UPM

UNIVERSITI PUTRA MALAYSIA

AN IMPROVED USER AUTHENTICATION MODEL FOR MOBILE APPLICATION SYSTEMS

KARTINI BINTI MOHAMED

FSKTM 2018 5

AN IMPROVED USER AUTHENTICATION MODEL FOR MOBILE APPLICATION SYSTEMS

By

KARTINI BINTI MOHAMED

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Master of Science

September 2017

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

AN IMPROVED USER AUTHENTICATION MODEL FOR MOBILE APPLICATION SYSTEMS

By

KARTINI BINTI MOHAMED

September 2017

Chairman: Assoc. Prof. Fatimah Sidi, PhD
Faculty: Computer Science and Information Technology

In today’s digital communication era, people around the world can conveniently communicate with each other at any time and any places by just using mobile phones. Besides making phone calls and sending messages, mobile phones can also be used to download many interesting and useful apps for personal, businesses or even entertainment purposes. Due to borderless competition in the digital world, a lot of exciting and necessary mobile apps available for free downloads from the Internet. Unfortunately, mobile apps are communicating using wireless networks which are very vulnerable to data stealing or sniffing by intruders. People who communicate using unprotected mobile apps are in high risks if the used apps deal with personal or highly confidential data such as in mobile banking, mobile payment, and mobile purchase or even in certain government related affairs including income tax payment, health monitoring systems, etc.

There are many ways the mobile apps can be protected. One of the common ways is to control the access to the apps using a strong user authentication. Even though researchers have introduced many ways to make user authentication strong, this study proposes an improved user authentication model by making it not only strong but also acceptable by mobile users. The user authentication is made strong using three different techniques namely multi-factoring, ciphering, and watermarking techniques. It is considered acceptable by mobile users based on the results obtained from statistical analysis carried out in this study. To validate the proposed user authentication model, several prototype mobile apps are developed using a uSign-Mf+ module containing the proposed improvements and sent for evaluation by CyberSecurity Malaysia Sdn. Bhd. (CSM), an independent testing body.

Based on the statistical analysis results, majority of the users agree that the proposed improvement of user authentication is strong and acceptable. However, they consider that the proposed model is strong with all the proposed improvement techniques except the use of hashing in the ciphering technique. Even though the users believe that the existing encryption is good enough without hashing, experts have proven that hashing can improve the data integrity and protect the system from several attacks such as brute force and tampering attacks. Therefore, the use of hash in this model should be retained. Meanwhile, from the evaluation by CSM, the proposed model is effective without major modifications required on the prototype mobile apps. Thus, it is concluded that the proposed model is strong and acceptable by mobile phone users.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
Sebagai memenuhi keperluan untuk ijazah Master Sains

PENAMBAHBAIKAN MODEL KATA KUNCI PENGGUNA APPLIKASI TELEFON MUDAH ALIH

Oleh

KARTINI BINTI MOHAMED

September 2017

Pengerusi: Prof. Madya Fatimah Sidi, PhD
Fakulti: Sains Komputer dan Teknologi Maklumat

Di dalam era komunikasi digital sekarang, orang ramai di seluruh dunia boleh berkomunikasi antara satu sama lain pada bila-bila masa di mana sahaja dengan selesa dengan hanya menggunakan telefon mudah alih. Selain dari membuat panggilan telefon dan menghantar mesej, telefon mudah alih juga boleh digunakan untuk memuat turun banyak aplikasi yang menarik dan berguna untuk kegunaan peribadi, perniagaan atau pun hiburan. Disebabkan oleh persaingan tanpa sempadan di dalam dunia digital, banyak aplikasi yang boleh dimuat turun secara percuma dari Internet. Malangnya, aplikasi telefon mudah alih berkomunikasi secara tanpa wayar yang mana ianya sangat mudah untuk dicerobohi dan boleh menyebabkan data dicuri atau dikesan oleh penceroboh. Orang ramai yang berkomunikasi menggunakan aplikasi telefon mudah alih yang tidak dilindungi berada di dalam risiko yang tinggi sekirannya mereka menggunakan aplikasi telefon mudah alih yang menggunakan data yang sangat peribadi atau sangat sulit seperti pengunaan bagi urusan berkaitan perbankan, pembayaran atau pembelian atau pun bagi sesetengah urusan kerajaan seperti pembayaran cukai pendapatan, sistem pemantauan kesihatan dan lain-lain.

