 164, no. 1, (2005), pp. 83-98

[9] J. H. Park, B. G. Kang and J. W. Han, "Cryptanalysis of Zhou, et al., proxy-protected signature schemes", Appl. Math Comput., vol. 169, no. 1, (2005), pp. 192-197.

[10] Z. Shao, "Provably secure proxy-protected signature schemes based on RSA", Comput. Electr. Eng., vol. 35, (2009), pp. 497-505.

[11] Y. Yong, M. Yi, W. Susilo, Y. Sun and Y. Ji, "Provably secure proxy signature scheme from factorization", Mathematical and Computer Modelling, vol. 55, (2012), pp. 1160-1168.

[12] Y. Liu, H. Wen and C. Lin, "Proxy-protected signature secure against the un-delegated proxy signature attack", Comput Electron Eng., vol. 33, no. 3, (2007), pp. 177-185.

[13] R. Lu and Z. Cao, "Designated veri_er proxy signature scheme with message recovery", Appl Math Comput., vol. 169, no. 2, (2005), pp. 1237-1246.

[14] R. Lu, X. Dong and Z. Cao, "Designing e_cient proxy signature schemes for mobile communication", In: Science in China, vol. 51, no. 2, (2008), pp. 183-195.

[15] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. IT-l 22, no. 6, PP. 644-654, November, 1976.

[16] K. Chalkias, F. Mpaldimtsi, D. H. Varsakelis, and G. Stephanides, "On the Key-compromise impersonation vulnerability of one-pass key establishment protocols," in Proc. International Conference on Security and Cryptography (SECRYPT 2007), Barcelona, Spain, July 28-31, 2007.

[17] Swati Verma and Birendra Kumar Sharma," An Efficient Proxy Signature Scheme Based On RSA Cryptosystem," International Journal of Advanced Science and Technology Vol. 51, February, 2013,pp.121-126

[18] H. Elkamchouchi, M. R. M. Rizk, and Fatma Ahmed," A New Secure Protocol for Authenticated Key Agreement," IACSIT International Journal of Engineering and Technology, Vol. 5, No. 2, April 2013,pp.245-248

AUTHORS

H. Elkamchouchi obtained his B.Sc Electrical Communication Engineering - Excellent with First Class Honors - Faculty of Engineering – Alexandria University - June 1966, Master Communications Engineering (specialization accurate: antennas and propagation) Faculty of Engineering – Alexandria University - September 1969, B.Sc of Science in Applied Mathematics - Excellent with honors - Britain's Royal College of Science - University of London - England - August 1970, Doctor Communications Engineering (specialization accurate: antennas and propagation) - Faculty of Engineering - Alexandria University -March 1972. He work Professor Emeritus, Faculty of Engineering, Alexandria University from September 2003 until now.

Heba Gaber held a Masters' of science in Electrical Engineering from Faculty of Engineering, Arab Academy for Science and Technology. She works on Arab Academy for Science and Technology. She studies for Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.

Fatma Ahmed held a Masters' of science in Electrical Engineering from Faculty of Engineering, Alexandria University. She works on Alexandria Higher Institute of Engineering and Technology. She Held a Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.

Dalia ElKamchouchi held a Masters' of science in Electrical Engineering from Faculty of Engineering, Alexandria University. She works on Alexandria Higher Institute of Engineering and Technology. She Held a Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.

INTENTIONAL BLANK

A SECURE DIGITAL SIGNATURE SCHEME WITH FAULT TOLERANCE BASED ON THE IMPROVED RSA SYSTEM

H. Elkamchouchi[1], Heba G. Mohamed[2], Fatma Ahmed[3] and Dalia H. ElKamchouchi[4]

[1]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, helkamchouchi@ieee.org
[2]Dept. of Electrical engineering, Arab Academy for Science and Technology (AAST), heba.g.mohamed@gmail.com
[3]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, moonyally@yahoo.com
[4]Dept. of Electrical engineering, Faculty of Engineering, Alexandria University, Daliakamsh@yahoo.com

ABSTRACT

Fault tolerance and data security are two important issues in modern communication systems. In this paper, we propose a secure and efficient digital signature scheme with fault tolerance based on the improved RSA system. The proposed scheme for the RSA cryptosystem contains three prime numbers and overcome several attacks possible on RSA. By using the Chinese Reminder Theorem (CRT) the proposed scheme has a speed improvement on the RSA decryption side and it provides high security also.

KEYWORDS

Digital Signature, Fault tolerance, RSA Cryptosystem, Security Analysis

1. INTRODUCTION

Digital signature schemes with fault tolerance make it possible for error detections and corrections during the processes of data computations and transmissions. Recently, Zhang, in 1999 [1] Lee and Tsai, in 2003[2] have respectively proposed two efficient fault-tolerant schemes based on the RSA cryptosystem. Both of them can efficiently check the sender's identity and keep the confidentiality of the transmitted document. Furthermore, they can detect the errors and correct them. However, these schemes have a common weakness in security, that is, different messages may easily be computed that have the same signature. Thus, a valid signature could be reused in another document.

The vulnerability of Zhang's scheme was pointed out by Iuon-Chang Lei et. Al [3], i.e. a pernicious client could produce an alternate message with the same signature by permuting the rows or columns in the original message matrix *X*. They suggested a new method; this is certainly

Natarajan Meghanathan et al. (Eds) : ICAIT, CRYPIS, NC, ITCSE-2016
pp. 35–44, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60704

improved of Zhang's scheme in which the original message matrix is multiplied by two prime matrices with the same length of the original message. Next for the resulting matrix hash value is calculated to determine which digital signature it is. Afterwards, the checksum calculated for each row and column is inserted at the end of the original matrix. The hash value is appended to the last position of the matrix. The resulting (m+1) × (n+1) matrix is converted into ciphertext and sent to the desired user. They showed that a pernicious client cannot forge a valid message with the same signature by permuting the rows and columns in the matrix.

In 2013, Shreenath Acharya, Sunaina Kotekar and Seema S Joshi [4] have improved the mechanism of Iuon-Chang Lei et. Al with providing extra security by making use of transpose matrix based on the RSA. If a malicious looks into the message he will find it difficult to understand or calculate checksum/ hash value, thus it will confuse the malicious. To keep the confidentiality of the data that transfers over a public network R. Rivest et. al [5] have proposed RSA technique as a public key cryptosystems. According to the proposed scheme, the sender can use the receiver's public key to encrypt a message and the receiver can use his secret key to decrypt the encrypted message. Also, they conveyed that a message can be signed with the secret key of the sender and the signature can be verified by any receiver using the sender's public key. As a result the RSA technique is useful in keeping the confidentiality of the transmitted message, verifying the integrity of the received message, and to prove the sender's identity.

In 2014, [6] Nikita Somani and Dharmendra Mangal have proposed a new security scheme for the RSA cryptosystem contains three prime numbers and overcome several attacks possible on RSA. The new scheme has a speed improvement on the RSA decryption side by using the Chinese Reminder Theorem (CRT). This paper addresses a secure and efficient digital signature scheme with fault tolerance based on the improved RSA system. The remaining parts of this paper are organized as follows: In Section 2, we elaborate Improved of Zhang's scheme. Next, we discuss the improved of the standard RSA in Section 3. In Section 4, we proposed our scheme. We analyze the security properties and common attacks of our proposed scheme in Section 5. Finally, in Section 6, we give our conclusion.

2. IMPROVED VERSION OF ZHANG'S SCHEME

Improved version of Zhang's digital signature scheme [4] with fault tolerance is based on the RSA cryptography. In the RSA cryptography, each user provides a public key (e, N) and a secret key d, where N is the product of two large prime numbers p and q such that $N = p \times q$, and the public key e and secret key d must satisfy the equation $d = e^{-1}(p-1)(q-1)$. Let (e_A, N_A) and (e_B, N_B) be the public keys of user A and user B, d_A and d_B are their secret keys. Moreover, assume $N_A \neq N_B$ and the length of N_A and N_B are the same for simplification. An improved algorithm is as shown. Here the original message matrix is not directly encrypted. But the transpose of the message matrix is taken and then encrypted. As observed in the result part though anyone tries to decrypt the message it is not the clear message line by line. Suppose that user B wants to send a message X to user A,

Algorithm 1:

Step1: User B sends an n×m message matrix to X user A:

$$X = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nm} \end{pmatrix}$$

Where $x_{ij}, 1 \le i \le n, 1 \le j \le m,$ is a message block which has the same length as N_A and N_B

Step 2: Now we take the transpose of the original matrix:

$$T = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ t_{21} & t_{22} & \cdots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} & t_{m2} & \dots & t_{mn} \end{pmatrix} = \begin{pmatrix} x_{11} & x_{21} & \dots & x_{n1} \\ x_{12} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1m} & x_{2m} & \dots & x_{nm} \end{pmatrix}$$

Step 3: User B then creates two prime number matrix P and Q as follows:

$$P = \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & \ddots & \vdots \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \quad , \quad Q = \begin{pmatrix} q_1 & q_1 & \dots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \ddots & \vdots \\ q_m & q_m & \dots & q_m \end{pmatrix}$$

Where matrix P and Q both have the same dimensions with the message matrix T, which is a (m × n) matrix.

Step 4: The sender *B computes* a new message matrix $\bar{X}$ which is the entry-wise product of the matrix T, *P* and *Q:*

$$\bar{T} = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ t_{21} & t_{22} & \cdots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} & t_{m2} & \dots & t_{mn} \end{pmatrix} \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & \ddots & \vdots \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \begin{pmatrix} q_1 & q_1 & \dots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \ddots & \vdots \\ q_m & q_m & \dots & q_m \end{pmatrix}$$

$$= \begin{pmatrix} t_{11} \times p_1 \times q_1 & t_{12} \times p_2 \times q_1 & \dots & t_{1n} \times p_n \times q_m \\ t_{21} \times p_1 \times q_2 & t_{22} \times p_2 \times q_2 & \cdots & t_{2n} \times p_n \times q_m \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} \times p_1 \times q_m & t_{m2} \times p_2 \times q_m & \dots & t_{mn} \times p_n \times q_m \end{pmatrix}$$

$$= \begin{pmatrix} \bar{t}_{11} & \bar{t}_{12} & \dots & \bar{t}_{1n} \\ \bar{t}_{21} & \bar{t}_{22} & \cdots & \bar{t}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{t}_{m1} & \bar{t}_{m2} & \dots & \bar{t}_{mn} \end{pmatrix}$$

Step 5: For the message matrix $\bar{T}$, the sender B now constructs an (n+1)*(m+1) matrix T_h as follows:

$$T_h = \begin{pmatrix} \bar{t}_{11} & \bar{t}_{12} & \dots & \bar{t}_{1n} & T_1 \\ \bar{t}_{21} & \bar{t}_{22} & \cdots & \bar{t}_{2n} & T_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \bar{t}_{m1} & \bar{t}_{m2} & \cdots & \bar{t}_{mn} & T_m \\ T_1 & T_2 & \cdots & T_n & h \end{pmatrix}$$

Where,

$$T_i = \prod_{j=1}^{n} t_{ij} * p_j \bmod N_B \text{ , for } 1 \le i \le m \text{ , } T_j = \prod_{i=1}^{m} t_{ij} * q_i \bmod N_B \text{ , for } 1 \le j \le n \text{ and}$$

$$h = \prod_{j=1}^{n} \left(\prod_{i=1}^{m} t_{ij} \bmod N_B \right) \bmod N_B$$

Step 6: The sender B computes an (n+1)*(m+1) ciphered matrix as follows:

$$C_h = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} & c_1 \\ c_{21} & c_{22} & \cdots & c_{2n} & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} & c_m \\ c_1 & c_2 & \cdots & c_n & h_c \end{pmatrix}$$

Where,

$c_{ij} = \bar{t}_{ij}^{\,e_A} mod\ N_A$, $C_i = T_i^{\,e_A} mod\ N_A$, $C_j = T_j^{\,e_A} mod\ N_A$, $h_c = h^{d_B} mod\ N_B$, *for all* $1 \le i \le n, 1 \le j \le m$

Note that T_i and T_j are the checksums and C_i and C_j are the ciphered checksums.

Step 7: The receiver A uses his/her secret key d_A to decrypt C_h and obtains decrypted message as follows:

$$\bar{T}_h = \begin{pmatrix} \bar{t}_{11} & \bar{t}_{12} & \cdots & \bar{t}_{1n} & \bar{T}_1 \\ \bar{t}_{21} & \bar{t}_{22} & \cdots & \bar{t}_{2n} & \bar{T}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \bar{t}_{m1} & \bar{t}_{m2} & \cdots & \bar{t}_{mn} & \bar{T}_m \\ \bar{T}_1 & \bar{T}_2 & \cdots & \bar{T}_m & \bar{h} \end{pmatrix}$$

Step 8: Now the receiver A verify the checksum to check the following:

$$\bar{T}_i = \prod_{j=1}^{n} \bar{t}_{ij} * p_j \bmod N_B \text{ , for } 1 \le i \le m$$

$$\bar{T}_j = \prod_{i=1}^{m} \bar{t}_{ij} * q_i \bmod N_B \text{ , for } 1 \le j \le n$$

$$\bar{h} = \prod_{j=1}^{n} \left(\prod_{i=1}^{m} \bar{t}_{ij} \bmod N_B \right) \bmod N_B$$

If the verifications are positive, then the receiver believes that the message was not altered during the transmission. Otherwise, there are some errors in the decrypted message.

Step 9: Then user *A* can detect the error by the following two equations

$$\bar{T}_k \neq \prod_{j=1}^{n} \bar{t}_{ij} * p_j \bmod N_B \text{ , for } 1 \le i \le m$$

$$\bar{T}_l \neq \prod_{i=1}^{m} \bar{t}_{ij} * q_i \, mod N_B \, , for \; 1 \leq j \leq n$$

Assuming that the error occurs in the message block $\bar{t}_{kl}$ then, user *A* can correct the error by computing one of the following equations:

$$\bar{t}_{kl} = \bar{T}_k \times \left(\prod_{j=1, j \neq l}^{n} \bar{t}_{kj} \right)^{-1} mod \; N_B$$

$$\bar{t}_{kl} = \bar{T}_l \times \left(\prod_{i=1, i \neq k}^{n} \bar{t}_{il} \right)^{-1} mod \; N_B$$

Step 10: The receiver A takes the transpose of the matrix which will result in message as follows:

$$X_h = \begin{pmatrix} \bar{t}_{11} & \bar{t}_{21} & \cdots & \bar{t}_{m1} \\ \bar{t}_{12} & \bar{t}_{22} & \cdots & \bar{t}_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{t}_{1n} & \bar{t}_{2n} & \cdots & \bar{t}_{mn} \end{pmatrix} = \begin{pmatrix} \bar{x}_{11} & \bar{x}_{12} & \cdots & \bar{x}_{1m} \\ \bar{x}_{21} & \bar{x}_{22} & \cdots & \bar{x}_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{x}_{n1} & \bar{x}_{n2} & \cdots & \bar{x}_{nm} \end{pmatrix}$$

3. IMPROVEMENTS OVER THE STANDARD RSA

The improved RSA scheme provides an enhancement of the Hamami and Aldariseh [7] method by improving the speed on the RSA decryption side and also provides the security by avoiding some attacks possible on RSA. If the same message is encrypted more than one time it will look different every time by using the random number k. The general idea of the improved scheme is to use the Key generation algorithm of Hamami and Aldariseh method and proposed a scheme for encryption and decryption algorithm. The existence of three prime numbers, the difficulty of analysis of variable n must be increases and the key generation time must be reduces. The algorithm for the proposed scheme is as follows:

3.1 Key Generation for Improved RSA Scheme

To generate the key using three prime numbers, user B should do the following:

a) Generate three large prime numbers p, q, and s.
b) Calculate $n = p \times q \times s \;\; and \;\; \varphi(n) = (p-1)(q-1)(s-1)$.
c) Select *e* such that $(e, \varphi(n))$are relatively co-prime.
d) Get the value of d by using $ed \; mod \; \varphi(n) = 1$.
e) Find $d_p = d \; mod(p-1), d_q = d \; mod(q-1), \;\; d_s = d \; mod(s-1)$.
f) Public Key $K_u < e, n >$ and Private Key $K_r < d, p, q, s, d_p, \; d_q, \; d_s >$.

