International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

An Improved User Authentication Model for Mobile Application Systems: Statistical Assessment of User Acceptance

Kartini Mohamed, Fatimah Sidi, Iskandar Ishak, Marzanah A. Jabar, SitiRaba’ahHamzah

Abstract: One of the reasons mobile phones become one of the worldwide commonly usedcommunication devices nowadays is because they allow the installation of various mobile apps which are mostly interesting and useful to mobiles users. Unfortunately, mobile apps involve transmissions of digital data wirelessly and vulnerable to hacking activities. An improved user authentication modelhas been introduced in this study. Its strength in preventing hacking activities and the level of user acceptance are being analyzed. The strength is built based on the multi-factoring, ciphering and watermarking techniques being introduced in the model. It is technically measured based on the vulnerability and penetration tests done by an appointed independent party but excluded in this paper. On the other hand, the level of acceptance is measured using a quantitative method. Even though the quantitative method in this study undergoes expert review, pilot study and survey, this paper only focuses on the survey since its outcome is used to conclude the level of acceptance by mobile users. The statistical analysis results indicate that mobile users perceive ciphering technique contributes the most to this strength while watermarking technique has the strongest relationshipsandbecome the dominant factor in making the model acceptable by users.

Keywords: Mobile Application Systems, Survey, Quantitative Methodology, User Authentication

I.INTRODUCTION

Wireless communications using mobile phones are not safe and have very high risk of being hacked if not properly protected (Acharya and Kumar, 2011; Belkhede*et al.*, 2012; Elkhart *al.*, 2012).The hackers may intrude to steal or sniff the information or data being communicated using mobile apps.The mobile communications involving the use of apps can be protected by controlling the access to the apps by using user authentication with unique username and password.

Realizing that hackers are getting more advanced, researchers haveproposed several ways to make the user authentication stronger.

One of the ways is using multi-factor user authentication which uses more than username and password as the authentication. Location signature and time (Acharya and Kumar, 2011), IMEI and SIM Card Numbers (Elkhodr*et al.*, 2012), biometric and pin number (Meng*et al.*, 2015) are among the proposed elements of multi-factor user authentication.

However, the improved model in this study proposes several techniques to make the authentication stronger besides the multi-factor user authentication. The model also requires using ciphering and watermarking besides multi-factoring techniques.

In multi-factoring technique, several elements including time, IMEI number, SIM Card number and random number are introduced besides username and password. Even though several elements are added, the users are not required to key in other than username and password because they are automatically generated by the mobile device and retrieved by the proposed system. Meanwhile the ciphering technique allows all the data to be encrypted and hashed so that they become unreadable even if they are being stolen or sniffed. Finally, they are being scrambledin a way that they are unable to be unscrambled without using the secret formula when the watermarking technique is being applied.

Even though the user authentication has been made stronger in the proposed model, it is meaningless if they proposed model is not accepted or usable by the users(Bruun *et al.*, 2014; Seto *et al.*, 2015; Shay *et al.*, 2016).For instance, the users may be reluctant to use any system if they experience difficulties, costly or time consuming. Thus, this study not only tests the strength of the proposed protection but also measures the level of acceptance by users. The strength is being tested using vulnerability and penetration tests by the third party who is independent from the system while the level of acceptance is being measured using a quantitative method. However, the strength test results are not within the scope in this paper.

In this study the quantitative method consists of an expert review, a pilot study and a survey. The expert review is performed to get a consentfrom the experts in the related field while the pilot study is carried out to do a pre-evaluation of the survey questions. In the pilot study, any doubted questions are being fine-tuned to ensure they are reliable when being used for the survey. This paper explains in more details on how the survey is being done and how the analysis is carried out to conclude the level of acceptance by users.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author
Kartini Mohamed*, Group Human Resource, SIRIM Berhad, No.1, PersiaranDato’ Menteri, PetiSurat 7035, Section 2, 40700 Shah Alam, Selangor, Malaysia.
Fatimah Sidi, Department of Computer Science, Faculty of Computer Science and Information Technology, University Putra Malaysia, 43400 Serdang, Selangor, Malaysia.
Iskandar Ishak, Department of Computer Science, Faculty of Computer Science and Information Technology, University Putra Malaysia, 43400 Serdang, Selangor, Malaysia.
Marzanah A. Jabar, Department of Software Engineering and Information System, Faculty of Computer Science and Information Technology, University Putra Malaysia, 43400 Serdang, Selangor, Malaysia.
SitiRaba’ahHamzah, Department of Professional Development and Continuing Education, Faculty of Educational Studies, University Putra Malaysia, 43400 Serdang, Selangor, Malaysia.

Retrieval Number: A2658109119/2019©BEIESP
DOI: 10.35940/ijeat.A2658.109119
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

This paper is organized in the following sequence. Section 2 explains in detail on the quantitativemethod being conducted. Section 3 describes the results and the discussions of the survey while section 4 concludes the findings of the survey. The acknowledgement of those who involve in this study is elaborated in Section 5.