Terdapat pelbagai cara untuk melindungi aplikasi telefon mudah alih. Salah satu cara yang biasa digunakan adalah dengan mengawal kemasukkan ke aplikasi dengan menggunakan kata kunci yang kebal. Walaupun penyelidik telah memperkenalkan pelbagai cara untuk menjadikan kata kunci kebal, penyelidikan ini mencadangkan satu model kata kunci yang ditambahbaik dengan menjadikannya bukan sahaja kebal tetapi juga diterima pakai oleh pengguna telefon mudah alih. Kata kunci ini dijadikan lebih kebal dengan menggunakan tiga teknik yang berbeza yang dinamakan sebagai teknik *multi-factoring, ciphering,* dan *watermarking.* Ianya dianggap telah diterima pakai oleh pengguna telefon mudah alih berdasarkan keputusan yang diperolehi dari penilaian statistik yang dilaksanakan di dalam penyelidikan ini. Bagi mengesahkan keberkesanan model kata kunci yang dicadangkan, beberapa aplikasi telefon mudah alih yang prototaip dibangunkan dengan menggunakan modul uSign-Mf+, yang mengandungi penambahbaikan yang diperkenalkan, dan dihantar untuk dinilai oleh CyberSecurity Malaysia Sdn. Bhd. (CSM), sebuah badan penilai yang berkecuali.

Merujuk kepada keputusan analisa statistik, kebanyakkan pengguna bersetuju bahawa penambahbaikan yang diperkenalkan terhadap kata kunci adalah kebal dan boleh diterima pakai. Walau bagaimanapun, mereka menganggap bahawa model yang diperkenalkan adalah kebal disebabkan oleh kesemua teknik penambahbaikan yang diperkenalkan kecuali pengunaan *hashing* di dalam teknik *ciphering*. Walaupun para pengguna percaya bahawa *encryption* yang sedia ada adalah mencukupi tanpa pengunaan *hashing*, pakar telah membuktikan bahawa *hashing* dapat meningkatkan integriti data dan melindungi sistem dari beberapa serangan seperti serangan *brute force* dan *tampering*. Dengan ini, pengunaan *hash* di dalam model ini patut dikekalkan. Dari penilaian yang telah dibuat oleh CSM pula, model yang diperkenalkan adalah kebal tanpa sebarang perubahan yang *major* terhadap aplikasi telefon mudah alih yang prototaip. Oleh itu, adalah dirumuskan bahawa model yang diperkenalkan adalah kebal dan boleh diterima pakai oleh pengguna telefon mudah alih.

ACKNOWLEDGEMENTS

I would like to convey my sincere thanks to all those who have spent their times, money and efforts in helping me directly or indirectly to prepare, write and complete all works related to this thesis throughout my studies in Universiti Putra Malaysia (UPM).

I would like to sincerely thank my supervisor Prof. Madya Dr. Fatimah Sidi for guiding me without despair day and night until I have successfully submitted my thesis. Thank you very much also for steering me during my article submissions to local and international journal publishers and my participations in local and international conferences and showcases. Not to be missing out from my list of sincere thanks are my supervisory committee members, Prof. Madya Dr. Marzanah A. Jabar and Dr. Iskandar Ishak as well as other lecturers including Dr. Siti Rabaah, Pn. Jasmin etc. who have given me valuable lessons and guidance during my studies.

Special thanks to my employer SIRIM Berhad especially the president, the Human Resource personnel and my bosses Dr. Wan Abdul Rahman Jauhari Wan Harun, Tuan Hj. Suhaimi Mahmood and Hasmafatiha Harun for sponsoring my studies and giving me study leaves two days every week. Also thank you so much to my colleagues and friends for giving me countless assistance, advices and encouragement to further my studies.