3.2 Encryption Algorithm

To encrypt the message M user A should do the following:
User A should obtained the public key of user B <e, n>

a) Represent the message M as an integer form in interval [0 to n-1].
b) Select k as a random integer $GCD(k, n) = 1$ and 1< k < n-1.
c) Compute C1=$k^e \; mod \; n$.

d) Compute C2=$M^e k \ mod \ n$.
e) Send the cipher text values (C1, C2) to user A

3.3 Decryption Algorithm

On decryption process the concept of RSA is used with CRT. To recover the message from cipher text C2 user A should do the following:

a) Calculate $C_p = C1 \ mod \ p, \ \ C_q = C1 \ mod \ q, \ C_s = C1 \ mod \ s$ and then calculate $k_p = {C_p}^{d_p} \ mod \ p, k_q = {C_q}^{d_q} \ mod \ q \ \ and \ k_s = {C_s}^{d_s} \ mod \ s.$
b) By using the formula calculate k
$k = [\ k_p.(qs)^{(p-1)} \ mod \ n + \ k_p.(ps)^{(q-1)} \ mod \ n + \ k_s.(pq)^{(s-1)} \ mod \ n].$
c) By using the Euclidean algorithm, calculate the value of the unique integer
$t * k \ mod \ n = 1$ and 1< t < n.
d) Then compute M^e, C2*t = (M^e.k)*t = (M^e) k*t = $M^e \ mod \ n$.
e) For getting the value of message M should do the following steps
First calculate $\grave{C}_p = M^e \ mod \ p, \ \grave{C}_q = M^e \ mod \ q, \grave{C}_s = M^e \ mod \ s$ and then calculate $M_p = \grave{C}_p \ mod \ p, M_q = \grave{C}_q \ mod \ q \ , M_s = \grave{C}_s \ mod \ s.$
f) Finally, recover the message M by using the following formula:
$M = [\ M_p.(qs)^{(p-1)} \ mod \ n + \ M_p.(ps)^{(q-1)} \ mod \ n + \ M_s.(pq)^{(s-1)} \ mod \ n].$

4. PROPOSED SCHEME

We propose a secure and efficient digital signature scheme with fault tolerance based on the improved RSA system. In the RSA cryptography, each user provides a public key (*e*, *N)* and a secret key *d,* where *N* is the product of three large prime numbers $p, q \ and \ s$ such that $N = p \times q \times s$, and the public key *e* and secret key *d* must satisfy the equation $d = e^{-1}(p-1)(q-1)(s-1)$.

Algorithm 2:
Step 1to5: Same as Algorithm 1
Step 6: Compute the following ciphertext matrix:
a) Select k as a random integer $GCD(k, N_B) = 1$ and 1< k < $N_B - 1$.
b) Compute C1 = $k^{e_A} \ mod \ N_A$.
c) Compute C2 = ${T_h}^{e_A} k \ mod \ N_A$.

$$C2 \ = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} & c_1 \\ c_{21} & c_{22} & \dots & c_{2n} & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mn} & c_m \\ c_1 & c_2 & \dots & c_n & h_c \end{pmatrix} * k$$

Where,
$c_{ij} = \bar{t}_{ij}^{\ e_A} \ mod \ N_A, \ C_i = {T_i}^{e_A} mod \ N_A, C_j = {T_j}^{e_A} \ mod \ N_A, \ \ h_c = h^{d_B} mod \ N_B,$
for all $1 \le i \le n, 1 \le j \le m$
d) Send the cipher text values (C1, C2) to user A

Step 7: To recover the message T_h from cipher text C2 user A should do the following:

a) Calculate $C_p = C1 \ mod \ p, \quad C_q = C1 \ mod \ q, \ C_s = C1 \ mod \ s$ and then calculate

$k_p = {C_p}^{d_p} \bmod p, k_q = {C_q}^{d_q} \bmod q \ \text{and} \ k_s = {C_s}^{d_s} \bmod s.$

b) By using the formula calculate k
$k = [\, k_p.(qs)^{(p-1)} \bmod N_A + k_p.(ps)^{(q-1)} \bmod N_A + k_s.(pq)^{(s-1)} \bmod N_A \,].$

c) By using the Euclidean algorithm, calculate the value of the unique integer t, $t * k \bmod N_A = 1$ and $1< t <N_A$.

d) Then compute ${T_h}^{e_A}$, C2*t = (${T_h}^{e_A}$.k)*t = (${T_h}^{e_A}$) k*t = ${T_h}^{e_A} \bmod N_A$.

e) For getting the value of message M should do the following steps
First calculate $\dot{C}_p = {T_h}^{e_A} \bmod p$, $\dot{C}_q = {T_h}^{e_A} \bmod q$, $\dot{C}_s = {T_h}^{e_A} \bmod s$ and then calculate $T_p = \dot{C}_p \bmod p, T_q = \dot{C}_q \bmod q\ , T_s = \dot{C}_s \bmod s.$

f) Finally, recover the message T_h by using the following formula:
$T_h = [\, T_p.(qs)^{(p-1)} \bmod N_A + T_p.(ps)^{(q-1)} \bmod N_A + T_s.(pq)^{(s-1)} \bmod N_A].$

$$\bar{T}_h = \begin{pmatrix} \bar{t}_{11} & \bar{t}_{12} & \cdots & \bar{t}_{1n} & \bar{T}_1 \\ \bar{t}_{21} & \bar{t}_{22} & \cdots & \bar{t}_{2n} & \bar{T}_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \bar{t}_{m1} & \bar{t}_{m2} & \cdots & \bar{t}_{mn} & \bar{T}_m \\ \bar{T}_1 & \bar{T}_2 & \cdots & \bar{T}_m & \bar{h} \end{pmatrix}$$

Step 8: Now the receiver A verify the checksum to check the following:

$$\bar{T}_i = \prod_{j=1}^{n} \bar{t}_{ij} * p_j \bmod N_B\ , for\ 1 \le i \le m$$

$$\bar{T}_j = \prod_{i=1}^{m} \bar{t}_{ij} * q_i \bmod N_B\ , for\ 1 \le j \le n$$

$$\bar{h} = \prod_{j=1}^{n} \left(\prod_{i=1}^{m} \bar{t}_{ij} \bmod N_B \right) \bmod N_B$$

If the verifications are positive, then the receiver believes that the message was not altered during the transmission.

Step 9: The receiver A takes the transpose of the matrix which will result in message as follows:

$$\bar{X} = \begin{pmatrix} \bar{t}_{11} & \bar{t}_{21} & \cdots & \bar{t}_{m1} \\ \bar{t}_{12} & \bar{t}_{22} & \cdots & \bar{t}_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{t}_{1n} & \bar{t}_{2n} & \cdots & \bar{t}_{mn} \end{pmatrix} = \begin{pmatrix} \bar{x}_{11} & \bar{x}_{12} & \cdots & \bar{x}_{1m} \\ \bar{x}_{21} & \bar{x}_{22} & \cdots & \bar{x}_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{x}_{n1} & \bar{x}_{n2} & \cdots & \bar{x}_{nm} \end{pmatrix}$$

5. SECURITY ANALYSIS

The proposed scheme further provides extra security and speed improvements by making use of transpose matrix and improve the decryption side of RSA. If an intruder appearance into the message he can realize it difficult to know or calculate checksum/ hash value therefore it'll confuse the intruder. Hence this is often a really smart solution for eavesdropping drawback.
Next, we show that our scheme is heuristically secured by considering the following attacks [8].

Common Modulus Attack: The common modulus attack (CMA) [8] can be occurred by using the same modulus n, when the same message X is encrypted twice and by that attack one can retrieve the message X algorithm. The CMA is applicable in Iuon-Chang Lei et. al [3] scheme method because it uses the encryption and decryption as same as original RSA. In the proposed scheme using a unique integer k by that there are two cipheretext generated and it appears to be impractical to apply that attack on proposed scheme.

Chosen Cipher Text Attack: Chosen-cipher text attack (CCA) [9] is possible in RSA due to the multiplicative property of the modular arithmetic [10] following by RSA. That means product of the two cipher texts is equal to the encryption of the product of the corresponding plaintexts. The CCA is applicable in both original RSA algorithm, and in the proposed one, but by applying CCA on the proposed scheme for getting the value of message X, it appears to be complex and more time consuming as compared to the original RSA algorithm.

Timing Attack: An attacker can determine the value of the private key by maintaining the track of how much time a computer takes to decrypt the encrypted message this because of Timing attack that occurs at RSA implementation Kocher [11]. Timing attack is applicable in majority digital signature fault tolerant schemes based on original RSA algorithm because by measuring the time for encryption and decryption, and time for key generation one can determine the value of the secrete key exponent d, but in the proposed scheme by using a random unique integer k in both the encryption and decryption process makes it difficult to distinguish between the time for public key e or private key d and the time for k.

Known Plain-Text Attack: If the attacker has known some quantity of plaintext and corresponding ciphertext, this will refer to known-plaintext attack [12]. The known-plaintext attack deals with the some known plaintext corresponding to the ciphertext and it is applicable in the digital signature with fault tolerance based on the original RSA algorithm. But it seems to be impractical in the proposed scheme because here, generating the two ciphertexts for the one particular plaintext and if it is applicable to the proposed scheme, it is very difficult to get the value of particular plaintext by applying these attacks.

6. CONCLUSION

The proposed scheme described in the paper is an attempt to provide a speed improvement on the decryption side of digital signature scheme fault tolerance based on improving the RSA algorithm using the concept of the Chinese remainder theorem. The algorithm for the proposed scheme can protect us from several common attacks. Further, it provides extra security measures by making use of transpose matrix of the original message.

REFERENCES

[1] C.N. Zhang, “Integrated Approach for Fault Tolerance and Digital Signature in RSA,” IEEE Proceedings-Computers & Digital Techniques, vol. 146, no. 3, pp. 151-159, 1999

[2] N. Lee and W. Tsai, “Efficient Fault-tolerant Scheme basd on the RSA system,” IEEE Proceedings – Computer and Digital Techniques, vol. 150, no. 1, pp. 17-20, 2003.

[3] Iuon-Chang Lin and Hsing-Lei Wang, “An Improved Digital Signature Scheme with Fault Tolerance in RSA”, Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE, 2010

[4] Shreenath Acharya, Sunaina Kotekar, Seema S Joshi, Shradda Shetty and Supreetha Lobo,” Implementing Digital Signature based Secured Card System for Online Transactions”, International Journal of Computer Applications 65(24):27-32, March 2013.

[5] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-key Cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[6] Nikita Somani and Dharmendra Mangal, “An Improved RSA Cryptographic System”, International Journal of Computer Applications 105(16):18-22, November 2014.

[7] A. H. Al-Hamami and I. A. Aldariseh, "Enhanced Method for RSA Cryptosystem Algorithm," IEEE International Conference on Advanced Computer Science Applications and Technologies, pp. 402-408, 2012.

[8] D. Boneh, "Twenty Years of Attacks on the RSA Cryptosystem," Notices of the AMS, vol. 46, no. 2, pp. 203-213, 1999.

[9] Y. Desmedt and A. M. Odlyzko, "A Chosentext Attack on RSA Cryptosystem and some Discrete Logarithm Schemes," Advances in Cryptology CRYPTO ’85, vol. 218, pp. 5116-521, 1986.

[10] R. Kumar, "Security Analysis and Implementation of an Improved Cch2 Proxy Multi-Signature Scheme," International journal of computer network and Information security, vol. 4, pp. 46-54, 2014.

[11] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," Advances in Cryptology-CRYPTO '96, pp. 104-113, 1996.

[12] R. C. Merkle, "Secure Communications over Insecure Channels," Communications of the ACM, vol. 21, no. 4, pp. 294-299, 1978.

AUTHORS

H. Elkamchouchi obtained his B.Sc Electrical Communication Engineering - Excellent with First Class Honors - Faculty of Engineering – Alexandria University - June 1966, Master Communications Engineering (specialization accurate: antennas and propagation) Faculty of Engineering – Alexandria University - September 1969, B.Sc of Science in Applied Mathematics - Excellent with honors - Britain's Royal College of Science - University of London - England - August 1970, Doctor Communications Engineering (specialization accurate: antennas and propagation) - Faculty of Engineering - Alexandria University - March 1972. He work Professor Emeritus, Faculty of Engineering, Alexandria University from September 2003 until now.

Heba Gaber held a Masters' of science in Electrical Engineering from Faculty of Engineering, Arab Academy for Science and Technology. She works on Arab Academy for Science and Technology. She studies for Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.

Fatma Ahmed held a Masters' of science in Electrical Engineering from Faculty of Engineering, Alexandria University. She works on Alexandria Higher Institute of Engineering and Technology. She Held a Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.

Dalia ElKamchouchi held a Masters' of science in Electrical Engineering from Faculty of Engineering, Alexandria University. She works on Alexandria Higher Institute of Engineering and Technology. She Held a Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University.

IMPROVING SCHEDULING OF DATA TRANSMISSION IN TDMA SYSTEMS

Timotheos Aslanidis[1] and Leonidas Tsepenekas[2]

[1]National Technical University of Athens, Athens, Greece
taslan.gr@gmail.com
[2]National Technical University of Athens, Athens, Greece
ltsepenekas@corelab.ntua.gr

ABSTRACT

In an era where communication has a most important role in modern societies, designing efficient algorithms for data transmission is of the outmost importance. TDMA is a technology used in many communication systems such as satellites and cell phones. In order to transmit data in such systems we need to cluster them in packages. To achieve a faster transmission we are allowed to preempt the transmission of any packet in order to resume at a later time. Such preemptions though come with a delay in order to setup for the next transmission. In this paper we propose an algorithm which yields improved transmission scheduling. This algorithm we call MGA. We have proven an approximation ratio for MGA and ran experiments to establish that it works even better in practice. In order to conclude that MGA will be a very helpful tool in constructing an improved schedule for packet routing using preemtion with a setup cost, we compare its results to two other efficient algorithms designed by researchers in the past.

KEYWORDS

Communication networks, setup delay, preemption, packet routing

1. INTRODUCTION

In the course of the last fifty years technological and scientific evolution has lead to an era of vast information and the need for fast and efficient communication. In the framework of enhancing communication network performance and dissemination of information researchers have introduced the Time Division Multiple Access (TDMA) technology. TDMA technology has been for decades a cornerstone of the global network infrastructure, as it plays an important role in many different communication systems.

To be more precise:

- Most 2G cellular systems are TDMA based. The GSM (Global System for Mobile Communications) currently accounts for approximately 80% of the subscribers worldwide. Many other 2G systems use TDMA technology among which are Personal Digital Cellular (PDC), the Digital Enhanced Cordless Telecommunications (DECT) standard for portable phones and PHS. Surprisingly enough 2G systems are not at all obsolete. They are still often used independently or in co-existence with the newest 3G and 4G systems.

Natarajan Meghanathan et al. (Eds) : ICAIT, CRYPIS, NC, ITCSE-2016
pp. 45–53, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60705

- TDMA technology is used in some 3G cellular systems such as the Universal Mobile Telecommunications System (UMTS).

- TDMA technology is also still used in satellite systems, in combat-net radio systems and in the Passive Optical Networks (PON).

TDMA based systems aim in transmitting data between multiple sender and receiver stations in packages simultaneously. While trying to reduce the time frame, preemption of a transmission is allowed in order to send the remaining parts of the messages at a later time with a newly scheduled package. Yet, in order to ready for the next package's transmission there is a setup cost which results in delaying the overall data transmission. Figure 1 depicts how a TDMA based technology transmission might work. This problem is referred to in bibliography as the MINSWT problem in case the number of frequencies does not suffice to serve all stations at once. In case the number of frequencies is at least as large as the number of senders as well as the number of receivers the problem is referred to as PBS. In this paper we handle the later. To this end we have designed a near optimal algorithm with an efficient approximation ratio. We have provided a proof for that approximation ratio and compared it to two other efficient algorithms handling the same problem. One which minimizes the number of packets and one which has the best approximation proven in bibliography so far.