II.MATERIALS AND METHODS

The improved user authentication model proposed in this study consists of independent and dependent variables where the independent variables are made of multi-factoring, ciphering and watermarking techniques while dependent variables consists of strong and acceptable user authentication as depicted in Figure 1.

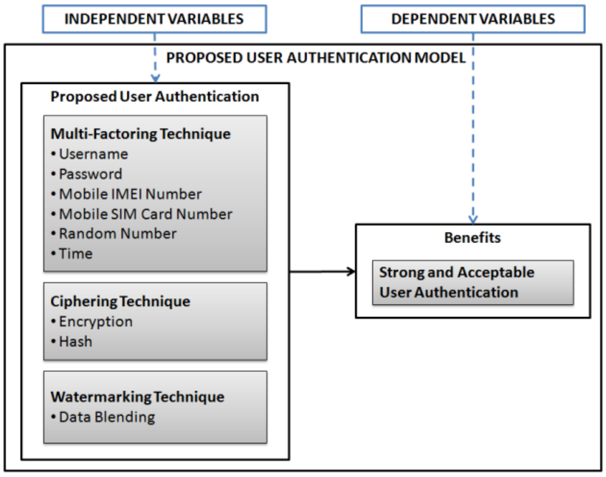

Fig. 1 The Improved User Authentication Model

Even though there are two benefits – strength and acceptability of user authentication, the survey being conducted only focuses on the acceptability level since the strength level is already being technically tested by an independent party. When performing the survey, survey forms are distributed to a group of mobile phone users. A total of 175 respondents are collected from 250 survey forms being distributed.Each survey form contains 21 questions or items derived from the pre-evaluation done in the pilot study, whichare divided into 5 components namely A, B, C, and D,as shown in Table 1. For each of the items, the respondents are given five (5) choices of answer. The answer should contain value one (1) to five (5) to represent "Strongly Disagree" to "Strongly Agree".

Table. 1 Components of Survey Questionnaire

No	Component Name	Component Description	No. of Items
1	A	Text-Based Multi-Factor User Authentication	6
2	B	Text Ciphering Technique	4
3	C	Data Watermarking Technique	4
4	D	Acceptable User Authentication	7
		Total	21

III.RESULTS AND DISCUSSION

The results of the survey are analyzed using a quantitative method which consists of 3 types of statistical analysis -(a) Descriptive Analysis, (b) Pearson Correlation, and (c) Multiple Linear Regressions.

Descriptive Analysis

Descriptive Analysis is applied to understand the level of agreements among the mobile phone users related to the proposed techniques of multi-factoring, ciphering and watermarking.In the descriptive analysis, each of the items in each of components A, B, C, and D is measured in terms of mean, standard deviation, level, and rank. The mean value is considered the highest if it is at the highest rank which starts with rank 1.In this analysis, level of agreement is determined based on three (3) categories namely low, moderate, and high with the minimum value range is set not less than one (1), and maximum range is not more than five (5). Therefore, the formula to set the range for each category should be set as

$(5-1) / 3 = 1.33$

based on the formula adopted by George and Mallery (2013). Thus, the three (3) levels of agreement should be obtained as per Table 2.

Table. 2 Ranges of Each Level

Level	Minimum	Maximum
Low	1	1 + 1.33 = 2.33
Moderate	2.34	2.33 + 1.33 = 3.66
High	3.67	5

Table 3 illustrates the results of the survey for components A, B and C which represent the independent variables and component D representsthe dependent variable in the model. The mean values are all above 3.67 which indicates high level of agreement. These illustrate that the respondents strongly agree with and accept the questions or items which support the statement that the use of multi-factoring, ciphering and watermarking techniques helps in making the user authentication stronger. Even though the three techniques make the user authentication stonger, the ranks indicate that the respondents feel that ciphering technique helps the most in making the user authentication stronger, followed by watermarking and multi-factoring techniques.

Table. 3 The Level of Variables (n=175)

Component Name	Component Description	Mean	Std. Deviation	Level	Rank
A	Text-Based Multi-Factor User Authentication	3.89	0.62	High	3
B	Text Ciphering Technique	4.16	0.72	High	1
C	Data Watermarking Technique	4.05	0.67	High	2
D	Acceptability of User Authentication	3.91	0.64	High	4

Note: Low (1 - 2.33), Moderate (2.34 - 3.66), High (3.67 - 5)

Pearson Correlation

This statistical analysis is applied to find the relationships between independent and dependent variables where the dependent variables are the benefits of implementing the independent variable.Therefore, the correlation between "Multi-Factoring, Ciphering, and Watermarking Techniques" and "Acceptability of User Authentication"needs to be analyzed. To find the relationships between the two variables, the Rule of Thumb by Guildford (1973) is adopted in which the r value represents the level of the relationships as shown in Table 4.