Big thank you to the Managing Director of HICE Engineering and Services Sdn. Bhd., Mr. Mohd. Zahli bin Majid for giving me a lot of financial and moral supports throughout my studies. Similar thanks to my lovely mother Habibah Ismail, all my brothers and sisters as well as my family members Mohamad Amirul Hafiz, Siti Nur Amanina, Siti Nur Hamiza, Siti Nur Hazira and Muhammad Amirul Hariz for having good understanding and being passionate with my busy schedules until I manage to complete my studies.

My sincere thanks are also to the staffs of CyberSecurity Malaysia especially Pn. Nor'azuwa Muhamad Pahri for a very good cooperation given to ensure the required testing can be performed by the relevant experts. Not to be missed, a big thank you to the members of MySEF and MyVAC especially Pn. Norahana Salimin and Pn. Maslina Daud as well as their team members Nor Safwan Amirul Salleh, Abdul Qaiyum Hamzah, Ahmad Dahari Jarno, Muhammad Faeez Pauzi, Hafizah Che Hassan and Abdul Fuad Abdul Rahman for giving priceless supports and cooperation in providing the appropriate testing for the prototype software application systems developed in this study.

Last but not least, my thanks also to others whom I could not name here. Thank you so much and please also accept my sincere apologies for all the troubles I have made throughout my studies here in UPM, Serdang, Selangor, Malaysia.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Fatimah Sidi, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Marzanah A. Jabar, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Iskandar Ishak, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

____
ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ____
Name of Chairman of
Supervisory Committee: Prof. Madya Dr. Fatimah Sidi

Signature: ____
Name of Member of
Supervisory Committee: Prof. Madya Dr. Marzanah A. Jabar

Signature: ____
Name of Member of
Supervisory Committee: Dr. Iskandar Ishak

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
ANOVA	Analysis of Variance
APK	Android Application Package
ATE	Security Functional Test
AVA	Vulnerability Assessment
CBC	Cipher Block Chaining
CFB	Cipher Text Feedback
CSM	CyberSecurity Malaysia
ECB	Electronic Codebook
ECDH	Elliptic Curve Diffie Hellman
FSKTM	Faculty of Computer Science and Information Technology
GLOMONET	Global Mobility Network
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IMS	Integrity Management Services
IMEI	The International Mobile Equipment Identity
LAN	Local Area Network
MANET	Mobile Ad hoc Network
MBAN	Medical Body Area Network
MOSTI	Ministry of Science, Technology and Innovation
MySEF	Malaysian Security Evaluation Facility
MySQL	Open Source SQL database management system
OCB	Offset Codebook
OFB	Output Feedback
PHP	Hypertext Preprocessor
PKI	Public Key Infrastructure
PPMC	Pearson Product Moment Correlation
QoS	Quality of Service
QR Code	Quick Response Code
SHA	Secure Hash Algorithm
SIM Card	Subscriber Identification Module Card
SMS	Short Message Services
SSO	Single Sign On
SPSS	Statistical Package for Social Sciences
TAC	Transaction Authorization Code
TLS	Transport Layer Security
UPM	Universiti Putra Malaysia
VAPT	Vulnerability Assessment and Penetration Test
VSS	Visual Secret Sharing
WAN	Wide Area Network
WBAN	Wireless Body Area Networks
WSN	Wireless Sensor Network

CHAPTER 1

INTRODUCTION

1.1 Overview

Currently, there are many mobile application systems available on the Internet that can be downloaded either freely or with charges into mobile phones especially smart phones. Many of these mobile apps involved with the communications of sensitive data such as personal, financial or legal data that require high level protections from any unauthorized users. These types of data need to have certain level of protections to prevent them from being stolen or misused such as by using user authentication which gives permissions to only registered or approved users. However, the levels of protections to secure such highly confidential data depend so much on the strength of user authentication.

Communications using mobile apps involves wireless data transmissions which are more vulnerable to hacking activities by intruders compared to communications in a wired (non-wireless) environment. Thus, stronger security protections are required to properly control the access to mobile apps. Many studies have been carried out by researchers to improve the security protections related to user authentication (Liao and Lee, 2009; Gordon and Sankaranarayanan, 2010; Acharya and Kumar, 2011; Belkhede *et al.*, 2012, Elkhodr *et al.*, 2012). Many of them propose the use of multi-factor instead of single factor user authentication, which only have username and password. Multi-factor user authentication uses more than username and password as the user authenticating factors.