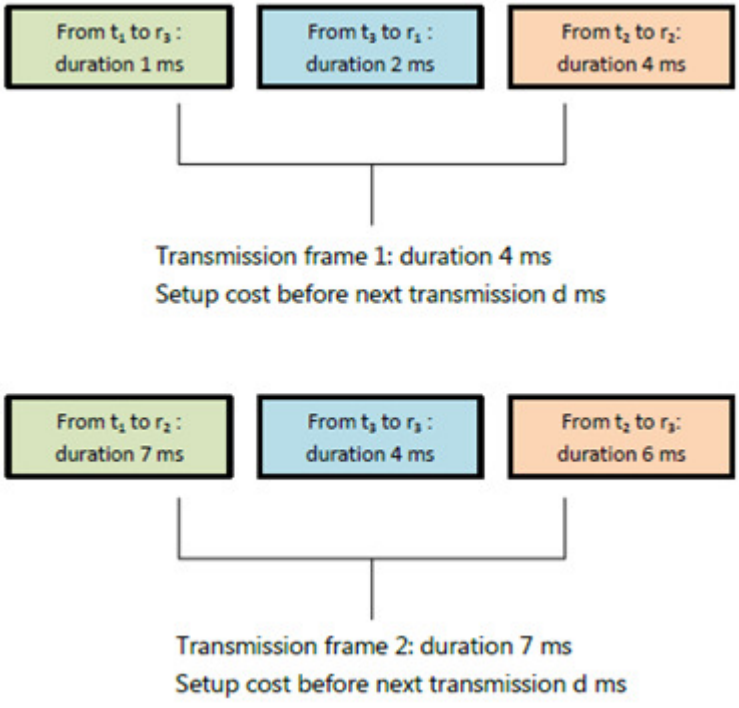

Figure 1. TDMA transmission in a 3-source:(t_1,t_2,t_3) , 3-receiver:(r_1,r_2,r_3) system.

2. GRAPH REPRESENTATION AND NOTATIONS

For the purposes of our research we will represent an input instance by a bipartite graph G(V,U,E,w). V will denote the transmitters, U will stand for receivers, whereas the set of edges will comprise the information about data traffic through the TDMA system. The weight w(v,u),

assigned to each edge e=(v,u), $v \in V$, $u \in U$ is the time required for the full transmission of each message.

Furthermore the following notation will be used: $\Delta=\Delta(G)=\max\{\max_{v\in V}(\deg(v)), \max_{u\in U}(\deg(u))\}$, that is, Δ will denote degree of the bipartite graph which in practice equals to the maximum number of messages to be transferred from or to any of the stations.

$W=W(G)=\max\{\max_{v\in V}\{\sum_{u\in U} w(v,u)\}, \max_{u\in U}\{\sum_{v\in V} w(v,u)\}\}$, that is W will denote the maximum total weight of all the edges adjacent to any of the nodes. This in turn equals to the maximum total workload of any station.

$d \in Z^{*}_{+}$ will denote the setup delay, namely the time required so that the next transmission may begin.

The objective function to be minimized is $F(G,d)=\sum_{i=1}^{N} t(M_i) + d \cdot N$, where N is the number of distinct transmissions in order to transfer the entire data workload and $t(M_i)$ is the time required for the completion of a specific transmission M_i.

Since transmission cannot be concluded before the maximum workload of any station is scheduled and the number of transmissions will be at least as many as the messages to be sent or received by any station, a lower bound to the optimal solution is $LB=W+d \cdot \Delta$. Yet, this lower bound is not always achievable as shown in [6].

3. PREVIOUS RESEARCH

As shown in [4], PBS is 4/3-ε inapproximable for any ε>0, unless P=NP. Even though the problem is NP-Hard there do exist special cases of input for which the optimal solution can be found in polynomial time ([1], [4], [5], [6]). The best approximation ratio proven so far is $2-\frac{1}{d+1}$ by the authors of [1]. Experiments have been ran by many researchers to test the output of various algorithms proposed in [2], [4], [5], [6], [10] and [12].

The performance of our newly presented algorithm will be compared to that of two algorithms found in bibliography:

- The algorithm presented in [8] which we will refer to as GWA (Gopal-Wong Algorithm). GWA calculates exactly Δ matchings, corresponding to Δ transmission packages. GWA will always achieve the minimum number of switchings and in order to produce a competitive transmission time for each package, the matchings are constructed so that edges of similar weight are grouped together. GWA has been tested in experiments in [6] and appears to perform well when the value of d increases significantly compared to duration of the messages. Unfortunately it has an unbounded approximation ratio as shown also in [6].

- A-PBS(d+1) as described in [1], preempts each edge to a multiple of d+1 and repeatedly computes matchings that correspond to transmission packets. Until now A-PBS(d+1) is the only algorithm that has a proven approximation ratio strictly less than 2. Yet, in most cases it produces schedules with makespan undesirably larger than the optimal.

Table 1. Summary of the 3 algorithms comparison: GWA, A-PBS(d+1), MGA

Algorithm	Approximation ratio	Experimental results' conclusions
GWA	Unbounded	Works well only for large values of d and works undesirably bad for specific instances regardless the value of d.
A-PBS(d+1)	$2-\frac{1}{d+1}$	Often produces results with more than 50% deviation from the optimal.
MGA	Δ+1	Produces efficient schedules on average as well in the worst case scenario regardless the input.

Our newly developed algorithm, which we call MGA aims in mitigating these disadvantages of WGA and A-PBS(d+1). MGA tackles GWA's disadvantage, namely the fact that there are instances for which GWA produces a solution of unbounded approximation ratio and in addition it produces schedules that are on average a lot close to the optimal than those produced by A-PBS(d+1). Table 1 illustrates all of the above.

4. MGA: AN IMPROVED ROUTING ALGORITHM FOR DATA TRANSMISSION IN TDMA SYSTEMS

For the purposes of this paper we have designed an algorithm aiming in mitigating the disadvantage of GWA, namely an algorithm with a bounded approximation ratio. We will refer to this algorithm as MGA (MultiGraph Algorithm), as the main concept in order to achieve a bounded approximation ratio is to split each edge of undesirably large weight into smaller edges to be handled and scheduled independently.

The MultiGraph Algorithm (MGA)

Step1: Split each edge of weight more than $\left\lfloor \frac{W}{\Delta} \right\rfloor$ in parts each having weight no more than $\left\lfloor \frac{W}{\Delta} \right\rfloor$. The splitting will be done in the following way: Split each edge $e \in E$ with weight w(e) into at most $\left\lfloor \frac{w(e)\Delta}{W} \right\rfloor$+1 edges the weight of each of which will be $\left\lfloor \frac{W}{\Delta} \right\rfloor$ except perhaps for the last one which will weigh $w(e)-\left\lfloor \frac{w(e)\Delta}{W} \right\rfloor \cdot \left\lfloor \frac{W}{\Delta} \right\rfloor = w(e) \text{ MOD } \left\lfloor \frac{W}{\Delta} \right\rfloor$.Thus G will become a multigraph.

Step 2: Add nodes and edges to the multigraph in order to make it a regular multigraph. Each newly added edge e, will have w(e)=0.

Step 3: Compute a perfect matching for the regular multigraph and schedule the corresponding parts of the edges of this matching for transmission.

Step 4: Remove the edges corresponding to the previous transmission from the multigraph.

Step 5: repeat steps 3 and 4 until $E=\varnothing$.

Theorem1: MGA's approximation ratio is bounded by Δ+1.

Proof: In the multigraph constructed by steps 1 and 2 the maximum edge weight is $\left\lfloor \frac{W}{\Delta} \right\rfloor$. Therefore the cost of each transmission will not exceed $\left\lfloor \frac{W}{\Delta} \right\rfloor$. The multigraph's degree is at most $\Delta' \leq (\left\lfloor \frac{w_{max} \cdot \Delta}{W} \right\rfloor + 1) \cdot \Delta$ since there can be at most Δ edges to be split and each will be split in $\left\lfloor \frac{w_{max} \cdot \Delta}{W} \right\rfloor + 1$ parts, where w_{max} is the maximum weight of any edge in the graph. Step 2 ensures that each node has degree Δ′ and that removing the edges of a perfect matching from G will reduce the graph's degree by exactly one after each iteration. Thus the number of terations will be Δ′. Therefore the cost C of the entire process to transmit all data will be bounded by:

$$C \leq (\left\lfloor \frac{w_{max} \cdot \Delta}{W} \right\rfloor + 1) \cdot \Delta \cdot \left\lfloor \frac{W}{\Delta} \right\rfloor + d \cdot \Delta' \leq (\left\lfloor \frac{w_{max} \cdot \Delta}{W} \right\rfloor + 1) \cdot \Delta \cdot \left\lfloor \frac{W}{\Delta} \right\rfloor + d \cdot (\left\lfloor \frac{w_{max} \cdot \Delta}{W} \right\rfloor + 1) \cdot \Delta$$

Taking into account that $w_{max} \leq W$, $\lfloor a \rfloor \leq a$, for all $a \in \boldsymbol{Q}$ we conclude that

$$C \leq (\frac{W \cdot \Delta}{W} + 1) \cdot \Delta \cdot \frac{W}{\Delta} + d \cdot (\frac{W \cdot \Delta}{W} + 1) \cdot \Delta = (\Delta+1) \cdot W + d \cdot (\Delta+1) \cdot \Delta = (\Delta+1) \cdot (W + d \cdot \Delta)$$

Which implies that $C \leq (\Delta+1) \cdot LB$, thus bounding MGA's approximation ratio by Δ+1

5. RUNNING TEST CASES TO EVALUATE THE PERFORMANCES OF THE THREE ALGORITHMS

One thousand test cases have been ran for a 50 source-50 destination system for values of setup cost varying from 0 to 100 and message durations varying from 0 to 100. We have to point out that since PBS is an NP-Hard problem, calculating an optimal schedule is inefficient therefore to estimate the approximation ratio we have used the lower bound to the optimal solution which is $W+\Delta \cdot d$.

Figure 2 establishes that MGA works better than GWA not only in the theoretical sense that theorem 1 implies but also in practice as well. We ran both algorithms using as input the "bad" instance presented in [6]. MGA will still yield an approximation ratio lower than 2 and will regardless the value of d perform better than GWA. We thereof have established that our newly presented algorithm will perform well, even for the worst transmission scenario.

Figure 3 presents the worst performance of MGA. It suggests that even though our proven approximation is Δ-dependent, in practice MGA will not exceed an approximation ratio of 2 or even less. In fact MGA's (worst case/lower bound) will in no case exceed 1.55. Furthermore MGA's worst performance for any instance does not fluctuate much from its average performance, making it a stable and reliable tool for constructing an efficient schedule for the problem at hand.

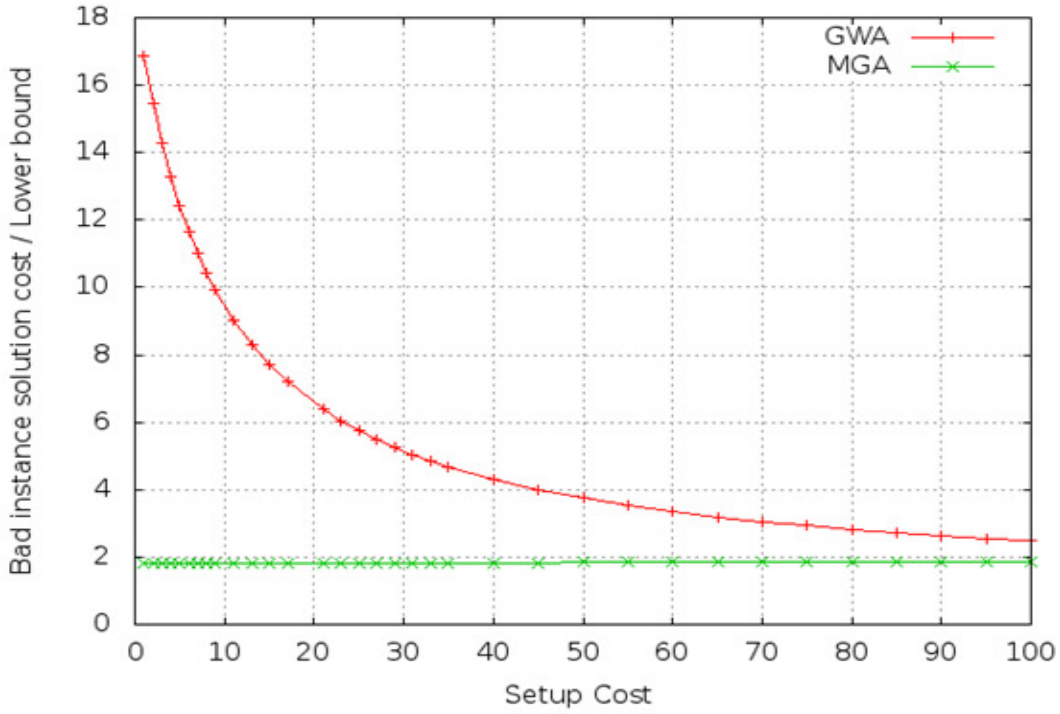

Figure 2. Solution cost/lower bound comparison of GWA and MGA for a single "bad" instance.

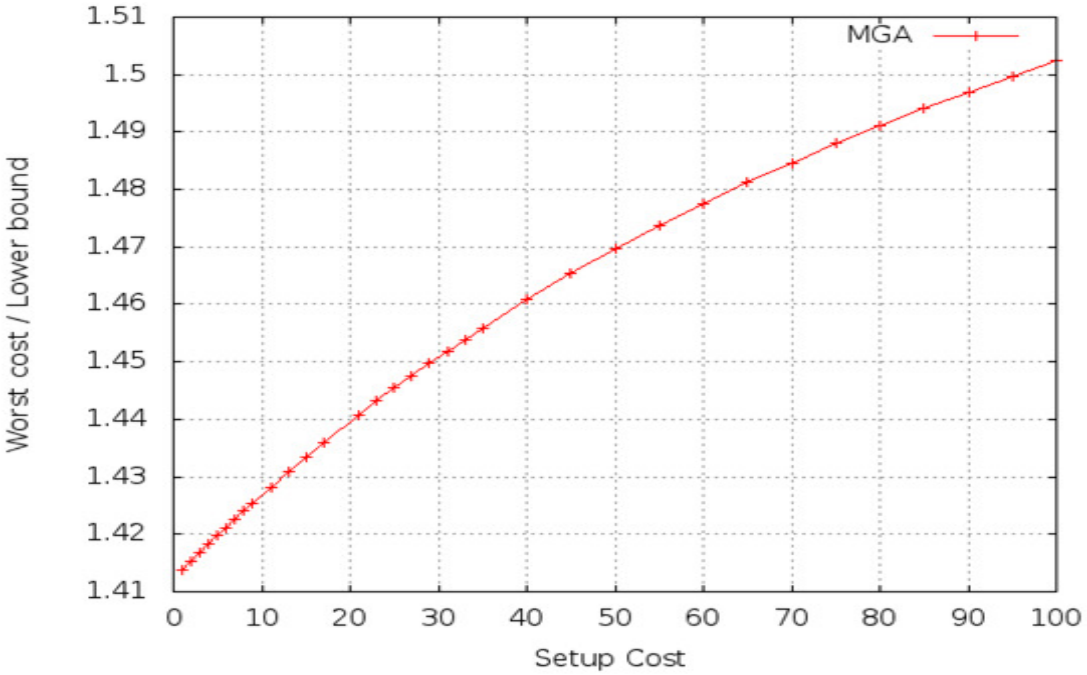

Figure 3. worst performance of MGA

Figure 4 compares MGA with A-PBS(d+1). A-PBS(d+1) will perform better only for very small values of d and even though it has a better approximation ratio, MGA produces a lot better results as d's value increases.

