ISSN 2278-3091
Volume 8, No.1.4, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse7481.42019.pdf
https://doi.org/10.30534/ijatcse/2019/7481.42019

An Improved User Authentication Model for Mobile Application Systems: An Expert Review Verification

Kartini Mohamed[1], Fatimah Sidi[2], Iskandar Ishak[2], Marzanah A. Jabar[2], Siti Raba'ah Hamzah[3]
[1]Group Human Resource, SIRIM Berhad, No.1, Persiaran Dato' Menteri, Peti Surat 7035, Section 2, 40700 Shah Alam, Selangor, Malaysia, kartinim@sirim.my
[2]Faculty of Computer Science and Information Technology, University Putra Malaysia, 43400 Serdang, Selangor, Malaysia, fatimah@upm.edu.my, iskandar_i@upm.edu.my, marzanah@upm.edu.my
[3]Department of Professional Development and Continuing Education, Faculty of Educational Studies, University Putra Malaysia, 43400 Serdang, Selangor, Malaysia, srh@upm.edu.my
Corresponding author E-mail: fatimah@upm.edu.my

ABSTRACT

Mobile application systems (mobile apps) are now being commonly installed in smart phones or mobile devices. Many of these mobile apps are dealing with sensitive or confidential information that requires good protection using strong user authentication. This study has proposed an improved user authentication model which is aimed not only to obtain strong user authentication but also to be acceptable by users. The strong user authentication is achieved using the combination of three security techniques namely multi-factoring, ciphering and watermarking techniques while the level of acceptance by users is measured using a quantitative research method. This method consists of three research instruments namely expert review, pilot study and survey. However, this paper only focuses on how the expert review is being carried out to obtain the consent whether the proposed model is valid and feasible. Questionnaires for the expert review are constructed based on the model being proposed including the techniques and targeted benefits. From the review results, a modification is required related to the number of expert reviewers to be increased. Others are just suggestions which are not critically affecting the study. With this modification being done, and justifications being made, the expert reviewers finally agree that the proposed model is valid and feasible. This means the proposed model is capable in providing strong and acceptable user authentication for mobile apps.

Key words: Mobile Application System, Expert Review, User Authentication, Methodology, Mobile Security

1. INTRODUCTION

Communication using mobiles are vulnerable to hacking activities by intruders [1], [8], [11] which mean good protection is required for any communications done using mobile devices including mobile phones. Mobile apps are among those that require such protection. The protection of mobile apps can be obtained by using strong user authentication such as multi-factor user authentication [1], [11], [5]. This means more than the normal single-factor (e.g. password) being used. Many other factors being proposed by researchers and some of them are location signature and time [1], IMEI and SIM Card Numbers [11], and biometric and pin number [5]. Since mobile devices are detached from the main storages, they have limited power supply and memory space and depend so much on the local battery power and data storage capacities. Thus, the types of user authentication to be selected must also consider these constraints [1], [16], [10]. Therefore, the use of text-based user authentication is recommended and non-text based data which use high processing power and memory space such as images, photos, videos or sound should be avoided. However, each set of multi-factor user authentications has its own strengths and weaknesses [12]. To compensate these potential weaknesses, the data should be ciphered with hash and encryption [3], [6], [9], [10]. Watermarking is another protection that can be applied to make the user authentication strong by means of resistible to alterations [2] and providing data integrity [4], [7]. Therefore, the techniques of multi-factoring, ciphering and watermarking are proposed in the improved user authentication model in this study. The objective of the improved model is to achieve not only strong but also acceptable user authentication by users. The achievement level for the technical strength is validated based on testing done on prototype mobile apps while the user's perceptions on strength and acceptance are evaluated using a quantitative research method. There are three instruments adopted in this research method namely expert review, pilot study and survey and this paper only focuses on how expert review is performed. Expert review is necessary to get verifications from the experts in the related field [13]. Pilot study, however, is carried out as a feasibility study since no commonness is known about the characteristics of a survey while the survey is performed to collect the information about the characteristics of the population being studied [14].