One of the studies done by researchers related to strengthening user authentication for the apps used in mobile banking is found to be relevant to this study (Elkhodr *et al.*, 2012). Since banking services deal with highly confidential data the researcher recommends the use of four factors for user authentication, namely: username, password, IMEI Number and SIM Card Number as part of the procedure to secure the access to the apps. However, based on the explanation given by Parker (2017), IMEI Number and SIM Card Number can be stolen if someone manages to get into the mobile phone setting. Thus, using username, password, IMEI Number, and SIM Card number are not enough to control the access to mobile apps.

Another group of researchers are also attempting to strengthen the user authentication especially for use in Global Mobility network or GLOMONET. Yoon *et al.* (2011) and Li and Lee (2012), for example, have found out that random number and time can make the user authentication strong to protect sensitive or highly confidential data or information in GLOMONET. Therefore, it is necessary if a study can be carried out to analyze the strength of user authentication using the combinations of the above user authentication factors. On the other hands, according to Bruun *et al.* (2014), Seto *et al.* (2015), and Shay *et al.* (2016) the use of user authentication not necessarily need to be only strong but also need to be usable and suitable for use by mobile users. Thus, user authentication models that are strong and acceptable by mobile users seem to be very useful to be introduced in the present days.

1.2 Problem Statement

Mobile apps used to transmit private and confidential data should be well protected to prevent data leakage to irresponsible individuals. Mobile users may face many risks if these data are leaked out. The risks may include identity theft which can lead to losses of data, money, time, and reputations (Schneider, 2012).

Thus, access onto mobile application (mobile app) has become an utmost task to be made secure as it ensures the safety and privacy of mobile application usage. User authentication has been the highlights of research in recent years and among the approach introduced is multi-factor based user authentication. Based on literatures, previous approaches have proposed different combination of multi-factor user authentication and according to Acharya and Kumar (2011), Elkhodr *et al.* (2012) and Meng *et al.* (2015) the more factors used, the safer or reliable the user authentication is. For example, Acharya and Kumar (2011) propose the use of location signature and time while Elkhodr *et al.* (2012) prefer to use IMEI number and SIM card number besides username and password. Meng *et al.* (2015) however recommend the use of biometric and pin number. Different sets of authentication factors proposed by previous researchers have created such predicament onto the selection of a strong and acceptable set of the authentication factors (Seto *et al.,* 2015). Each factor introduced in the literatures possesses its own strengths and weaknesses and the combination of these authentication factors must be considered properly (Seto *et al.,* 2015). Additional mechanisms have also been proposed in supporting the authentication such as hashing and encryption and have been proven to strengthen the multi-factor authentication. The inclusion of these supporting mechanisms must be justified prudently based on the need and demand of the mobile system environment.

Having mobile apps provided with strong user authentication factors alone does not mean users will accept the apps. The selection of user authentication factors must consider the acceptability or usability by users (Bruun *et al.*, 2014; Seto *et al.*, 2015; Shay *et al.,* 2016). Among problems that users face to run mobile apps are constraint power (Ahmad *et al.,* 2015) and memory capacities (Chen and Girod, 2014). To run mobile apps, adequate storages of power supply and memory space are required. However, mobile phones can run out of power supply and memory space after sometimes and they cannot be operated until the batteries are recharged and memory spaces are restored. This means mobile phone could have constrain power or memory capacities at a certain time which is critical to run mobile apps. Thus, having a user authentication that requires less power supply and memory space will be an advantage.

Even though strong user authentication requires more factors, the authentication should not make it more difficult to use such as having additional user interventions. Users might be reluctant to use the apps if they have to key in more data every time to login the apps. To make it acceptable to users, the user authentication should be made without additional user interventions.

The above matters are some of the issues that need to be tackled when introducing a user authentication model for mobile apps that deals with very sensitive or confidential data or information.

1.3 Objectives

The main objective of this study is to improve the user authentication for mobile apps by strengthening the user authentication and analyze the level of acceptability among mobile users.