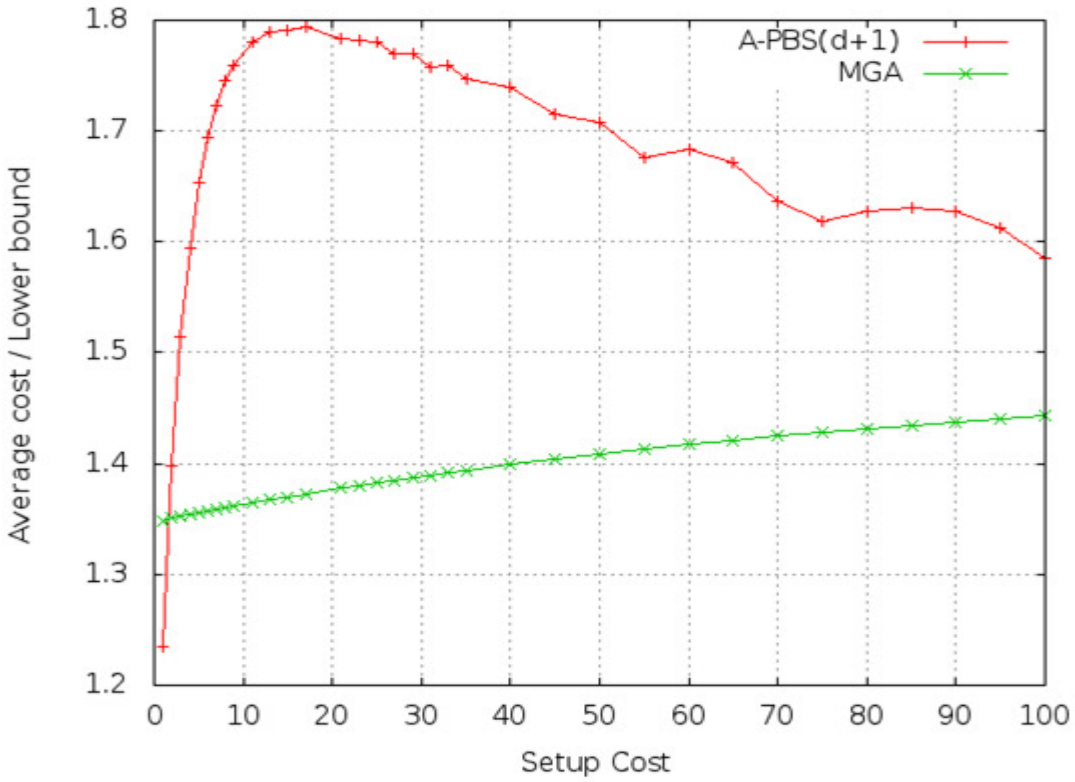

Figure 4: Average cost/lower bound comparison of A-PBS(d+1) and MGA

6. CONCLUSIONS AND FUTURE WORK

In this paper we have presented MGA, a Δ+1- approximation algorithm for the problem of transmitting data packages through a TDMA based communication system. Furthermore, we ran experiments to establish how efficient MGA is in practice. Experiments suggest that it might be possible to prove a better approximation ratio than Δ+1. That approximation ratio may even be less than two. We compared MGA with two algorithm found in bibliography. One which achieved the minimum number of preemtions and another which has the best approximation ratio proven so far, to establish that MGA works even better in practice. Yet, in order to prove MGA's approximation ratio we designed MGA so that it forcefully preempts transmission numerous times resulting in a schedule burdened by many delays. Future work might also suggest of a way to reduce the number of those preemptions leading to even better experimental results or even a proof for a lower approximation ratio.

REFERENCES

[1] F. Afrati, T. Aslanidis, E. Bampis, I. Milis, Scheduling in Switching Networks with Set-up Delays. Journal of Combinatorial Optimization, vol. 9, issue 1, p.49-57, Feb 2005.

[2] T. Aslanidis, M.E. Kogias, Algorithms for Packet Routing in Switching Networks with Reconfiguration Overhead. In Proceedings, Second International Conference on Computer Science and Engineering (CSE-2014), April 2014.

[3] G. Bongiovanni, D. Coppersmith and C. K.Wong, An optimal time slot assignment for an SS/TDMA system with variable number of transponders, IEEE Trans. Commun. vol. 29, p. 721-726, 1981.

[4] J. Cohen, E. Jeannot, N. Padoy and F. Wagner, Messages Scheduling for Parallel Data Redistribution between Clusters, IEEE Transactions on Parallel and Distributed Systems, vol. 17, Number 10, p. 1163, 2006.

[5] J. Cohen, E. Jeannot, N. Padoy, Parallel Data Redistribution Over a Backbone, Technical Report RR-4725, INRIA-Lorraine, February 2003.

[6] P. Crescenzi, X. Deng, C. H. Papadimitriou, On approximating a scheduling problem, Journal of Combinatorial Optimization, vol. 5, p. 287-297, 2001.

[7] I. S. Gopal, G. Bongiovanni, M. A. Bonucelli, D. T. Tang, C. K. Wong, An optimal switching algorithm for multibeam satellite systems with variable bandwidth beams, IEEE Trans. Commun. vol. 30, p. 2475-2481, Nov. 1982.

[8] I. S. Gopal, C. K. Wong Minimizing the number of switchings in an SS/TDMA system IEEE Trans. Commun. vol. 33, p. 497-501, 1985.

[9] T. Inukai, An efficient SS/TDMA time slot assignment algorithm IEEE Trans. Commun. vol 27, p. 1449-1455, Oct. 1979.

[10] E. Jeannot and F. Wagner, Two fast and efficient message scheduling algorithms for data redistribution over a backbone, 18th International Parallel and Distributed Processing Symposium, 2004.

[11] A. Kesselman and K. Kogan, Nonpreemptive Scheduling of Optical Switches, IEEE Transactions in Communications, vol. 55, number 6, p. 1212, 2007.

[12] M.E. Kogias, T. Aslanidis, A comparison of Efficient Algorithms for Scheduling Parallel Data Redistribution, International Journal of Computer Networks & Communications, May 2014, vol. 6, num. 3.

[13] K. S. Natarajan and S. B. Calo, Time slot assignment in an SS/TDMA system with minimum switchings IBM Res. Rep. 1981.

[14] B. Towles and W. J. Dally, Guaranteed Scheduling of Switches with Configuration Overhead, in Proc. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM '02. pp. 342-351, June 2002.

AUTHORS

Timotheos Aslanidis was born in Athens, Greece in 1974. He received his Mathematics degree from the University of Athens in 1997 and a master's degree in computer science in 2001. He is currently doing research at the National and Technical University of Athens in the School of Electrical and Computer Engineering. His research interests comprise but are not limited to computer theory, number theory, network algorithms and data mining algorithms.

Leonidas Tsepenekas was born in Athens, Greece in 1992. Currently, he is finishing his studies as an undergraduate student at the National Technical University of Athens. His main research interests focus on approximation, online and randomized algorithms

INTENTIONAL BLANK

MEASURING TECHNOLOGICAL, ORGANIZATIONAL AND ENVIRONMENTAL FACTORS INFLUENCING THE ADOPTION INTENTIONS OF PUBLIC CLOUD COMPUTING USING A PROPOSED INTEGRATED MODEL

Dr. Minimol Anil Job

Assistant Professor, ITC Department, Faculty of Computer Studies,
Arab Open University, Kingdom of Bahrain

ABSTRACT

The main objective of this research is to identify the factors influencing the intentions to adopt the public computing by the private sector firms. In this research the researcher examined the ten factors influencing the cloud computing adoption using a proposed integrated model which incorporates aspects of the Technology, Organization and Environment factors such as Complexity, Compatibility, Security Concerns, Trialability, Cost Saving, Top Management Support, Prior IT Experience, Organizational Readiness, Competitive Pressure and External Support. In order to test influencing factors a survey was conducted and one hundred and twenty two valid responses were received from IT decision makers from forty firms in different industries. The results revealed that the Compatibility, Cost Saving, Trialability and External Support are the main influential factors in the adoption intentions of public cloud computing. Future research could be built on this study by developing different model for each industry because each industry has unique characteristics that can influence the adoption of the technological innovations.

KEYWORDS

cloud computing, virtualization, security, Compatibility, Complexity, Trialability

1. INTRODUCTION

Due to the intense market competition and a rapidly changing business environment, firms have been driven to adopt various modern information technologies in order to improve their business operations and increasing their productivity [1]. Since the private sector firms are important players in each industry which significantly contribute to the economy's Gross domestic product and labor force, it is important to propose new strategies and technologies that can help

Natarajan Meghanathan et al. (Eds) : ICAIT, CRYPIS, NC, ITCSE-2016
pp. 55–66, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60706

the private sector firms to become more efficient and effective. The high cost of computing technologies is due to complex information architecture and infrastructure, and that will discourage the firms from adopting advanced IT services [2]. Based on that, one approach that helps the firms to enhance the productivity and being efficient is to invest in public cloud computing. . Cloud computing offers several benefits for enterprises. The cloud frees organizations from having to set up an IT infrastructure and allows them to rent resources and pay only for the services they use [3]. Yet, the emergence of cloud computing solves this problem by reducing direct expenses of information technology. For many firms, the adoption of public cloud computing became more beneficial as it can quickly add more capabilities to their IT systems without investing in new expensive infrastructure, buying or deploying new application systems, or training new IT personnel. The concerns related to the clients' data privacy and protection, problems with data separation in the cloud and long-term viability of the public cloud provider can negatively affect the firms' willingness to adopt the public cloud computing. Thus such firms are mostly hesitant to adopt the public cloud services. This research studied the factors that influence the adoption intentions of public cloud computing by the IT decision makers in the private sector firms using a proposed integrated model and the research aims to spot the light to the adoption intentions of cloud computing in a wide range of private sector firms from different industries, as well as contributing to the body of knowledge related to the factors of adoption.

2. METHODOLOGY

Public Cloud Computing is one of the emerging areas in the field of information technology. Cloud computing is considered in the second place after business intelligent on the list of the top five most influential technologies. However, despite the fact that the adoption of public cloud computing has been growing, its rate of acceptance remains practically very low in the developing countries to about 37% , and the rate expected to be even lower in the less developed countries as the case with most of the technological innovations [1]. Therefore, it is important to investigate the factors that affect the adoption intentions of public cloud computing by IT decision makers in the private sector firms. [4][5]The diagram below is a model proposed model to identify the factors influencing the public cloud adoption in the private sectors. The ten factors influence in the cloud computing adoption is examined in this research is using the proposed integrated model incorporates aspects of the Technology, Organization and Environment factors such as Complexity, Compatibility, Security Concerns, Trialability , Cost Saving, Top Management Support, Prior IT Experience, Organizational Readiness, Competitive Pressure and External Support [6][7].

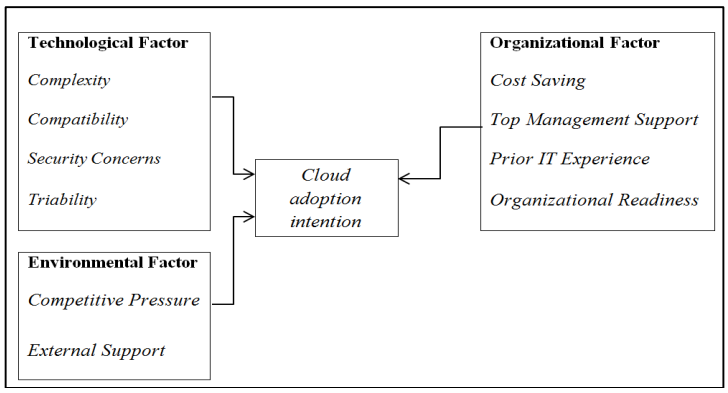

Figure1: A proposed model for cloud computing adoption

The main question of this research is "*What are the factors that influence the intentions in adopting public cloud computing in the private sector firms?"* with the following main objectives.

- Analyze the technological, organizational and environmental factors influencing the IT decision maker intentions to adopt public cloud computing in the private sector.

- Provide suggestions and recommendations for the firms and the service providers in order to increase the adoption rate of public cloud computing between the firms in the private sector.

The targeted population in this research is defined as "managers and professionals who are involved in the decision process for the adoption of a new information technology in large firms in the private sector"[10][11]. This measure taken in this research to avoid small and medium firms based on the assumption that the large firms have more knowledge about the cloud computing because they mostly have experience with its related technologies such as virtualization and utility computing. As part of this research the researcher measured the degree of satisfaction in the firms already adopted the cloud services. A list of 30 firms preferably known as leader firms in different industries have selected as the target population[8][9]. The senior personnel of the IT department in these firms were contacted to in identifying the relevant hypothetical respondents for this survey within their firms as the targeted sample. An online questionnaire survey was conducted among the participants.

3. DATA ANALYSIS

Respondents' Profile:

All the participants in this research are IT decision makers who are familiar with public cloud computing. In addition to the participants' job titles, the type of industry in which the firms conducted their business was also captured. In terms of the respondents' profile, the collected data indicated that 76% of the respondents were not adopting public cloud computing services in their firms, while 29 % were already adopting. Figure 3 views the respondents adoption status of public cloud computing.

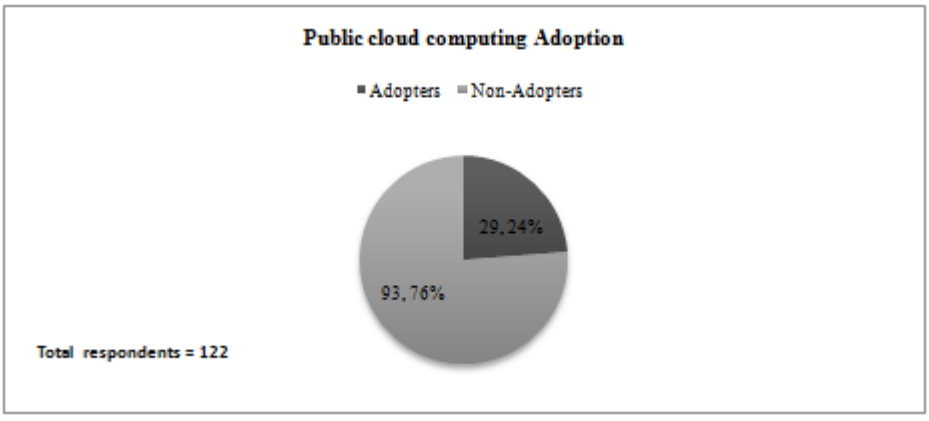

Figure 2: respondents' adoption status of public cloud computing

Technological Factors

Complexity:

As shown in Figure 3, only 27% of the respondents agreed with the fact that the work with cloud computing is complicated and about 26% agreed that the integration between their current IT infrastructure and cloud based services is difficult. At last, about 19% of the respondents agreed with the fact that administrating and monitoring the cloud based services are complex tasks.

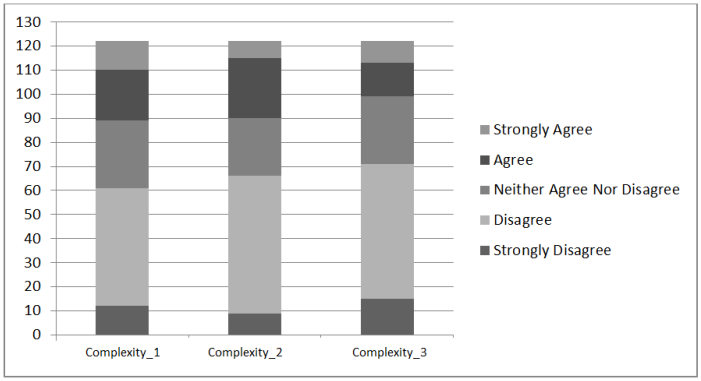

Figure 3: Analysis of respondents' perception about Complexity

Compatibility:

Using three questions, this construct measures the degree to which cloud computing is perceived as consistent with the existing infrastructure, culture and previous practices of the firms. As it can be viewed in Figure 4, about 66% of respondents think that cloud computing is compatible with the business model of their firms (Compatibility_1). More than 60% agreed that the adoption of cloud computing is compatible with the norms and culture of their firms (Compatibility _2). About 61% think that cloud computing is compatible with their current IT infrastructure (Compatibility _3).