Next section explains on each of the techniques being applied in the improved user authentication model. It is followed by the sections that describe about the expert review methodology. Results and discussion is explained in the following section. Finally, the paper concludes the expert review methodology in this study.

2. IMPROVED USER AUTHENTICATION MODEL

The user authentication model proposed in this study has been adopted from several models proposed by the previous researchers such as [11] as shown in Figure 1 and [10] and [9] as per Figure 2. However, the model proposed

in this study not only combining the multi-factoring and ciphering techniques proposed by the above researchers but also adding another security technique known as watermarking technique to make the model even stronger. The above researchers claim that their models are strong but never tested whether they are acceptable by users. The model proposed in this study not only has additional watermarking techniques but also has the confirmation that the model is strong and acceptable by users as indicated in Figure 3. However, the server authentication proposed by [11] is excluded from the scope of this study since it does not involve with authentication within mobile devices. study and survey. A set of questions or a questionnaire is prepared for the expert reviewers to answer and verbal explanation on the background information is given to them prior to answering the questionnaire. The questionnaire, which is partly derived from [15], are categorized into three parts with three different objectives as listed in Table 1.

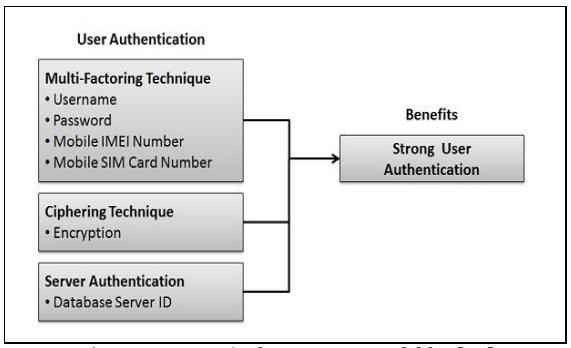

Figure 1: User Authentication Model by [11]

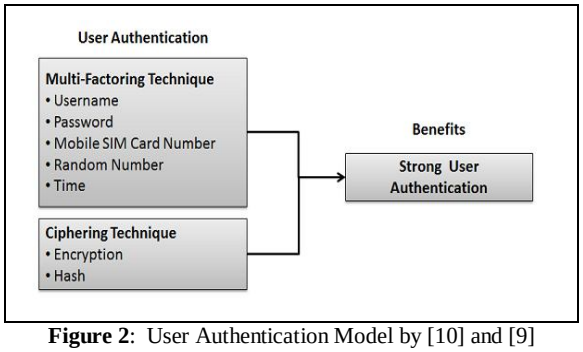

Figure 2: User Authentication Model by [10] and [9]

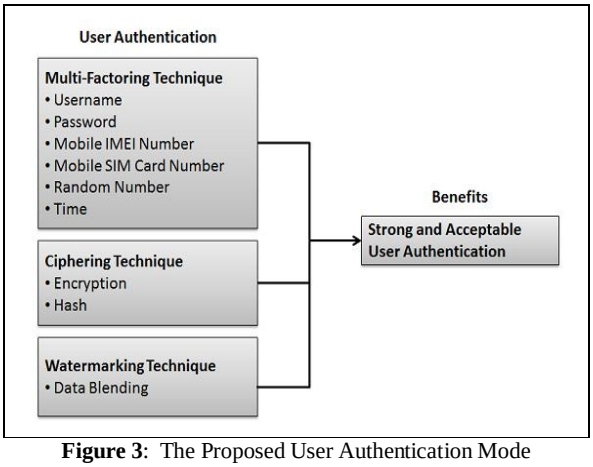

Figure 3: The Proposed User Authentication Mode

Next section explains on how the expert review methodology is performed to confirm the validity and feasibility of the user authentication model proposed in this study.