1.4 Research Scope

In mobile communication environment, there are several number of uncontrolled parameters that may affect the validation results. Thus, the following considerations have to be taken to limit the scope of research.

The factors for user authentication can be categorized into text based and non-text based. However, this study only focuses on text based factors because non-text based factors such as biometrics can have several disadvantages such as additional hardware installation, unstable accuracy, and low speed (Meng *et al.*, 2015). Furthermore, non-text based factors are made of images, videos or sound which may require high computational cost (Zhou, *et al.*, 2009). Text based factors are considered for improvement in this study to ensure less power supply and memory space are required.

System’s performance based on various geographical locations will not be analyzed in this research since they have many uncontrolled parameters that can affect the quality of services (QoS) in data transmission such as traffic congestions, network coverage, distances, etc.

1.5 Organization of the Thesis

This thesis consists of Chapter 1 to Chapter 6 and each of the chapters has the following descriptions:

Chapter 1 explains about the overview, problem statement, objectives and research scope.

Chapter 2 describes about literature review related to user authentication and ciphering techniques. The use of watermark is also reviewed.

Chapter 3 describes about the methodology of research which details out the research process.

Chapter 4 elaborates the proposed improvement for user authentication model which includes the techniques of multi-factoring, ciphering, and watermarking.

Chapter 5 explains on the results and discussions related to testing and analysis carried out to measure the improved performance of the proposed model.

Chapter 6 summarizes and concludes the research findings as well as describes the recommendations for future research.

REFERENCES

Acharya, D., & Kumar, V. (2011). Security of MBAN based Health Records in Mobile Broadband Environment. *The 8th International Conference on Mobile Web Information Systems, 5*, 539–545.

AES Encryption. (n.d.). Retrieved December 26, 2017, from AES Encryption: https://aesencryption.net/#PHPaesencryptionexample

Ahmad, R. W., Gani, A., Hamid, S. H., Xia, F., & Shiraz, M. (2015). A Review on Mobile Application Energy Profiling: Taxonomy, StateoftheArt, and Open Research Issues. *Journal of Network and Computer Applications*(58), 2459.

Ahrens, A., & Zascerinska, J. (2014). A Framework for Selecting Sample Size in Educational Reserach on ebusiness Application. *11th International Conference on eBusiness (ICEB)* (pp. 3946). IEEE Conference Publications.

Alkandari, A. A., AlShaikhli, I. F., & Alahmad, M. A. (2013). Cryptographic Hash Function: A High Level View. *International Conference on Informatics and Creative Multimedia (ICICM)* (pp. 128134). IEEE.

Alshaikhli, I. F., Alahmad, M. A., & Munthir, K. (2012). Comparison and Analysis Study of SHA3 Finalists. *International Conference on Advanced Computer Science Applications and Technologies (ACSAT)* (pp. 366371). IEEE Conference Publications.

Bartlett, J. E., Kotrlik, J. W., & Higgins, C. C. (2001). Orgazinational Research: Determining Appropriate Sample Size in Survey Research. *Information Technology, Learning and Performance Journal, 19*(1), 4350.

Bawaskar, S., & Verma, M. (2016). Enhanced SSO based Multi-Factor Authentication for Web Security. *International Journal of Computer Science and Information Technologies (IJCSIT), 7*(2), 960966.

Belkhede, M., Gulhane, V., & Bajaj, P. (2012). Biometric Mechanism for Enhanced Security of Online Transaction on Android System: A Design Approach. *ICACT*, 11931197.

Bhattarai, S., Ge, L., & Yu, W. (2012). A Novel Architecture against False Data Injection Attacks in Smart Grid. *Communication and Information Systems Security Symposium*, 907911.

Bluman, A. G. (2012). *Elementary Statistics, A Step by Step Approach* (7th ed.). New York: McGraw Hill.

Bruun, A., Jensen, K., & Kristensen, D. (2014). Usability of Single and Multi-factor Authentication Methods on Tabletops: A Comparative Study. *International Federation for Information Processing*, 299306.

Chen, D. M., & Girod, B. (2014). MemoryEfficient Image Databases for Mobile Visual Search. *IEEE Xplore*, 1423.