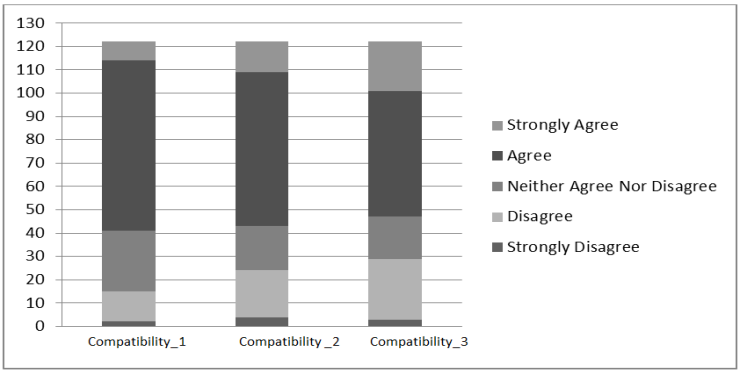

Figure 4: Analysis of respondents' perception about Compatibility

Security Concerns:

As shown in Figure 5, 46% of respondents think that it is unsecured to keep their business data in the Cloud providers' data center (Security_1). About 41% claim that it is unsecured to use the

cloud services over the internet to conduct their business' operations (Security_2), and 38.5% claim that the cloud computing concept does not satisfy their firms' security and privacy policies (Security_3).

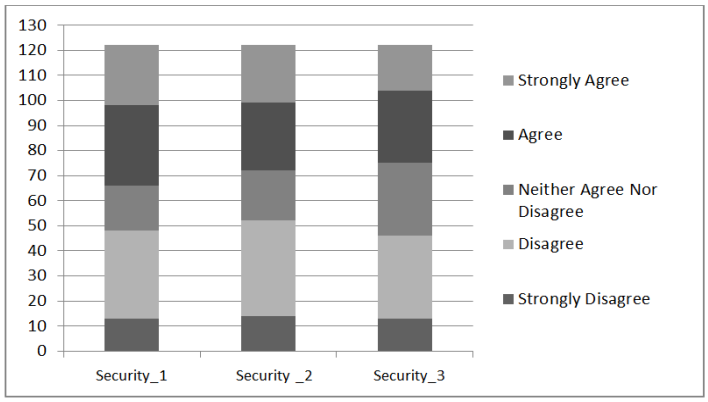

Figure 5: Analysis of respondents' perception about the security concerns

Trialability:

As shown in Figure 6, more than 70% of the participants think that before taking the adoption decision they will have the opportunity to use cloud computing services on a trial basis (Triability_1) and run partial integration test between the cloud applications and their existing system (Triability_2). Also, about 58% agreed that the cloud providers offer their services on a trial basis long enough to prove the platform capabilities and benefits (Triability_3).

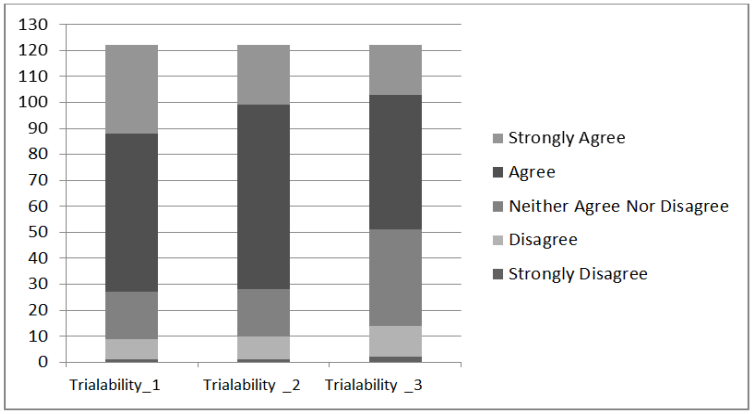

Figure 6: Analysis of respondents' perception about Perceived Trialability

Environmental Factors

Competitive Pressure:

Figure 7 depicted that more than 75% of the respondents perceive very intense competition within their industry. About 72% claimed that their competitors are always looking for the technological innovation to gain competitive advantages, and about 63% of respondents believe that cloud computing can enhance the competitive power of their firms.

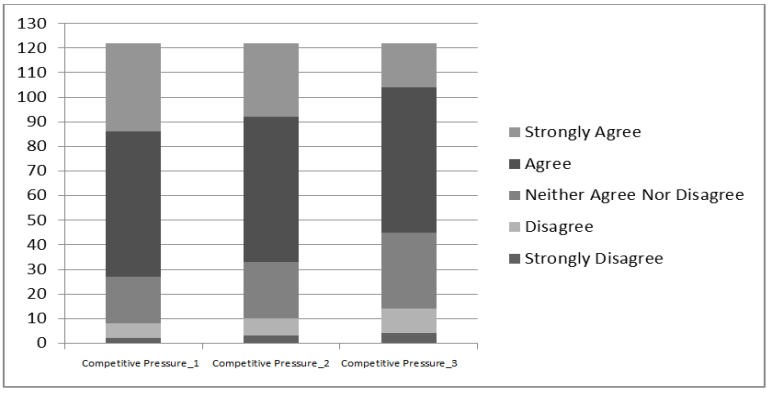

Figure 7: Respondents' perception about Competitive Pressure

External Support:

External support measured the participants expectations about the training program (External_Support_1); the technical support (External_Support_2); and the live support (hotline) provided by major cloud providers in the market (External_Support_3). Figure 8 shows the overall responses to each one. More than 80% of respondents believe that the level of external support delivered by cloud providers in each question either good, very good or excellent.

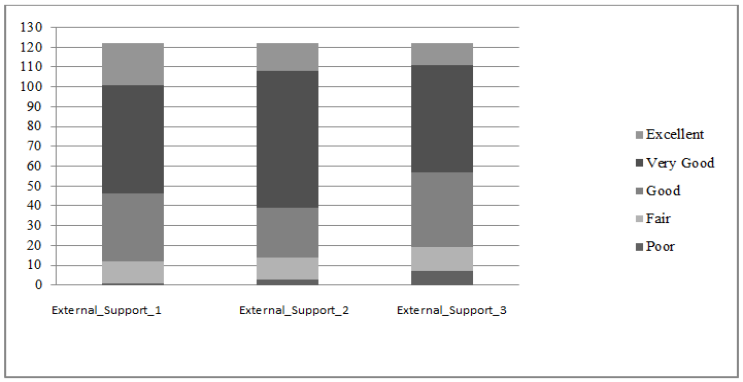

Figure 8: Analysis of respondents' perception about External Support

<u>Organizational Factors</u>

Cost Saving:

The participants opinion about the cost of adopting public cloud computing is measured from different perspectives. As it can be observed from Figure 9, about 77% think that the benefits of cloud computing are greater than the costs of its adoption (Cost_Saving_1). Around 73% agreed that acquiring applications systems through cloud computing is more economical than developing it in-house (Cost_Saving_2), and 62% of the participants think that adopting an application system via cloud computing is more economical than purchasing it as Off-the-Shelf (Cost_Saving_3).

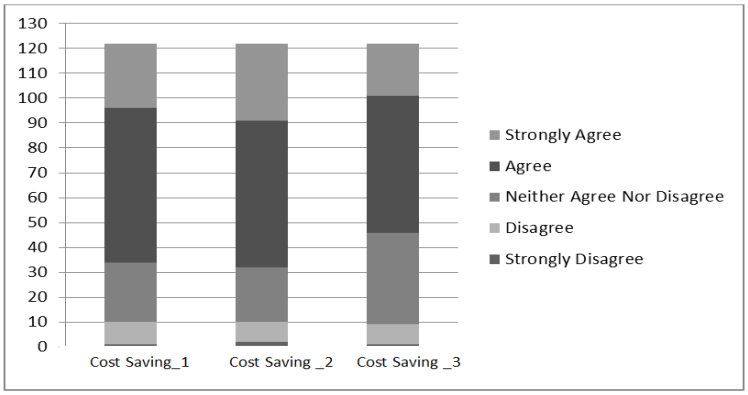

Figure 9: Analysis of respondents' perception about Cost Saving

Top Management Support:

Top management support is defined as the degree to which top management in the firm provides adequate resources and encourages the adoption of new technological innovations. As it can be viewed in Figure 10, about 70% agreed that their top management supports the implementation of the new technological innovations (Top_Mgt_Support_1) and provides strong leadership and engagements when it comes to the adoption of new technology (Top_Mgt_Support_2). At the same time, only 52% think that their top management is willing to take the responsibility of unfavorable consequences related to the adoption of the new technology (Top_Mgt_Support_3).

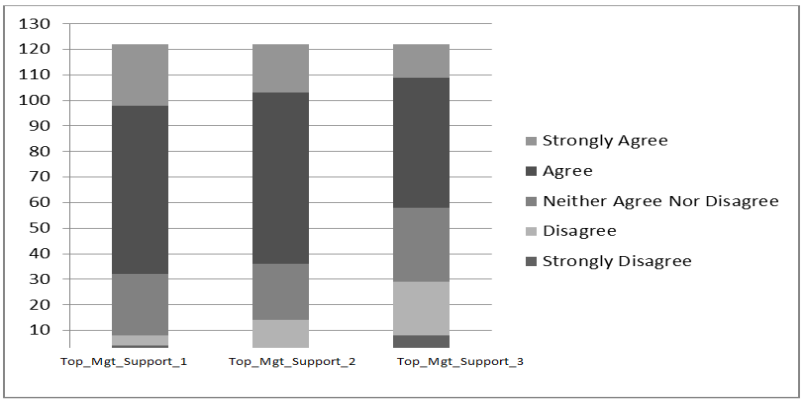

Figure 10: Analysis of respondents' perception about Perceived Top Management Support

Prior IT Experience:

Three questions were used to measures the firms' previous experience in the virtualization (Prior_IT Experience_1); Cluster computing (Prior_IT Experience_2); and Multi-Tenancy software architecture (Prior_IT Experience_3). Figure 11 shows that, 79% of the participants have enough experience in virtualization technology in their firms, 81% claimed that they have experience in cluster computing, and about 73% have experience in multi-tenancy software architecture.

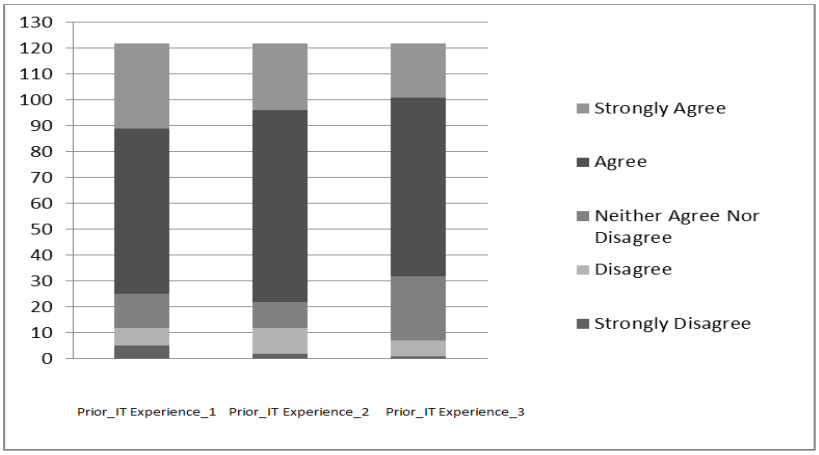

Figure 11: Analysis of respondents' perception about Prior IT experience

Organizational Readiness:

In this research the organizational readiness is defined as the degree to which the organization is technically and financially prepared to implement the cloud computing. As viewed in Figure 12, 72% of the participants claimed that their firms have sufficient financial resources to adopt cloud computing (Organizational_Readiness_1); 77% think that their firms have the technological resources to adopt cloud computing (Organizational_Readiness _2); and about 75% claimed that they have a qualified IT staff in order to adopt cloud computing (Organizational_Readiness _3).

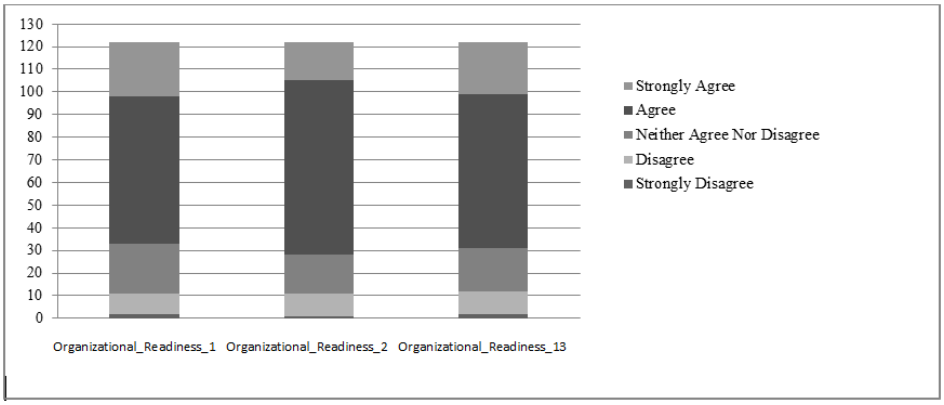

Figure 12: Analysis of respondents' perception about Organizational Readiness

Satisfaction Level:

For the participants who are already adopted the public cloud computing in their firms, we asked whether they are satisfied with the services received from cloud provider. As it can be seen in Figure 13, 79% (24 % + 55%) of participants are satisfied with the service they receive.

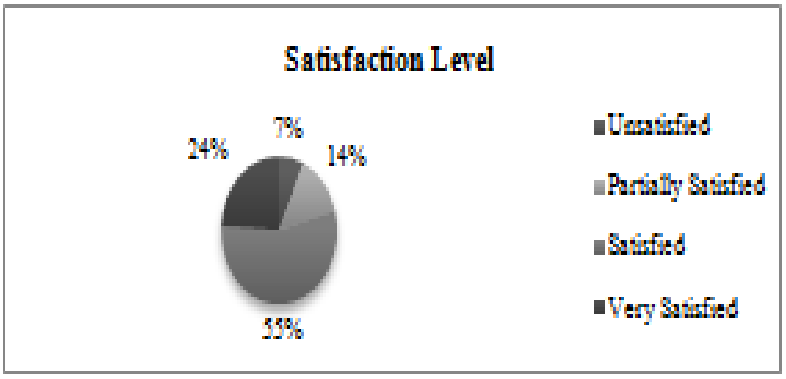

Figure 13: Cloud Adopters' Satisfaction

Adoption Intentions:

Only respondents, who have not adopted cloud computing yet, answered the questions related to the adoption intentions. The respondents asked whether the concept of cloud computing is acceptable in their firms (Adoption_Int_1); whether they recommend to use the cloud based applications in their firms in the future (Adoption_Int _2); whether they intent to adopt cloud computing in the coming two years (Adoption_Int _3); and whether they plan to adopt cloud computing in the next coming two years (Adoption_Int _4). As Figure 14 shows, about 72% of the non-adopters think that the concept of public cloud computing is acceptable in their firms and recommended the adoption of cloud based applications. Also, about 74% think that they should adopt (or plan to adopt) public cloud based applications in coming two years. Overall the intention to adopt public cloud computing is high.