3. EXPERT REVIEW DEVELOPMENT

Expert review is a method that is used to evaluate and verify the proposed model before any survey is carried out [13]. The aim of expert review in the context of this study is to let the experts confirm the validity and feasibility of the proposed model. The experts are selected based on the minimum three years of experience in the related field and independent from the groups who participate in the pilot

Table 1: Objective of Each Part of the Questions

Part No.	Objective
1	To verify the feasibility and applicability of the proposed model
2	To validate the model in terms of its comprehensiveness, understandability, correctness and coherent
3	To verify the validity of the user authentication model

Each part consists of several questions that must be responded with one of three options given below:

Option 1: Yes, without modification
Option 2: Yes, with modification
Option 3: No

Option 1 means the experts totally agree with the statement given. Option 2 allows the experts to give comment on how the questions could be improved even if they partially agree with the statement. However, Option 3 is to be selected if the experts do not agree with the statement. Comments and suggestions are also required to clarify on the error and rectify weaknesses of the statements where possible.

Table 2: Part 1 of the Expert Review Questionnaire

Question No.	Statement Details
1	Does the model (multi-factoring technique, ciphering technique, watermarking technique, and the outcomes of strong and acceptable) is perceived useful?
2	Are the multi-factoring technique, ciphering technique, watermarking technique, and the outcomes of strong and acceptable clear and understandable?
3	Do the multi-factoring technique, ciphering technique, and watermarking technique good enough to support the achievement of the outcomes of strong and acceptable?
4	Comparing with existing user authentication models by Elkhodr *et al*. (2012), Yoon *et al*. (2011) and Li and Lee (2012), does the proposed model answers the gap in the knowledge?
5	Is the model easy to implement?
6	Does the model cover sufficient variables to provide practical outcomes of strong and acceptable?
7	Can the model generate strong and

	acceptable outcomes of strong and acceptable?
8	Are the factors and techniques in the proposed model adequate and sufficient?
9	In term of the model's outcomes of strong and acceptable, do they provide the expected results?

Table 3: Part 2 of the Expert Review Questionnaire

Question No.	Statement Details
1	Is the proposed model correct?
2	Comparing with existing models, does the proposed model achieve satisfaction by providing stronger user authentication?
3	Is the proposed model complete?
4	Is the structure of the proposed model consistent and well organized?
5	The model is easy to implement?
6	Are the factors and techniques in the proposed model valid and sufficient?
7	Is the proposed model satisfactory for designed purposes?

Table 4: Part 3 of the Expert Review Questionnaire

Question No.	Statement Details
1	Are the proposed data collection and analysis methods enough to evaluate the proposed user authentication model?
2	Are the proposed data evaluation methods adequate to achieve precise evaluation?
3	Are the data collection and analysis methods consistent and compatible with the goals of the study?
4	Is the number of respondents enough to suggest an evaluation could be performed adequately?
5	Do you think data collection method is sufficient?
6	Are the introduced factors and techniques adequate to validate the proposed user authentication in this study?

Table 2, Table 3 and Table 4 shows the three parts of the questions provided to the expert reviewers.

Table 5: List of Expert Reviewers

Expert Review No.	Expert Field	Years of Experience
ER1	Cyber Security	8
ER2	IT Infrastructure	14
ER3	Network and Server Administrator	14
ER4	Evaluator of ICT Products	3
ER5	Evaluator of IT Security Products	5

A total of five expert reviews from three different institutions were selected in this study which include a public high educational institution in Malaysia, an institute responsible for doing research and standards for Malaysian government and industries, and a technical agency under The Ministry of Science, Technology and Innovations that has been appointed as the National Body to monitor National e-security aspect and responsible for ensuring safe and secure cyberspace. All the reviewers are experts in different field to ensure feedbacks given are based of vast background knowledge. The minimum number of years' experience is decided to be 3 since young people are normally more adventurers in information technologies. The list of expert reviewers selected in this study is as indicated in Table 5. The whole process of conducting the expert review is summarized in Figure 4.