Cox, I. J., & Miller, M. L. (1997). A Review of Watermarking and the Importance of Perceptual Modeling. *To appear in the Proceeding of Electronics Imaging 1997.* Princeton, NJ 08540: NEC Research Institute.

Dahal, R. K., Bhatta, J., & Dhamala, N. (2013). Performance Analysis of SHA2 and SHA3 Finalist. *International Journal on Cryptography and Information Security (IJCIS), 3*(3), 110.

Das, A. K., Odelu, V., & Goswami, A. (2014). A Robust and Effective SmartCardBased Remote User Authentication Mechanism Using Hash Function. *The Scientific World Journal* , 116.

Das, M. L. (2009). TwoFactor User Authentication in Wireless Sensor Networks. *IEEE Transaction on Wireless Communications, 8*(3), 10861090.

Debiez, J., Hughes, P., & Apvrille, A. (2003, Oct 28). *Patent No. US 6,640,294 B2 .* U.S.A.

Delice, A. (2010). The Sampling Issues in Quantitative Research. *Educational Sciences: Theory and Practice, 10*(4), pp. 20012018.

Dilli, R., & Reddy, P. C. (2016). Implementation of Security Features in MANETs using SHA3 Standard Algorithm. *International Conference on Computational System and Information System for Sustainable Solutions*, 455458.

Dunkelman, O., Keller, N., & Shamir, A. (2015). Improved SingleKey Attacks on 8Round AES192 and AES256. *Journal of Cryptology, 28*, 397422.

Edward, S., Sumathi, S., & Ranihemamalini, R. (2011). Person Authentication Using Multimodal Biometrics With Watermarking. *International Conference on Signal Processing, Communication, Computing and Networking Technologies* (pp. 100104). IEEE.

Elanis. (20172018). *Dehash.me*. Retrieved January 10, 2018, from Dehash.me Hash texts and reverse hashes instantly!: https://dehash.me

Elkhodr, M., Shahrestani, S., & Kourouche, K. (2012). A Proposal to Improve the Security of Mobile Banking Applications. *Tenth International Conference on ICT and Knowledge Engineering* (pp. 260265). IEEE.

Fellegi, I. P. (2003). *Survey Methods and Practices.* Ministry of Industry. Ottawa: Authority of the Minister Responsible for Satistics Canada.

Fingerprint Clipart. (n.d.). Retrieved November 13, 2017, from Clipart Library: http://clipartlibrary.com/fingerprintclipart.html

George, D., & Mallery, P. (2013). *IBM SPSS Statistics 21 Step By Step: A Guide and Reference* (13th ed.). Pearson.

Gliem, J. A., & Gliem, R. R. (2003). Calculating, Interpreting and Reporting Cronbach's Alpha Reliability Coefficient for LikertType Scales. *Midwest Research to Practice Conference in Adult, Continuing and Community Education*.

Gordon, M., & Sankaranarayanan, S. (2010). Biometric Security Mechanism in Mobile Payments. *IEEE*.

Guildford, J. P. (1973). *Foundamental Statistics in Psychology and Education* (5th ed.). New York, USA: McGrawHill.

Harjito, B., Potdar, V., & Singh, J. (2012). Watermarking Technique for Copyright Protection of Wireless Sensor Network Data using LFSR and Kolmogorov Complexity. *MoMM2012* (pp. 208217). Bali, Indonesia: ACM.

HernándezRamos, J. P., MartinezAbad, F., & Garcia, F. J. (2012). Teacher Attitude Scale Regarding the Use of ICT. Reliability and Validity Study. *International Symposium on Computers in Education (SIIE)* (pp. 16). IEEE Conference Publications.

Hong, S. (2015). Multi-Factor User Authentication on Group Communication. *Indian Journal of Science and Technology, 8*(15), 16.

How do I locate my phone's IMEI number? (n.d.). Retrieved November 13, 2017, from Samsung: http://www.samsung. com/au/support/skp/faq/1039431

Hsu, C. L., & Lin, J. C. (2015). What Drives Purchase Intention for Paid Mobile Apps? – An expectation. *Electronic Commerce Research and Applications, 14*, 46–57.