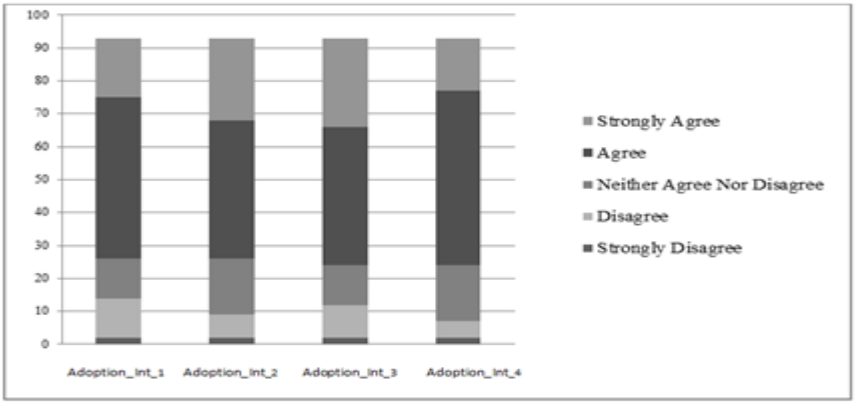

Figure 14: Analysis of non-adopters Intentions to adopt cloud computing

4. CONCLUSION

This research tries to increase the theoretical background about public cloud computing adoption in the private sector firms in the developing countries from different points of views by adopting a complete framework that incorporates Technological, Organizational and Environmental factors to examine the intentions adoption of cloud computing. This research demonstrates several key

findings about the factors influencing the adoption intentions of public cloud computing in private sector firms. These key findings are as follows:

- Four variables (Compatibility, Cost Saving, Trialability, and External support) were found to be significant determinants of public cloud computing adoption.

- Two variables (Organizational readiness, prior IT experience) were found to be positively related to the intentions to adopt the public cloud computing. However they have no significant impact.

- Three variables (Complexity, Security concerns and Competitive presser) were found to be negatively related to the intentions to adopt the public cloud computing but they have no significant impact.

- Among the determinants, Cost saving and External support were observed to be the most influential factor affecting the firm's adoption intentions.

According to the findings, there was no agreement between the participants on whether to consider the public cloud computing as secure or not. This resulted from the fact that the cloud computing concept still needs more time in order to prove its security capabilities and benefits to firms. Accordingly, when the firm is willing to adopt public cloud computing, it is better to start with services that do not mandates storing the critical business data in the provider's storage such as Virtual PBX phone service, Desktop as a Service, and Microsoft Office 365. [13][14] This will help the firm to be more knowledgeable about the capabilities exist within the cloud computing before implementing critical services such as ERP and CRM.

In order to be prepared for cloud computing, it is essential for the firm to optimize its network by installing intelligent load balancers in their infrastructure. Those devices allow the firm to manage, redirect and priorities the network traffic belong to mission-critical cloud applications when their bandwidth is under pressure, as well as allowing to scale up capacity over peak times. Also, it is important to analyze the existing IT assets to identify the tools that can re-use in the cloud without any modification and estimate how much effort (in terms of new development and deployment effort) will be required to integrate them with cloud based services before taking the adoption decision. [15][16]On the other hand, the cloud providers need to be aware of the concerns that firms experience when they make their adoption decision, such as cost saving, trialability and external support. The cloud providers should utilize various mass media in order to convince the firms that the migration to cloud-based system can help to dramatically reduce not only the fixed costs (such as licensing, hardware, software, storage, etc.), but also operating costs (such as cost of infrastructure administration, hardware and software maintenance, systems updates and upgrade, etc.) as well as training costs[17]. In addition, the service provider must arrange their services in order to be experimental. Giving the opportunity for the firms to try the services in experimental environment long enough to prove the platform capabilities and concept which more likely result an increase in the adoption rate. Although the of the majority participants in this research perceive the cloud services as more likely to be trialable ,it is necessary for service providers to make trialability more convenient and accessible. Furthermore, the cloud provides should support their clients according to a comprehensive service level agreement that assure high quality remote and onsite technical support[18]. That will allow the firms to obtain assistance for suspected defects and get valuable answers for task-oriented

questions related to the installation and operation of the currently acquired services. In addition, it is essential to maintain a 24/7 responsive support service, and to offer electronic access to the provider's technical support knowledgebase and technical product specialists.

5. RECOMMENDATIONS

Future research could be built on this study by developing different model for each industry other than a comprehensive one, because each industry has unique characteristics that can influence the adoption of the technological innovations. In addition, this research investigates only the large firms which in turn limit the ability to generalize the findings. Therefore, the future researches could investigate the small and medium-sized enterprises (SMEs) in addition to the large ones. In order to enhance the data quality in future researches, it is essential to conduct semi-structured interview in addition to the survey. This approach is useful in delving into business-related decision analysis and gives the opportunity for the researchers to interact directly with the decision-makers to clarify any misleading points related to the data collection instruments.

REFERENCES

[1] Empirical Analysis for the Factors Affecting the Adoption of Cloud Computing Initiatives by Information Technology Executives Journal of Management Research ISSN 1941-899X 2013, Vol. 5, No. 1

[2] A Complete History of Cloud Computing . (2012, January). Retrieved October 5, 2013, from SalesForce: http://www.salesforce.com/uk/socialsuccess/cloud-computing/the-complete-historyof-cloud-computing.jsp .

[3] Armando, F. (2011) "Cloud Computing—What's in it for Me as a Scientist?" Science (331)6016, p. 406.

[4] Barnhill, D.S. (2010) "Cloud Computing and Stored Communications: Another Look at Quon v. Arch Wireless," (Privacy Law) (Annual Review of Law and Technology), Berkeley Technology Law Journal (25), pp. 621–648.

[5] Bret, M. (2009) "In Clouds Shall We Trust?" IEEE Security & Privacy (7)5, pp. 3–3.

[6] Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud Computing: A Study of Infrastructure-as-a-Service .International Journal of Engineering and Information Technology, 60-63

[7] Behrand, T., Wiebe, E. N., London, J. E., & Johnson, E. C. (2010). Cloud computing adoption and usage in community colleges. Behaviour & Information Technology, 30(2), 231-240.

[8] Cloud Computing. (2013, January). Retrieved October 5, 2013, from Wikipedia, the free encyclopedia:http://en.wikipedia.org/wiki/Cloud_computing#History

[9] Choo , K. (2010) .Cloud computing: Challenges and future directions. Trends and Issues in Crime and Criminal

[10] Gupta, A., Pande, P., Qureshi, A. and Sharma, V. (2011). A proposed Solution: Data Availability and Error Correction in Cloud Computing. International Journal of Computer Science and Security, 5(4), 405-413.

[11] Katzan Jr., H. (2010c) "On the Privacy of Cloud Computing," International Journal of Management and Information Systems (14)2, p. 1

[12] Motta, G., Sfondrini, N. and Sacco, D. (2012), "Cloud Computing: A Business and Economical Perspective," 2012 International Joint Conference on Service Sciences, Ieee, pp. 18–22.

[13] McKendrick, J. (2011). Cloud bursts onto the enterprise mainstream. Database Trends and Applications, December, pp. 2-5.

[14] Ministry of industry and commerce, 2013; TAMKEEN , 2013

[15] Misra, S.C. and Mondal, A. (2010), "Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding return on investment", Mathematical and Computer Modelling, Vol. 53, pp. 504-21

[16] Pandey, S., W. Voorsluys, S. Niu, A. Khandoker, and R. Buyya (2011) "An Autonomic Cloud Environment for Hosting ECG Data Analysis Services," Future Generation Computer Systems(28)1, pp. 147-154, doi:10.1016/j.future.2011.04.022.

[17] R. Buyya, C. S. Yeo, S.Venugopal, J.Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype and reality for delivering computing as the 5th utility," Future Gener.Comput. Syst.,vol. 25, pp. 599–616, 2009

[18] Singh, B., 1 October 2011. Cloud Deployment Models – Private, Community, Public, Hybrid with Examples. Techno-Pulse. Available from: http://www.techno-pulse.com/2011/10/cloud-deployment-private-public-example.html [Accessed 7 October 2013].

AUTHOR

Dr Minimol Anil Job is working as an Assistant Professor in ITC Department, in AOU Bahrain Branch. She has more than ten tears of academic experience in the field of computer science and information technology. Her current research interests include Information Technology Management in the specialist area of Database management. She is a certified DBA (MS SQL). She has published several papers in the area of educational technology, e-learning, cloud computing and green computing in international journals. Her further area of interest is software development. She is invloled in many acadmic committees and also working as the Program Coordinator of Information Technology Department in AOU Bahrain Branch.

EMPLOYEES CHARACTERISTICS IN KNOWLEDGE TRANSFER AND PERFORMANCE

Saide[1], Hsiao-Lan Wei[2], Apol Pribadi Subriadi[3], Okfalisa[4], Nurul Aini[5], and Nesdi Evrilyan Rozanda[6]

[1]Department of Information Management, National Taiwan University of Science and Technology (NTUST), Taiwan. Department of Information System, Institute Technology of Sepuluh Nopember (ITS), Surabaya, Indonesia.
saidefc@gmail.com
[2]Department of Information Management, National Taiwan University of Science and Technology (NTUST), Taiwan.
hlwei@cs.ntust.edu.tw
[3]Department of Information System, Institute Technology of Sepuluh Nopember (ITS), Surabaya, Indonesia
apol@is.its.ac.id
[4]Department of Informatics Engineering, State Islamic University of Sultan Syarif Kasim Riau (UIN Suska Riau), Riau, Indonesia.
okfalisa@gmail.com
[5]Department of Information System, Diponegoro University, Semarang, Indonesia.
Nuruldotaini@gmail.com
[6]Department of Information System, State Islamic University of Sultan Syarif Kasim Riau (UIN Suska Riau), Riau, Indonesia.
nesdiev@yahoo.com

ABSTRACT

While most studies are concerned with the industry, but for non-profit organizations has not received much attention. Various have highlighted KS for creates value, however an obstacle from the perspective among employees still exists. The main problem is still difficult because employees will not share their knowledge. This study investigated factors and develop that influence KS among employees of non-profit organizations in Indonesia. The survey 364 respondents were used, 325 were returned, and 39 were not returned. Likert and smart PLS to confirm construct. This paper conclude factors that helping others, trust, soft reward, and personality of employees motivation are factors which influencing the KS behaviour. Finally, the findings were discussed.

KEYWORDS

Knowledge Management (KM), Knowledge Transfer, Knowledge Performance, Smart PLS, Employees Characteristics, Indonesia.

1. INTRODUCTION

Strategic plan each companies may impacts to progress and setbacks performance of the company. This is determined by seriously support from peoples at all level in company. Therefore, the maximizing transfer all resources together (employees and knowledge) that

Natarajan Meghanathan et al. (Eds) : ICAIT, CRYPIS, NC, ITCSE-2016
pp. 67–81, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60707

possessed must be closely connected with the presence from employees contribution in knowledge practice.

Based on the data from the Delphi Research Group that nearly 50% of 100% of organizational knowledge stored in the mind of their employees [1].That is to say, in the future the company needs to seriously attention for how to capture existing assets in the minds of their employees to be shared other employees and to achieve business objectives.

According to [2], knowledge transfer is a process where individual exchange his or her knowledge and ideas through discussions to create new knowledge or ideas. For individual employees, knowledge transfer is talking to colleagues to help them get something done better, more quickly, or more efficiently. Knowledge transfer can helps employees to new understanding their jobs and bring personal recognition within the department. Knowledge transfer include employee willingness to communicate actively with colleagues (i.e. donate knowledge), and actively consult with colleagues to learn from them (i.e. collect knowledge)

However, this is not always easy, because it is still embedded paradigm that tangible assets are always given more attention, while the capacity and scientific (intangible assets) actors rarely get more servings. In fact, if the long-term of mind-set puts forward that the challenge for productivity of all resources can be productively together.

A critical problem regarding the knowledge base in an organization is making employees willing to transfer knowledge from an employee to other employees or to the organization. This problem arises from the employee himself or the organization climate. An employee may be anxious that he will lose his power or value by transfer his knowledge.

Individuals do not always willing to share their knowledge and they may not be willing to share as much as the organization would like them to. It is important to understand when people are willing to share their knowledge and how an organization can facilitate this type of behaviour from both research and practical standpoint.

This is important because it is still crucial to accurately explain the knowledge transfer behaviour of individual professional groups [3]. This idea is also in line with suggestions from previous studied stating that findings from current studies need to be expanded team and organizational level knowledge is influenced by the extent to which knowledge transfer occurs between employees [4]-[7].

Therefore, while reciprocation arguably has attracted most attention, the author believe there are other reasons that deserve further research attention. Most studies in the literature, relating to all aspects of KM, are concerned with the manufacturing industry, and non-profit in particular has not received much attention, especially in Indonesia. This study differs essentially from prior studies by examining existing factors of knowledge transfer in the context where the employees come from different culture in Indonesia's organizations.

2. LITERATURE REVIEW

Nowadays, the ability of individuals in organization to share their knowledge within them is identifying as one of the critical contributing factors for organizational competitiveness. Due to this reason, there is a need to study the factors that influence individual knowledge transfer behaviour in organizations.

Knowledge management (KM) is critical to the operation of modern organizations and has attracted much attention by the business world since the introduction of the concept by [5], [8]. It

can help businesses retain their valuable intangible assets that are keeping in the mind of their employees. Particularly, effective knowledge transfer among units of an organization has been one of the most important issues of KM.

According to [9], there are two benefits organization gained if the members in organization shared their knowledge. Firstly, valuable knowledge can be disseminating effectively and efficiently within the organization through the process of knowledge transfer. Secondly, the ability of individual knowledge to recognize the value of knowledge, assimilate it, and apply it in the commercial end, can be increase by knowledge transfer among individuals of an organization. Knowledge transfer offers an organization the potential for increased productivity as well as retention of intellectual capital, even after employees leave the organization, which is necessary for business that creates value added [10].

Previous researchers tried to found what the reason why the employee didn't to share them knowledge to other and have noted that firms can successfully promote a knowledge transfer culture not only by directly incorporating knowledge in their business strategy, but also by changing employee attitudes and behaviours to promote willing and consistent knowledge transfer, like mentioned by [11]-[13]. This is a crucial process for an organization to become successful. [14]-[16] found that anticipated extrinsic rewards had a negative effect on attitudes toward knowledge transfer. Several studies found no relationship between extrinsic motivation and knowledge transfer intentions or attitudes toward knowledge transfer [10], [17].

It is important to recognize that employees may decide to share (or not share) knowledge for various reasons. For example, as [18] reviewed earlier, research has shown that individuals may share knowledge because they enjoy helping others as a result of reciprocation. It is a problem to encourage the employees to share their knowledge because the knowledge is with them and is a sign of power to them [19]. Achieving effective knowledge transfer practices thus depends on individuals' willingness to put significant effort into the associated social processes [20].

3. KNOWLEDGE TRANSFER

KM is the process through which organizations generate value from their intellectual and knowledge based assets. Defined in this manner, it becomes apparent that KM is concerned with the process of identifying, acquiring, distributing and maintaining knowledge that is essential to the organization.

The presence of KM concept began to attract attention as a device capable of supporting the company in maximizing the knowledge and information at all levels of management to help improve the performance of the company [21], [22]. An increasing performance is supported by KM practice and find successful implementation requires integration of four pillars, namely leadership, learning, organizational structure, and technology.

Knowledge creation phase includes the emergence of knowledge from the origin to the development, later stages of development, such as documentation of knowledge, recorder of knowledge, transfer of knowledge, and distribution of knowledge. There are two main aspects of KM, namely, information management and people management [23]. Viewed from this perspective, KM is about information, on one hand, and people, on the other.

Organizations must also consider how to transfer expertise and knowledge from experts who have it to novices who need to [24]. The presence of KM concept began as a device capable of supporting about how the company should maximize the knowledge and information asset at all levels management to help improve performance of the company.

Knowledge transfer challenges were caused by the fact that knowledge has become a routine process, but the employees are not fully aware of the separate steps taken in the process of explicitly expressing knowledge [22]. The fundamental reason why Japanese companies are successful, because of their skills and experience was created of organizational knowledge [5]. Knowledge creation is achieved through acquiring of synergistic relationship between tacit and explicit knowledge.