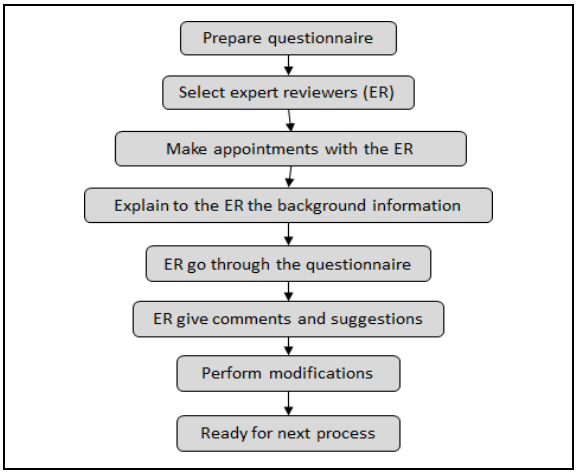

Figure 4: The Expert Review Development Process

4. RESULTS AND DISCUSSIONS

The responses form the expert reviews are collected immediately after the completion of the forms which are summarized in Table 6.

Table 6: Responses Received from the Expert Reviewers

Part No.	Question No.	ER1	ER2	ER3	ER4	ER5
1	1	1	1	1	1	1
	2	1	1	1	1	1
	3	1	1	1	1	1
	4	1	1	1	1	1
	5	1	1	1	1	2
	6	1	1	1	1	1
	7	1	1	1	1	1
	8	1	1	1	1	1
	9	1	1	1	1	1
2	1	1	1	2	1	1
	2	1	1	1	1	1
	3	1	1	1	1	1
	4	1	1	1	1	1
	5	1	1	2	1	2
	6	1	1	1	1	1
	7	1	1	1	1	1
3	1	1	1	1	1	2
	2	1	1	1	1	1
	3	1	1	1	1	2
	4	1	1	3	1	2
	5	1	1	1	1	1
	6	1	1	1	1	1

In Part 1 of the questions, all of the reviewers have chosen Option 1 except one reviewer has chosen Option 2 for Question No. 5 because he believes that the proposed model is not easy to implement due to users still need to fulfill the standard requirements and specification such as keying in username and password. However, these data are the basic information that users need to provide, and they are not required to key in any additional data. This means, the proposed model is still easy to implement as other existing models.

In Part 2, one of the reviewers has chosen Option 2 for Question 1 and 2 reviewers have chosen Option 2 for Question 5. The word 'correct' in Question 1 has made the reviewer feel ambiguous but no suggestion given to change it to a better word. Since majority of the reviewers have no problem with it, the word 'correct' is maintained in the question. Option 2 has been given for Question 5 because the reviewers believe that the model is not easy to be constructed by the developers. They believe that additional processes and phases may be required during the development stage. However, there is some confusion by the statement because it has been meant to be easy implementation by the users and not the developers. The statement may need to be changed so that nobody thinks that it is meant for the developers.

Part 3 of the questions has 1 reviewer who has chosen Option 3 for Question 4 and 1 reviewer who has chosen Option 2 for Question 1, 3 and 4. This means 2 of the reviewers do not agree with number of respondents of only 3 for expert review process (this number has been initially decided prior to the implementation of the expert review process). Due to this comment, the number of expert reviewers is then increased to 5 persons. One of the reviewers does not fully agree with Question 1 because he thinks that more experts should be chosen from the field related to mobile apps. He also partially agrees that the data collection analysis method consistent and compatible with the goals of the study. However, he suggested that the timeline should be included for easy monitoring of the system development progress.

The results of all the above parts indicate that majority of the reviewers agree with all of the questions given. This demonstrates that the model is feasible and applicable to provide a strong and acceptable user authentication model which means Pilot Study and Survey can be executed for further data collection and analysis for this study.

5. CONCLUSION

Any proposed user authentication model that is to be applied in mobile apps should has the intention to make the user authentication not only strong but also acceptable by mobile phone users. For this reason, this study has proposed to combine several protection techniques which include multi-factoring, ciphering and watermarking techniques. The strength of the prototype apps has been tested and proven acceptable by an independent testing body. To measure the level of user acceptance, a quantitative research method is applied which consist of three instruments - expert review, pilot study and survey. However, only expert review is being focused in this paper. Based from the responses from the expert reviewers, it is concluded that the proposed model is feasible with only a few modifications to be done. The main modification is adding the number of expert reviewers. The others are related to the rewording of the questions to avoid confusions. Once the modifications are completed, the pilot study and survey can be preceded to complete the research method used in this study.