Jankoviü, D. (2012). Key Security Measures for Personal Data Protection in IT Systems. *20th Telecommunications forum TELFOR 2012* (pp. 7982). Serbia, Belgrade: IEEE.

Li, C. T., & Lee, C. C. (2012). A Novel User Authentication and Privacy Preserving Scheme with Smart Cards for Wireless Communications. *Mathematical and Computer Modelling, 55*, pp. 3544.

Liao, K. C., & Lee, W. H. (2009). A OneTime Password Scheme with QRCode Based on Mobile Phone. *Fifth International Joint Conference on INC, IMS and IDC*, (pp. 20692071).

Liaw, H. T., Lin, J. F., & Wu, W. C. (2006). An Efficient and Complete Remote User Authentication Scheme Using Smart Cards. *Mathematical and Computer Modelling, 44*(12), 223228.

Liu, Q., Su, J. W., Wang, B. W., Jian, S., & Linge, N. (2013). An MSB Embedding Approach to Data Integrity Protection in a Ubiquitous Environment. *IEEE*, 97100.

Mallat, N., Rossi, M., Tuunainen, V. K., & Oorni, A. (2009). The Impact of Use Context on Mobile Services Acceptance: The Case of Mobile Tickecting. *Information and Management*, 190195.

Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the Development of Biometric User Authentication on mobile Phones. *IEEE: Communication Surveys and Tutorials*, 12681293.

Mun, H., Han, K., Lee, Y. S., Chan, Y. Y., & Choi, H. H. (2012). Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Mathematical and Computer Modeling, 55*, 214222.

Olson, K. (2010). An Examination of Questionnaire Evaluation by Expert Reviewers. *Field Methods, 22*(4), 295318.

Oxford. (2001). Research Design in Qualitative Analysis. Studies in Comparative International Development. *33*, 1845.

Panahy, P. H. (2014). Model for Assessing Relationship between Data Quality Dimensions and Improvement Progress in Information Systems. PhD Thesis, Universiti Putra Malaysia.

Parker, C. (2017, August 24). *Kit Guide: finding your SIM card number Android*. Retrieved November 13, 2017, from Team Know How: https://www.teamknowhow.com/kitguide/phones /smartphones/samsung/galaxys8/findyoursimcardnumberonandroid

PHP: HashManual. (n.d.). Retrieved December 26, 2017, from Php.net: php.net/manual/en/function.hash.php

Powell, D. (1991). Delta4: A Generic Architecture for Dependable Distributed Computing. In *Research Reports ESPRIT* (pp. 343348). France: SpringerVerlag.

Provelengios, G., Sklavos, N., Kitsos, P., & Koulamas, C. (2012). FPGABased Design Approaches of Keccak Hash Function. *15th Euromicro Conference on DIgital System Design*, (pp. 649653).

Ratna, A. A., Shaugi, A., Purnamasari, P. D., & Salman, M. (2013). Analysis and Comparison of MD5 and SHA1 Algorithm Implementation in SimpleO Authentication based Security System. *IEEE*, 99104.

Roy, S., & Manasmita, M. (2011). A Novel Approach to Format Based Text Steganography. *Proceedings of the 2011 International Conference on Communication, Computing & Security*, pp. 511516.

Sadikin, M., & Wardhani, R. W. (2016). Implementation of RSA 2018bit and AES 256bit with Digital Signature for Secure Electronic Health Record Application. *International Seminar on Intelligent Technology and Its Application* (pp. 387392). IEEE.

Salimin, N. (2015). *F024 IPSA Evaluation Technical Report uSignMf+.* Selangor, Malaysia: CyberSecurity Malaysia MySEF.

Sanou, B. (2013). *The World in 2013: ICT Facts and Figures.* Retrieved December 29, 2017, from International Telecommunications Union (ITU): https://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2013e.pdf

Sanou, B. (2015). *The World in 2015: ICT Facts and Figures.* Retrieved November 13, 2017, from International Telecommunications Union (ITU): https://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2015.pdf

Schierz, P. G., Schilke, O., & Wirtz, B. W. (2010). Understanding Consumer Acceptance of Mobile Payment Services: An Empirical Analysis. *Electronic Commerce Research and Applications*, 209216.