Table. 4 Interpretation of Correlation based on Rule of Thumb (Guildford, 1973)

Pearson (r)	Interpretation
0.0 ~ 0.29	Little or negligible relationship
0.3 ~ 0.49	Low relationship
0.5 ~0.69	Moderate or marked relationship
0.7 ~ 0.89	High relationship
0.9 ~1.0	Very high relationship

Based on Table5, the Y values, which represent the Pearson correlation, are between 0.5 and 0.69. This means the three techniques have moderate relationships with the acceptability of user authentication.Even though they have moderate relationships and their correlations are all significant, watermarking technique seems to have a higher acceptance value or correlation compared to those of ciphering and multi-factoring techniques.

Table. 5 Correlation between Independent Variables and Acceptability of User Authentication (n=175)

Variables	Y(Acceptance)
Y (Acceptance)	1.00
X1 (Multi-Factoring)	0.556**
X2 (Ciphering)	0.556**
X3 (Watermarking)	0.641**

*Note: ** Correlation is significant at the 0.01 level (2-tailed)*

Multiple Linear Regressions

Multiple Regression model is a suitable tool to identify the most dominant factor (Bluman, 2012). This analysis is used to find the dominant factor among the independent variables that contributes to the benefits or dependent variables in this study. The regression analysis is carried out for acceptability of user authentication and the results are as shown in Table 6.

Table. 6 Regression Coefficients for Acceptability of User Authentication

Proposed User Authentication Model		Un-standardized Coefficient		Standardized Coefficient	t	Sig. (*p*-value)
		B	Std. Error	Beta		
1	(Constant)	0.97	0.25		3.89	0.000
	Multi-Factoring	0.21	0.08	0.20	2.60	0.010
	Ciphering	0.13	0.07	0.14	1.76	0.080
	Watermarking	0.40	0.07	0.42	5.28	0.000

Dependent Variable: Acceptability of User Authentication, $R = 0.680$, $R^2 = 0.462$

The equation of the simple linear regression model is:

$Y_1 = B_0 + B_1X_1 + B_2X_2 + B_3X_3$

where,

Y_1 = Dependent variables
B_0 = Constant (Intercept)
B_{1-3} = Estimates (Regression Coefficients)
X_1, X_2, X_3 = Independent variables

Using the coefficients as provided in Table 6, the linear equation for the regression model is as follow, where Y_1 refers to regression coefficients for theacceptability and X_2 which represents the ciphering technique is not considered since it'snot significant due to p-value > 0.05.

$Y_1 = B_0 + B_1X_1 + B_3X_3$

$Y_1 = 0.97 + 0.21X_1 + 0.40X_3$

Mean while, the R-squared value indicates the percentage contribution of the independent variables towards the benefit or dependent variable. The R-squared value of 0.46 in

Retrieval Number: A2658109119/2019©BEIESP
DOI: 10.35940/ijeat.A2658.109119
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Table6 designates that the three independent variables contribute 46% toward the acceptability. The table also indicates that the watermarking technique is the dominat factor since the beta-value (B) and t-statistics (t) have the highest values followed by those of multi-factoring technique and ciphering technique.

IV.CONCLUSION

An improved user authentication model has been proposed in this study to better secure the access to mobile apps since communication using mobile apps involves wireless data transmission which is vulnerable to hacking activities. The acceptance of the model has been analysed using a quantitativemethod in which a survey is conducted with three (3) statistical analyses being performed namely, Descriptive Analysis, Pearson Correlation, and Multiple Linear Regression. The statistical anaylsis shows that eventhough the majority users agree that the three techniques helps in making the user authentication model acceptable by users, the ciphering technique is the highest contributor, while watermarking technique has the strongest relationship with the benefit of acceptability and becomes the dominat factor that contributes to the acceptability of the improved model.

ACKNOWLEDGMENT

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. 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.
2. Belkhede, M., Gulhane, V., & Bajaj, P. 2012. Biometric Mechanism for Enhanced Security of Online Transaction on Android System: A Design Approach. ICACT, 1193-1197.
3. Bluman, A. G. (2012). Elementary Statistics, A Step by Step Approach (7th ed.). New York: McGraw Hill.
4. 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, 299-306.
5. 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. 260-265). IEEE.
6. George, D., & Mallery, P. (2013). IBM SPSS Statistics 21 Step By Step: A Guide and Reference (13th ed.). Pearson.
7. Guildford, J. P. 1973. Foundamental Statistics in Psychology and Education (5th ed.). New York, USA: McGraw-Hill.
8. 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, 1268-1293.
9. Seto, J., Wang, Y., & Lin, X. 2015. User-Habit-Oriented Authentication Model: Toward Secure, User-Friendly Authentication for Mobile Devices. Emerging Topics in Computing, 3(1), 107-118.
10. Shay, R., Komanduri, S., Durity, A. L., Huh, P. S., Segreti, S. M., Ur, B., . . . Cranor, L. F. 2016. Designing Password Policies for Strength and Usability. Transactions on Information and System Security, 18(4), 13.1-13.34. doi:http://dx.doi.org/10.1145/2891411