ACKNOWLEDGEMENT

The work reported here is funded by the Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme (FRGS 03-12-10-999FR). Mygrants Reference Code is FRGS/2/2014/ICT07/UPM/02/1. This support is gratefully acknowledged.

REFERENCES

[1] D. Acharya and V. Kumar, **Security of MBAN based Health Records in Mobile Broadband Environment,** *The 8th International Conference on Mobile Web Information Systems*, vol. 5, p. 539–545, 2011. https://doi.org/10.1016/j.procs.2011.07.070

[2] I. J. Cox and M. L. Miller, **A Review of Watermarking and the Importance of Perceptual Modeling,** in *To appear in the Proceeding of Electronics Imaging 1997*, Princeton, NJ 08540, 1997. https://doi.org/10.1117/12.274502

[3] M. Gordon and S. Sankaranarayanan, **Biometric Security Mechanism in Mobile Payments,** *IEEE*, 2010. https://doi.org/10.1109/WOCN.2010.5587318

[4] Q. Liu, J. W. Su, B. W. Wang, S. Jian and N. Linge, **An MSB Embedding Approach to Data Integrity Protection in a Ubiquitous Environment,** *IEEE*, pp. 97-100, 2013.

[5] W. Meng, D. S. Wong, S. Furnell and J. Zhou, **Surveying the Development of Biometric User Authentication on mobile Phones,** *IEEE: Communication Surveys and Tutorials*, pp. 1268-1293, 2015. https://doi.org/10.1109/COMST.2014.2386915

[6] H. Mun, K. Han, Y. S. Lee, Y. Y. Chan and H. H. Choi, **Enhanced secure anonymous authentication scheme for roaming service in global mobility networks,** *Mathematical and Computer Modeling*, vol. 55, pp. 214-222, 2012.

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

[8] M. Belkhede, V. Gulhane and P. Bajaj, **Biometric Mechanism for Enhanced Security of Online Transaction on Android System: A Design Approach,** *ICACT*, pp. 1193-1197, 2012.

[9] C. T. Li and C. C. Lee, **A Novel User Authentication and Privacy Preserving Scheme with Smart Cards for Wireless Communications,** *Mathematical and Computer Modelling*, vol. 55, pp. 35-44, 2012. https://doi.org/10.1016/j.mcm.2011.01.010

[10] E. J. Yoon, K. Y. Yoo and K. S. Ha, **A User Friendly Authentication Scheme with Anonymity for Wireless Communications,** *Computers and Electrical Engineering*, vol. 356–364, p. 356–364, 2011.

[11] M. Elkhodr, S. Shahrestani and K. Kourouche, **A Proposal to Improve the Security of Mobile Banking Applications,** in *Tenth International Conference on ICT and Knowledge Engineering*, 2012. https://doi.org/10.1109/ICTKE.2012.6408565

[12] J. Seto, Y. Wang and X. Lin, **User-Habit-Oriented Authentication Model: Toward Secure, User-Friendly Authentication for Mobile Devices,** *Emerging Topics in Computing*, vol. 3, no. 1, pp. 107-118, 2015. https://doi.org/10.1109/TETC.2014.2379991

[13] K. Olson, **An Examination of Questionnaire Evaluation by Expert Reviewers,** *Field Methods*, vol. 22, no. 4, pp. 295-318, 2010. https://doi.org/10.1177/1525822X10379795

[14] I. P. Fellegi, **Survey Methods and Practices,** Authority of the Minister Responsible for Satistics Canada, Ottawa, 2003.

[15] P. H. S. Panahy, **Model for Assessing Relationship between Data Quality Dimensions and Improvement Progress in Information Systems,** PhD Thesis, Universiti Putra Malaysia, 2014.

[16] Y. Zhou, K. Panetta and S. Agaian, **Image Encryption Using Binary Key-Images,** in *International Conference on Systems, Man and Cybernetics*, San Antonio, TX, USA, 2009. https://doi.org/10.1109/ICSMC.2009.5346780