The process of knowledge integration often encounters barriers i.e. tacit and knowledge that are embedded in routines and standalone [25]. Tacit knowledge that exists in system and the organization made the implementation knowledge integration to be slow and difficult [13] [5].
There is ongoing debate on what is the most important enabler for KM. A number of management analysts contend that technology is the most important. Others consider people to be the most important in knowledge management and argue that KM initiatives that focus mainly on technology can and do often fail. Both are, of course, important to the success of any KM systems. But the success of a KM systems depends on many factors, and among the most important is the efficient management of people and culture within the organization.

Ways to do this include encouraging communication, offering opportunities to learn, and promoting the transfer of appropriate knowledge artefact (KM is an attempt to increase the useful knowledge in the organization, among nurture a culture of communication between personnel, provide opportunities for learning, and promoting each other to share the knowledge).

4. FRAMEWORK

The research framework (see Fig. 1) is formulated based on selected related research as important factors that influence knowledge transfer and performance. These factors of knowledge transfer behaviour in the research framework were derived from existing constructs in the knowledge transfer and knowledge performance domain [10], [26]–[31].

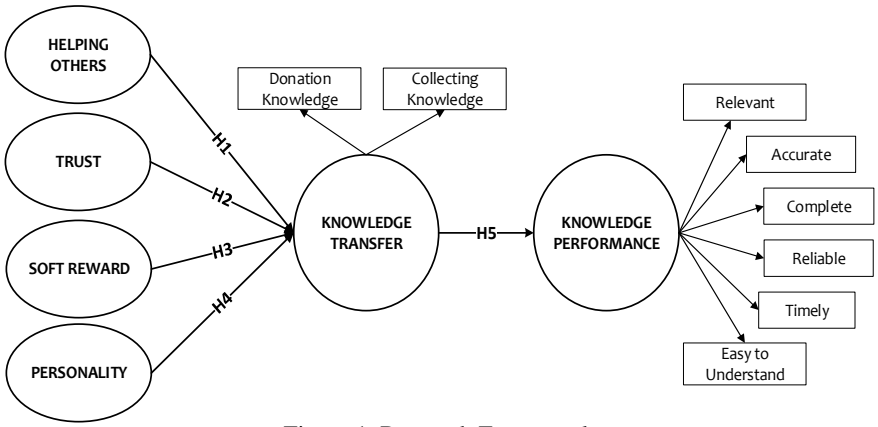

Figure 1. Research Framework

Six variables were selected to form the six hypotheses highlighted (H1, H2, H3, H4 and H5) in the research framework and empirically tested. The following discussion is presented to support our hypotheses.

4.1 Helping Others to Knowledge Transfer

Knowledge employees may be motivated by relative helping others owing to their desire to help others [8] [32]. Helping others as including discretionary behaviours that help specific others with organizationally relevant tasks or problems Organ (1998) as cited in [33]. Previous research

shows that employees are intrinsically motivated to contribute knowledge because engaging in intellectual pursuits and solving problems is challenging or pleasurable, and because they enjoy helping others [34].

4.2 Trust to Knowledge Transfer

Study conducted by [18] examined the impact of trust as a contextual factor and postulated that the degree of trust has an impact on collaborative efficiency in the organization. Many previous studies [35]–[39] have reported that a high level of trust facilitates knowledge transfer. Thus it concludes that high level of interpersonal trust correlate with high levels or willingness to knowledge transfer Kalantzis & Cope (2003) as cited in [2]. Many people are willing to share their knowledge with others if they feel that the person is honest and can be trusted [40].

4.3 Soft Reward to Knowledge Transfer

Soft rewards are defined as individuals expectations of achieving implicit outcomes (e.g., personal reputation and relationships with significant others) in return for performing knowledge transfer behaviour [18], [41], [42]. In addition, soft rewards may make individuals feel implicitly controlled or pressured to perform the behaviour due to the implicit consequences related to the behaviour, and are thus forms of interjected regulations/moderately controlled motivations [43], [44]. The following hypotheses are thus proposed.

4.4 Personality to Knowledge Transfer

The results of multiple regression analysis indicate that personality is the most significant predictor of knowledge performance followed by trust and awareness. This is evident when Awad & Ghaziri (2004) as cited in [28] suggest factors like personality and attitude; also suggests helpingothers in helping others and self-efficacy [33] and identifies motivations, trust and care that enable knowledge transfer [45].

4.5 Knowledge Transfer to Knowledge Performance

These two distinct processes are active processes in the sense that one is either engaged in active communication with others for the purpose of transferring knowledge, or consulting others in order to gain some access to their intellectual capital [46]. Knowledge donating aims to see individual knowledge become group and organizational knowledge over time, which in turn improves the stock of knowledge available to the firm [47]. However, previous research is still limitation discussed about collecting and receiving of knowledge that influence to knowledge transfer performance. According to [30] a system can be evaluated in terms of information quality. These items are known as main independent factors of the Delone and Maclean IS (information systems) success model. Then [48] mentioned that knowledge could be added to the information quality of the model as information or knowledge performance for achieving the KM success model. The performance of knowledge transfer was examined by the scale adapted from [29], [30].

5. RESEARCH METHOD

The data was collected by questionnaires, the data of this study also was taken from the non-profit organizations in Indonesia.

5.1 Sample and Data

We estimated total of respondents is about 364 respondents from 6 institutions that are willing to joint this research. The details are 4 universities and 2 schools in 3 district of Riau Province in Indonesia. For respondents in non-profit organization that total questionnaires returned is 325 of 364 questionnaires that we provided, there are 39 questionnaires were not returned. In this study, we used a structured questionnaire consisting of three parts. The first part is the briefly introduction about the important of this research. The second part is the demographic information about the participants which had seven demographic items including participant current position, age, how long participants have been work for company, education level of respondents, gender, name and email. The third part of the questionnaire measures based on the constructs in the research model, in conjunction with thirty-three main questionnaire items and also the last part of the questionnaire is the comment section by respondents for this study.

5.2 Measures

PLS and SPSS were used because its premises are less limiting and the sample size of data was relatively small [49]. These items were scored using Likert scale with 5 five-points, which 1 corresponds to "strongly disagree" and 5 to "strongly agree. We assess knowledge transfer behaviour using 8 items adapted from [31], [50]. For motivation and individual characteristics measures 15 items were adapted and we divided into four factors groups that helping others with 4 items, 4 items for trust, reward with 4 items and 3 items for personality adapted based on the study [10], [28], [51], [52]. For knowledge transfer performance we assess using 6 items adapted from [29], [30], [53]

6. RESULTS

To examine our proposed research model at both individual and organizational levels, the PLS technique was used for the data analysis. SmartPLS 3.2 was adopted for measurement validation and for testing the structural model based on the data collected from the 325 survey respondents in 6 non-profit organizations. Confirmatory factor analysis was performed to examine the validity and reliability of the constructs. In addition, a bootstrapping procedure was conducted for the significant tests of the research hypotheses.

Based on table 3 that show for male and female were 50.8% and 48.8%, is missing 1.2%. The questionnaire survey about job title of respondents were dean / vice dean (1.5%), chairman of department (2.8%), head of division (7.7%), staff (49.9%), secretary (0.9%) and staff is the biggest number (34.5%). The biggest of responses come from lecturer / teacher is 52.6%.

To assess confidence in their answers, respondents were also asked to indicate how long they had worked in their firms. Based on the data SPSS result Table 1, we know that 26.5% of the respondents had worked 1-3 years, 16.3% of the respondents had worked 4-6 years, 27.4% of the respondents had worked 7-9 years, 9.5% of the respondents had worked 10-12% years, and 18.8% of the respondents had worked for more than 13 years.

For education level, there is any the respondents of education in S3 (Doctoral) level is 2 respondents or 0.6% and for S2 (Master) 167 respondents or 51.4%, 20.9% of the respondents are S1 (Bachelor) level, 13.8% of the respondents are D3 (Diploma III) level, 11.1% of the respondents are Senior High School level, and for elementary school level only 0.6% of the respondents.

Table 1. Profile of Respondent (N=325)

Sample Characteristics		Frequency	%
Job Title	Dean / Vice Dean	5	1.5
	Chairman of Department	9	2.8
	Head of Division	25	7.7
	Lecturer / Teacher	171	52.6
	Secretary	3	0.9
	Staff	112	34.5
Working Year	1-3 years	86	26.5
	4-6 years	53	16.3
	7-9 years	89	27.4
	10-12 years	31	9.5
	More than 13 years	61	18.8
	Missing	5	1.5
Education Level	S3	2	0.6
	S2	167	51.4
	S1	68	20.9
	D3	45	13.8
	Senior High School	36	11.1
	Elementary School	2	0.6
	Missing	5	1.5
Gender	Male	165	50.8
	Female	156	48.8
	Missing	4	1.2

6.1 The Measurement Model

The measurement model was first assessed by CFA. The measurement model was further assessed for construct reliability and validity. Computing composite reliability assessed construct reliability. The composite reliability for each construct of this study is presented in Table 2. The composite reliability values was used to examine reliability shown in table 3, which all of the constructs composite reliability was exceed recommended cutoff of 0.7 that indicating a commonly acceptable level for confirmatory research [54].

6.1.1 Convergent Validity:

Convergent validity was evaluated for measurement scales using three criteria suggested by [55]–[59]. All indicator factor loading should be significant and exceed 0.6, composite reliability should exceed 0.7, and average variance extracted (AVE) from each construct should exceed 0.5 [55]–[59].

Table 2. Factors loadings and reliability

Constructs	Items	Loadings	Status	CA	AVE	CR
Helping Others	HO 1	0.85	Valid	0.85	0.70	0.90
	HO 2	0.91	Valid			
	HO 3	0.90	Valid			
	HO 4	0.68	Invalid			
Trust	Trs 1	0.74	Valid	0.79	0.62	0.86
	Trs 2	0.78	Valid			
	Trs 3	0.86	Valid			
	Trs 4	0.75	Valid			

Constructs	Items	Loadings	Status	CA	AVE	CR
Soft Reward	Srd 1	0.85	Valid	0.92	0.80	0.94
	Srd 2	0.92	Valid			
	Srd 3	0.90	Valid			
	Srd 4	0.90	Valid			
Personality	Per 1	0.84	Valid	0.75	0.66	0.85
	Per 2	0.80	Valid			
	Per 3	0.80	Valid			
Knowledge Transfer	Col 1	0.77	Valid	0.84	0.51	0.88
	Col 2	0.80	Valid			
	Col 3	0.73	Valid			
	Col 4	0.65	Invalid			
	Don 1	0.77	Valid			
	Don 2	0.70	Valid			
	Don 3	0.64	Invalid			
	Don 4	0.56	Invalid			
Knowledge Performance	KP 1	0.68	Valid	0.88	0.62	0.91
	KP 2	0.80	Valid			
	KP 3	0.83	Valid			
	KP 4	0.87	Valid			
	KP 5	0.82	Valid			
	KP 6	0.71	Valid			

Note: CA (Cronbach Alpha), AVE (Average Variance Extracted), CR (Composite Reliability)

The data collected were subjected to convergent and discriminant validity analysis before the final analysis was conducted. Factor loadings, composite reliability and average variance extracted were used to assess convergence validity. The loadings for all items exceeded the recommended value of 0.7 except items for Don 3 and 4 (knowledge transfer). Composite reliability values (see Table 2), which showed the degree to which the items indicated the latent construct, ranged from 0.70 (KT) to 0.94 (soft reward), which exceeded the recommended value of 0.7 [55]–[59]. The average variance extracted (AVE) was in the range of 0.51, which exceeded the recommended value of 0.5 and 0.7 [55]–[59].

6.1.2 Discriminant Validity

Discriminant validity measure by cross loading [60]. Discriminant validity can be examined by comparing the squared correlations between constructs and variance extracted from a construct. Table 3 indicating the measure has adequately discriminant validity.

Table 3. Correlation matrix (fornell-larcker) and discriminant validity

Constructs	AL	KSB	KSQ	PE	RE	TR
HO	**0.84**					
KT	0.46	**0.71**				
KP	0.30	0.61	**0.79**			
PE	0.34	0.52	0.51	**0.81**		
SR	0.44	0.48	0.37	0.44	**0.89**	
TR	0.34	0.43	0.36	0.26	0.36	**0.78**

Note: HO (Helping Others), KS (Knowledge Transfer), KP (Knowledge Performance), PE (Personality), SR (Soft Reward), TR (Trust).

6.2 The Model and Hypotheses Results

The results of the structural model analysis are displayed in Figure 2. The structural model links the constructs to one another. Analysis of the structural model is the analysis of patterns of relationships between variables is an analysis of the hypotheses of the study. Research hypothesis is acceptable if a connection variable correlated positively and significantly based on the test results of the t-test and path coefficients.

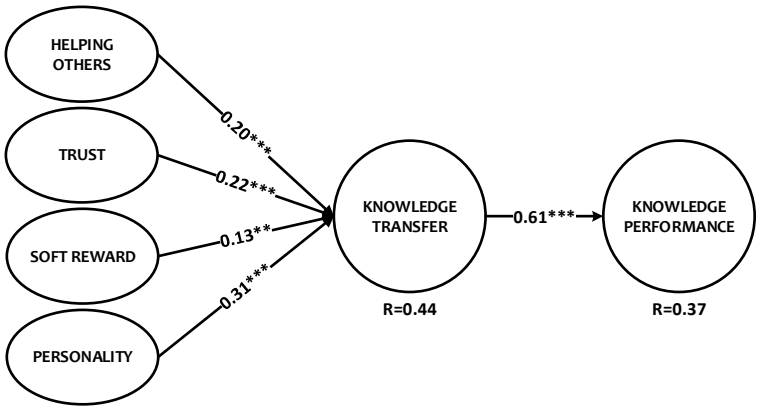

Figure 2. Results of structural model.

To identify the relationship between individual factors and knowledge performance, correlation analysis was conducted. Correlation analysis indicates the strength and direction of relationship between the independent and dependent variables under studied. The result of correlation analysis shows that all the variables are significantly correlated with knowledge transfer behaviour and knowledge performance. Based on Table 4 shows that the relationship between variables is positive or positively correlated and significant effect (t-statistic has a value greater than 1.96* for p-value<0.05, 2.59** for p-value<0.01, and 3.32*** for p-value<0.001 of 325 respondents).

Table 4. Hypothesis tests based on PLS-SEM based model

Hypothesis	Hypothesis Path	Coefficients	T-Values	P-Values	Accept / Reject
H1	Helping Others → Knowledge Transfer	0.20	4.29	0.00	Accept***
H2	Trust → Knowledge Transfer	0.22	4.91	0.00	Accept***
H3	Soft Reward → Knowledge Transfer	0.13	2.68	0.01	Accept**
H4	Personality → Knowledge Transfer	0.31	5.76	0.00	Accept***
H5	Knowledge Transfer → Knowledge Performance	0.61	17.36	0.00	Accept***

7. DISCUSSION

The research results also confirm the positive direct effects of trust, helping others, soft rewards and personality for knowledge transfer behaviour. We found that knowledge transfer behaviour influence to knowledge transfer performance. We measures that knowledge transfer behaviour from two sub-factors that donation and collecting knowledge among employees based on [31], [50]. Then, for knowledge transfer performance was examined by the scale adapted from [29], [30], these items measured by easy to understand, accuracy, completeness, reliability, and timeliness.

Many previous studies also suggested that helping others among employees is one of the success factors of knowledge transfer behaviours. The results of this study showed that helping others (H1, coefficient = 0.20, $p<0.05$), have significant influence on knowledge transfer behaviours. Helping others as including discretionary behaviours that help specific others with organizationally relevant tasks or problems Organ (1998) as cited in [10].

Trust among employees is a critical factor that influences knowledge transfer behaviour [35]–[39]. The results of this study showed that trust (H2, coefficient = 0.22, $p<0.05$), have significant influence on knowledge transfer behaviours. The result also indicates that trust among the employees is considered as an important factor that influences employees to share knowledge. This suggests that employees may share their knowledge based on trust and irrespective of others different cultures, educational level and also job position.