Schneider, D. (2012). The State of Network Security. *Network Security*, pp. 1420.

Seto, J., Wang, Y., & Lin, X. (2015). UserHabitOriented Authentication Model: Toward Secure, UserFriendly Authentication for Mobile Devices. *Emerging Topics in Computing, 3*(1), 107118.

Shay, R., Komanduri, S., Durity, A. L., Huh, P. S., Segreti, S. M., Ur, B., et al. (2016, May). Designing Password Policies for Strength and Usability. *Transactions on Information and System Security, 18*(4), 13.113.34.

Shen, Z., Shu, J., & Xue, W. (2017). Keyword Search With Access Control Over Encrypted Cloud Data. *Sensors Journal*, 858868.

Shukla, S. S., Singh, S. P., Shah, K., & Kumar, A. (2012). Enhancing Security & Integrity of Data Using Watermarking & Digital Signature. *International Conference on Recent Advances in Information Technology (RAIT).* IEEE.

Sklavos, N., Alexopoulos, A., & Koufopavlou, O. (2003, July). Networking Data Integrity: High Speed Architectures and Hardware Implementations. *The International Arab Journal of Information Technology, 1*(0), 5459.

Supian, S. R. (2015). Influence of Human Resource Practices on Talent Retention of Professional and Management Staff in a Malaysian Public University. Master Thesis, Universiti Putra Malaysia.

Tabachnik, G. B., & Fidel, S. L. (2007). *Using Multivariable Statistics* (5th ed.). New York: Pearson Edicational Inc.

Tsai, C. L., Lin, U. C., Chang, A., & Chen, C. J. (2010). Information Security Issue of Enterprises Adopting the Application of Cloud Computing. *IEEE*, (pp. 645649).

Vundela, P., & Sourirajan, V. (2011). A Robust MultiwaveletBased Watermarking Scheme for Copyright Protection of Digital Image Using Human Visual System. *IAJIT First Online Publication*.

Wertz, R. E. (2014). What is Learning Presence and What Can it Tell Us About Success in Learning Online? *IEEE Frontiers in Education Conference (FIE) Proceedings* (pp. 16). IEEE Conference Publications.

What is the difference of AES128 and AES512 using php's mcrypt? (n.d.). Retrieved December 26, 2017, from SitePoint Pty Ltd: https://www.sitepoint.com/community/t/whatisthedifferenceofaes128andaes512usingphpsmcrypt/207726

Xing, Y. Y., Jiang, P., & Cheng, Z. J. (2016). The Determinination Method on Products Sample Size Under the Condition of Bayesian Sequential Testing. *Proceeding of the 2016 IEEE IEEM* (pp. 16351639). IEEE.

Yang, S., Lu, Y., Gupta, S., Cao, Y., & Zhang, R. (2012). Mobile Payment Services Adoption Across Time: An Empirical Study of The Effects of

Behavioral Beliefs, Social Influences and Personal Traits. *Computers in Human Behavior*, 129142.

Ying, H. M., & Kunihiro, N. (2016). Decryption of Frequent Password Hashes in Rainbow Tables. *Fourth International Symposium on Computing and Networking (CANDAR)* (pp. 655661). IEEE Conference Publications.

Yoon, E. J., Yoo, K. Y., & Ha, K. S. (2011). A User Friendly Authentication Scheme with Anonymity for Wireless Communications. *Computers and Electrical Engineering, 356–364*, 356–364.

Zhao, M., Li, Z., Wang, Y., & Xu, Q. (2016). Longest Common Subsequence Computation and Retrieve for Encrypted Character Strings. *19th International Conference on NetworkBased Information Systems (NBiS)* (pp. 496499). IEEE Conference Publications.

Zhou, L., & Zhang, Z. (2012). A Secure Data Transmission Scheme for Wireless Sensor Networks Based on Digital Watermarking. *9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, 20972101.

Zhou, Y., Panetta, K., & Agaian, S. (2009). Image Encryption Using Binary KeyImages. *International Conference on Systems, Man and Cybernetics* (pp. 45694574). San Antonio, TX, USA: IEEE.