The results of this study showed that soft reward a positive influence on knowledge transfer behaviour (H3, coefficient = 0.13, $p<0.05$). Rewards are defined as individuals expectations of achieving implicit outcomes (e.g., personal reputation and relationships with significant others) in return for performing knowledge transfer behaviour [18], [41], [42].

Based on the PLS results, is that personality should implement a supportive knowledge transfer behaviours. The results of this study showed that personality (H5, coefficient = 0.31, $p<0.05$), have significant influence on knowledge transfer behaviours and also personality is that have a higher number of path coefficient among all factors that influence to knowledge transfer behaviour.

In this research found is that knowledge transfer behaviour (coefficient = 0.61), have significant influence on knowledge performance. Knowledge transfer has two facets, collecting or receiving and disseminating or sending knowledge.

8. CONCLUSION

This is important because it is still crucial to accurately explain the knowledge transfer behaviour of individual professional groups [3] and also because team and organizational level knowledge is influenced by the extent to which knowledge transfer occurs between employees [4]–[7]. For this reason, we have provided a research model derived from previous studies to be tested in a non-profit organization. This would provide helpful guidelines for human resource managers and knowledge employees working in today's growing number of knowledge-intensive organizations. As mentioned earlier, this study attempted to fill the gap in the current literature by examining the factors that influence knowledge transfer among employees of non-profit organizations. The results of this study indicated that helping others, trust, soft reward, and personality have an influence on knowledge transfer, and also knowledge transfer behaviour have an influence on knowledge performance.

REFERENCES

[1] F. A. Uriarte, "Introduction to Knowledge Management," Igarss 2014, no. 1, pp. 1–5, 2008.

[2] S. Alam, Z. Abdullah, N. Ishak, and Z. Zain, "Assessing Knowledge Sharing Behaviour among Employees in SMEs: An Empirical Study," Bus. Res., no. 1998, pp. 115–122, 2009.

[3] S. Ryu, S. H. Ho, and I. Han, "Knowledge sharing behavior of physicians in hospitals," Expert Syst. Appl., vol. 25, no. 1, pp. 113–122, 2003.

[4] E. F. Cabrera and A. Cabrera, "Fostering knowledge sharing through people management practices," Int. J. Hum. Resour. Manag., vol. 16, no. May, pp. 720–735, 2005.

[5] I. Nonaka, "A Dynamic Theory of Organizational Knowledge Creation," Organization Science, vol. 5, no. 1. pp. 14–37, 1994.

[6] P. Fingesten, "The tacit dimension ?: Garden City, N.Y., Doubleday and Co., 1966, 108 pages," J. Commun. Disord., vol. 1, no. 4, pp. 346–347, 1968.

[7] H. Tsoukas and E. Vladimirou, "What is organizational knowledge?," J. Manag. Stud., vol. 38, no. 7, pp. 972–993, 2001.

[8] T. H. Davenport, "Ten principles of knowledge management and four case studies," Knowl. Process Manag., vol. 4, no. 3, pp. 187–208, 1997.

[9] S. Gao, "Understanding knowledge sharing behavior." pp. 1–87, 2004.

[10] H. F. Lin, "Effects of extrinsic and intrinsic motivation on employee knowledge sharing intentions," J. Inf. Sci., vol. 33, no. 2, pp. 135–149, 2007.

[11] S. Moffett, R. McAdam, and S. Parkinson, "An empirical analysis of knowledge management applications," J. Knowl. Manag., vol. 7, no. 3, pp. 6–26, 2003.

[12] H. Lee and B. Choi, "Knowledge management enablers, processes, and organizational performance : An integration and empirical examination," J. Manag. Inf. Syst., vol. 20, no. 1, pp. 179–228, 2003.

[13] M. C. Jones, M. Cline, and S. Ryan, "Exploring knowledge sharing in ERP implementation: An organizational culture framework," Decis. Support Syst., vol. 41, no. 2, pp. 411–434, 2006.

[14] G. Bock, R. Zmud, and J.-N. Lee, "Behavioral Intention Formation in Knowledge Sharing," MIS Quarterly, vol. 29, no. 1. pp. 87–111, 2005.

[15] G.-W. Bock and Y.-G. Kim, "Breaking the Myths of Rewards: An Exploratory Study of Attitudes about Knowledge Sharing," Inf. Resour. Manag. J., vol. 15, no. 2, pp. 14–21, 2002.

[16] G. W. Bock and Y.-G. Kim, "Breaking the Myths of Rewards," Inf. Resour. Manag. J., vol. 15, no. 2, pp. 14–21, 2002.

[17] S. H. Kwok and S. Gao, "Attitude Towards Knowledge Sharing Behavior," J. Comput. Inf. Syst., vol. 46, no. 2, pp. 45–51, 2005.

[18] A. Kankanhalli, B. C. Y. Tan, and K.-K. Wei, "C Ontributing K Nowledge To E Lectronic K Nowledge R Epositories : a N E Mpirical," MIS Q., vol. 29, no. 1, pp. 113–143, 2005.

[19] H. Gumbley, "Knowledge Management," Emerald Insight, vol. 47, no. 5, pp. 175–177, 1998.

[20] H. H. Chang and S.-S. Chuang, "Social capital and individual motivations on knowledge sharing: Participant involvement as a moderator," Inf. Manag., vol. 48, no. 1, pp. 9–18, 2011.

[21] Saide and N. E. Rozanda, "Analisis kebutuhan manajemen pengetahuan pada perusahaan perbankan 1," Open Access J. Inf. Syst., vol. 5, no. 3, pp. 343–351, 2015.

[22] Saide and E. Mahendrawathi, "Knowledge Management Support For Enterprise Resource Planning Implementation," Procedia - Procedia Comput. Sci., vol. 72, pp. 613–621, 2015.

[23] F. A. Uriarte, "Introduction to knowledge management in the NHS," Asean Found., p. 179, 2008.

[24] P. J. Hinds, M. Patterson, and J. Pfeffer, "Bothered by abstraction: the effect of expertise on knowledge transfer and subsequent novice performance.," J. Appl. Psychol., vol. 86, no. 6, pp. 1232–1243, 2001.

[25] F. Blackler, "Knowledge, Knowledge Work and Organizations: An Overview and Interpretation," vol. 16, no. 6. pp. 1020–1046, 1995.

[26] Y. H. Al-Qadhi, K. Md Nor, A. C. Ologbo, and M. B. Knight, "Knowledge sharing in a multi-nationality workforce: Examining the factors that influence knowledge sharing among employees of diverse nationalities," Hum. Syst. Manag., vol. 34, no. 3, pp. 149–165, 2015.

[27] W. T. Wang and Y. P. Hou, "Motivations of employees' knowledge sharing behaviors: A self-determination perspective," Inf. Organ., vol. 25, no. 1, pp. 1–26, 2015.

[28] M. B. Ismail and Z. M. Yusof, "The Contribution of Technological Factors on Knowledge Sharing Quality among Government Officers in Malaysia," Knowl. Manag., pp. 239–255, 2010.

[29] W. H. Delone and E. R. Mclean, "Information Systems Success: The Quest for the Dependent Variable," no. 4, 1992.

[30] W. Delone and E. McLean, "The DeLone and McLean model of information systems success: a ten-year update," J. Manag. Inf. …, vol. 19, no. 4, pp. 9–30, 2003.

[31] S. Mohammed, A. Syed, and A. Alhady, "Knowledge Sharing Behavior and Individual Factors : A Relationship study in the i-Class Environment," Ipedr, vol. 6, pp. 137–141, 2011.

[32] D. Constant, K. Sara, and S. Lee, "Whats Mine is Ours, or is it ? A study of Attitudes about Information Sharing." 1994.

[33] H. Lin, "Knowledge sharing and firm innovation capability: an empirical study," Int. J. Manpow., vol. 28, no. 3/4, pp. 315–332, 2007.

[34] M. M. Wasko and S. Faraj, "Why Should I Share ? Examining Social Capital and Knowledge Contribution in," vol. 29, no. 1, pp. 35–57, 2005.

[35] C.-M. Chiu, M.-H. Hsu, and E. T. G. Wang, "Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories," Decis. Support Syst., vol. 42, no. 3, pp. 1872–1888, 2006.

[36] W. S. Chow and L. S. Chan, "Social network, social trust and shared goals in organizational knowledge sharing," Inf. Manag., vol. 45, no. 7, pp. 458–465, 2008.

[37] C.-L. Hsu and J. C.-C. Lin, "Acceptance of blog usage: The roles of technology acceptance, social influence and knowledge sharing motivation," Inf. Manag., vol. 45, no. 1, pp. 65–74, 2008.

[38] W. He and K.-K. Wei, "What drives continued knowledge sharing? An investigation of knowledge-contribution and -seeking beliefs," Decis. Support Syst., vol. 46, no. 4, pp. 826–838, 2009.

[39] B. van den Hooff and M. Huysman, "Managing knowledge sharing: Emergent and engineering approaches," Inf. & Manag., vol. 46, no. 1, pp. 1–8, 2009.

[40] M. Sharrat and A. Usoro, "Understanding Knowledge Sharing in Online Communities of Practice," Electron. J. Knowl. Manag., vol. 1, no. 2, pp. 187–196, 2003.

[41] H. G. K. Hummel, D. Burgos, C. Tattersall, F. Brouns, H. Kurvers, and R. Koper, "Encouraging contributions in learning networks using incentive mechanisms," J. Comput. Assist. Learn., vol. 21, no. 5, pp. 355–365, 2005.

[42] H. Hall and D. Graham, "Creation and recreation: motivating collaboration to generate knowledge capital in online communities," Int. J. Inf. Manage., vol. 24, no. 3, pp. 235–246, 2004.

[43] M. Gagne, "Hrm : Implications for the Professionals," Hum. Resour. Manage., vol. 45, no. 3, pp. 295–308, 2009.

[44] M. Gagne and E. L. Deci, "Self-determination theory and work motiviation," J. Organ. Behav., vol. 26, no. October 2003, pp. 331–362, 2005.

[45] P. van den Brink, Social, Organizational and Technological Conditions that enable Knowledge Sharing. 2003.

[46] B. Van Den Hooff and J. A. De Ridder, "Knowledge sharing in context : The influence of organizational commitment, communication climate and CMC use on knowledge sharing Knowledge sharing in context : the influence of organizational commitment, communication climate and CMC use on knowledge" 2004.

[47] J. Darroch, R. Mcnaughton, J. Darroch, and R. Mcnaughton, "Examining the link between knowledge management practices and types of innovation," 2006.

[48] M. E. Jennex and L. Olfman, "Assessing Knowledge Management Success / Effectiveness Models," vol. 00, no. C, pp. 1–10, 2004.

[49] R. Cheung and D. Vogel, "Predicting user acceptance of collaborative technologies: An extension of the technology acceptance model for e-learning," Comput. Educ., vol. 63, pp. 160–175, 2013.

[50] J. P. Nicolai, D. B. Minbaeva, T. Pedersen, and M. Reinholt, "Encouraging Knowledge Sharing Among Employees: How Job Design Matters," Hum. Resour. Manage., vol. 45, no. 3, pp. 295–308, 2009.

[51] Y. H. Al-Qadhi, K. Md Nor, A. C. Ologbo, and M. B. Knight, "Knowledge sharing in a multi-nationality workforce: Examining the factors that influence knowledge sharing among employees of diverse nationalities," Hum. Syst. Manag., vol. 34, no. 3, pp. 149–165, 2015.

[52] W.-T. Wang and Y.-P. Hou, "Motivations of employees' knowledge sharing behaviors: A self-determination perspective," Inf. Organ., vol. 25, no. 1, pp. 1–26, 2015.

[53] A. Sarkheyli, R. A. Alias, N. Ithnin, and M. D. Esfahani, "Dimensions of Knowledge Sharing Quality : An Empirical Investigation," J. Res. Innov. Inf. Syst., pp. 9–18, 2013.

[54] C. M. Chiu and E. T. G. Wang, "Understanding Web-based learning continuance intention: The role of subjective task value," Inf. Manag., vol. 45, no. 3, pp. 194–201, 2008.

[55] J. F. Hair, C. M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a Silver Bullet," J. Mark. Theory Pract., vol. 19, no. 2, pp. 139–152, 2011.

[56] J. F. Hair, M. Sarstedt, C. M. Ringle, and J. A. Mena, "An assessment of the use of partial least squares structural equation modeling in marketing research," pp. 414–433, 2012.

[57] J. Hulland, "Use of partial least squares (PLS) in strategic management research: A review of four recent studies," Strateg. Manag. J., vol. 20, no. 2, pp. 195–204, 1999.

[58] C. Fornell, D. F. Larcker, and S. Modeling, "Equation Algebra Error :," vol. XVIII, no. August, pp. 382–388, 1981.

[59] W. W. Chin, "The partial least squares approach to structural equation modeling," Mod. methods Bus. Res., pp. 237–246, 1998.

[60] D. Gefen, "Structural Equation Modeling and Regression : Guidelines for Research Practice Structural Equation Modeling and Regression : Guidelines for Research Practice," Struct. Equ. Model., vol. 4, no. August, p. 7, 2000.

AUTHORS

Saide.

He is currently Double Degree Master Student which in Department of Information Management at National Taiwan University of Science and Technology and Department of Information Systems at Institute Technology of Sepuluh Nopember (ITS), Surabaya, Indonesia. Received the B.Sc. degree of information systems in 2013 at State Islamic University of Sultan Syarif Kasim Riau, Indonesia.

His research majors includes knowledge management strategy, knowledge transfer framework, management information system, renewable energy, and project management. He also executive of operational management and project management at energy research center (enreach.or.id), Riau, Indonesia.

Dr. Hsiao-Lan Wei.

She is an associate professor at Department of Information Management, National Taiwan University of Science and Technology, Taiwan. She did her B.Sc degree in National Tsing Hua University. She received her M.Sc (1995) and Ph.D (2006) degree at National Central University, Taiwan.

Her research fields are in supply chain management, enterprise resource management, production management, and cross-organization information management.

Dr. Apol Pribadi Subriadi.

Currently he is chairman of graduate study and lecturer at Department of Information System at Institute Technology of Sepuluh Nopember (ITS), Surabaya, Indonesia. She did her B.Sc degree in Department of Electrical Engineering (1994) at ITS Surabaya University, M.Sc in Department of Industrial Engineering (2000) at ITS Surabaya University, and Ph.D degree at Department of Management and Business of Brawijaya University (2013).

His research interests includes information systems (business informatics), management information systems, information system management, online research methods, IT/IS investment, and IT/IS- bussiness alignment.

Dr. Okfalisa

Okfalisa finished her PhD in information System and Computer Science at Universiti Teknologi Malaysia in 2012. Her research focuses on performance measurement, strategy execution, management information system and decision support system through several research project, national and international publications funding by University Islamic Suska Riau and Indonesia Islamic Higher Education Ministry. She also reviews some locals and international journals under Scopus. Currently she is senior lecturer in Informatics Engineering Department and serves as vice dean of students' affairs and collaboration in Science and Technology Faculty University Islamic Suska Riau Indonesia.

Nurul Aini

She is currently Master Degree Student of Information System Department at Diponegoro University, Semarang, Indonesia. She did her B.Sc degree of Information System in 2012 at State Islamic University of Sultan Syarif Kasim Riau, Indonesia.

His research fields includes Green ICT, Management Information System, and Supply Chain Management.

Nesdi Evrilyan Rozanda, M.Sc

Currently he is chair of board of Energy Research Center (enreach.or.id) and lecturer at Department of Information System, State Islamic University of Sultan Syarif Kasim Riau, Indonesia. She did her B.Sc degree in Computer Science of STMIK "YPTK" Padang, West Sumatera Indonesia, and M.Sc titled in Universiti Teknologi Malaysia.

His research interests includes information systems, green ICT, knowledge management, renewable energy and artificial intelligence.

AUTHOR INDEX