



STRENGTHENING USER AUTHENTICATION FOR BETTER PROTECTION OF MOBILE APPLICATION SYSTEMS

KARTINI MOHAMED¹, FATIMAH SIDI², MARZANAH A. JABAR³, ISKANDAR ISHAK⁴, NORAHANA SALIMIN⁵, NOR SAFWAN AMIRUL SALLEH⁶, ABDUL QAIYUM HAMZAH⁷, AHMAD DAHARI JARNO⁸, MUHAMAD FAEZ PAUZI⁹

¹SIRIM Berhad
1, Persiaran Dato' Menteri, P.O. Box 7035,
Section 2, 40700 Shah Alam, Selangor,
Malaysia.

^{2,3,4}Faculty of Computer Science and Information Technology,
Universiti Putra Malaysia,
43400, UPM Serdang, Selangor,
Malaysia

^{5,6,7,8,9}CyberSecurity Malaysia,
Level 5, Sapura@Mines, The Mines Resort City,
43300 Seri Kembangan, Selangor,
Malaysia

Corresponding author: fatimah@upm.edu.my

ABSTRACT

For most of us now, life is incomplete if living without mobile phones. This is because mobile phones are like a necessity to many people nowadays. Statistics have shown that more than seven billion people in the world are having these devices in 2015. This also means 97% of the human world populations are actually mobile phone users. Besides, more than 50% of the mobile phone users are using smart phones which are capable of downloading a lot of mobile application systems (apps). It is estimated that more than 200 million apps are being downloaded in 2007 and this number is believed to be growing. Unfortunately, many of these apps involve the transfer of important and confidential personal data or business information. How to ensure this sensitive information is well protected from being stolen or misused by unauthorized parties? One of the ways to secure this communication is to properly control the access to the system by strengthening the user authentication. Thus, this paper focuses on one the techniques to enhance the protections of mobile apps to prevent intrusions by unpermitted users. The enhancement is focusing on improving the multi-factor elements and the text ciphering technique of the user authentication. In this study, random number and time are added in the existing text-based multifactor user authentication. Besides, encryption and hash are used as the text ciphering technique to improve the protection. To measure how secure the proposed enhancement is, an independent testing body has been appointed to perform Vulnerability Test and Functionality Test to the apps. If all these tests are passed, it can be said that the proposed enhancement is strong enough to protect the apps from being intruded. Based on the test results provided by the testing body, CyberSecurity Malaysia, the apps has passed all the Vulnerability Test and Functionality Test. This shows that the control of the access to these apps are strong and able to prevent from being accessed by unpermitted users. This also means the proposed enhancement is able to give better protections to ensure the mobile apps can't be easily broken into by unauthorized mobile phone users.

Keywords: *User authentication, Data Protection, Data Transmission, Wireless Communication, Mobile Application Systems*



1. INTRODUCTION

Majority of world population now are mobile phone users [1] and majority of them also like to download mobile apps [2]. Many mobile apps are being downloaded into smart phones due to their interesting and usefulness for many people such as for social networking and entertainment [3], for banking [4] or for medical purposes [5]. Furthermore, many of these apps can be downloaded freely from Google Play, App Store, Windows Phone Store, etc. [3]. Unfortunately, many of them deal with highly confidential information or data such as those dealing with mobile banking, mobile payment as well as mobile commerce [6][7][8] while mobile communications are vulnerable to security attacks [9].

Protections are required to prevent these confidential information or data from leaking out. In our previous paper, we have proposed the use of watermarking technique to secure wireless or mobile data transmission [10]. To further strengthen the mobile communication, we propose in this paper a way to control the access to the apps through the use of user authentication. The authentication can be done in many ways such as by having multi-factor elements or by applying text ciphering technique to the elements of the user authentication. The multi-factor elements could be made in text-based or non-text-based. The text-based elements normally consist of username and password while non-text-based are like biometrics. Biometric authentication is normally preferred because it is very unlikely to have similar biometric characteristics of more than one individual. There are two categories of biometric elements - physiological and behavioural [11]. According to [12], physiological elements are like fingerprint, face, iris, retina or hand and palm recognitions and behavioural refers to voice, signature and gait recognitions or behaviour profiling. Based on a survey on development of biometric user authentication done by [12], where eleven of these biometric approaches (five physiological and six behavioural) were analyzed, the most accurate biometric authentication is using the iris recognition. However, it requires an external device that can scan the eyes of a person and it will be more difficult if the person is wearing glasses. Furthermore, biometrics are not easy to get good accuracy with high speed for limited power and memory capacity of mobile phones. Due to this considerations, this study focuses on the enhancement of text-based elements

of user authentication. Even though biometric authentication is stronger than a normal text-based elements of authentication, the text-based elements can still be made strong using the enhancement as proposed in this paper.

Section 2 of this paper talks about the infrastructure of the experimental system. It is followed by section 3 which explains about the proposed technique. Section 4 describes about the test method while Section 5 analyses the results and Section 6 concludes the findings and future works.

2. THE INFRASTRUCTURE OF THE EXPERIMENTAL SYSTEM

The system has been constructed using several hardware devices consisting of a smart phone (Samsung Galaxy Note 2) and a laptop installed with android mobile platform. The algorithms are written in object oriented language PHP 5 compatible for use in android mobiles and the data are kept in MySQL database. However, the system is evaluated using publically available software and hardware and the Wi-Fi service subscribed by the testing body.

Both the algorithms and databases are placed in the same subscribed cloud server to eliminate the probable uncontrolled parameters such as bad quality of service, distance of communications, time of usage, etc.

3. THE PROPOSED ENHANCEMENT

The proposed enhancement basically focus in two areas - (1) the multi-factor elements of user authentication and (2) the data ciphering technique. The multi-factor elements of user authentication are enhanced by adding two more elements namely 'random number' and 'time' into the existing four elements as introduced by [13] comprising of username, password and mobiles' IMEI (The International Mobile Equipment Identity) number and SIM (Subscriber Identification Module) Card number. The elements proposed by [13] are selected for reference in this study since a claim has been made that they are effective for use in mobile banking. Meanwhile, the data ciphering technique is enhanced by combining encryption and hash instead of using encryption only by [13]. In this proposal, the data,

which are not in text form are not recommended because they can use up more memories or power supplies especially in limited capacities of mobile devices.

Interestingly, the proposed system doesn't require the user to key in more inputs even though the number of multi-factor elements have been increased. The user is still required to key in username and password as usual while the IMEI and SIM Card numbers are auto-retrieved from the mobile device. The random number is self-determined by the system while the time is enclosed in the background operation of the system. Similarly, the encryption and hashing do not involve any user's intervention.

The 'random number' is used only to obscure the hackers during wireless data transmission process. It is attached to the authentication data right after the key-in or input process is completed and discarded just before the storing of data into the database. The 'random number' being used has

10 digits which is self-determined by the algorithm written using android based PHP 5 as below:

```
$randomNum = mt_rand (1000000000, 9999999999);
```

In addition, the 'time' being applied is in term of service denial when wrong username and password are entered more than 3 consecutive times. It can also be restricted by denying the service when the screen is idle for 30 seconds or more.

Before a user can use the apps, he/she is required to register his/her username and password during a process called Registration Phase. The verification of these data can only be done in another process called Authentication Phase. When all the proposed elements and the text ciphering technique are applied in the system during both registration process and during authentication process, their process flows are as shown in Figure 1(a) for the Registration Phase and Figure 1(b) for Authentication Phase.

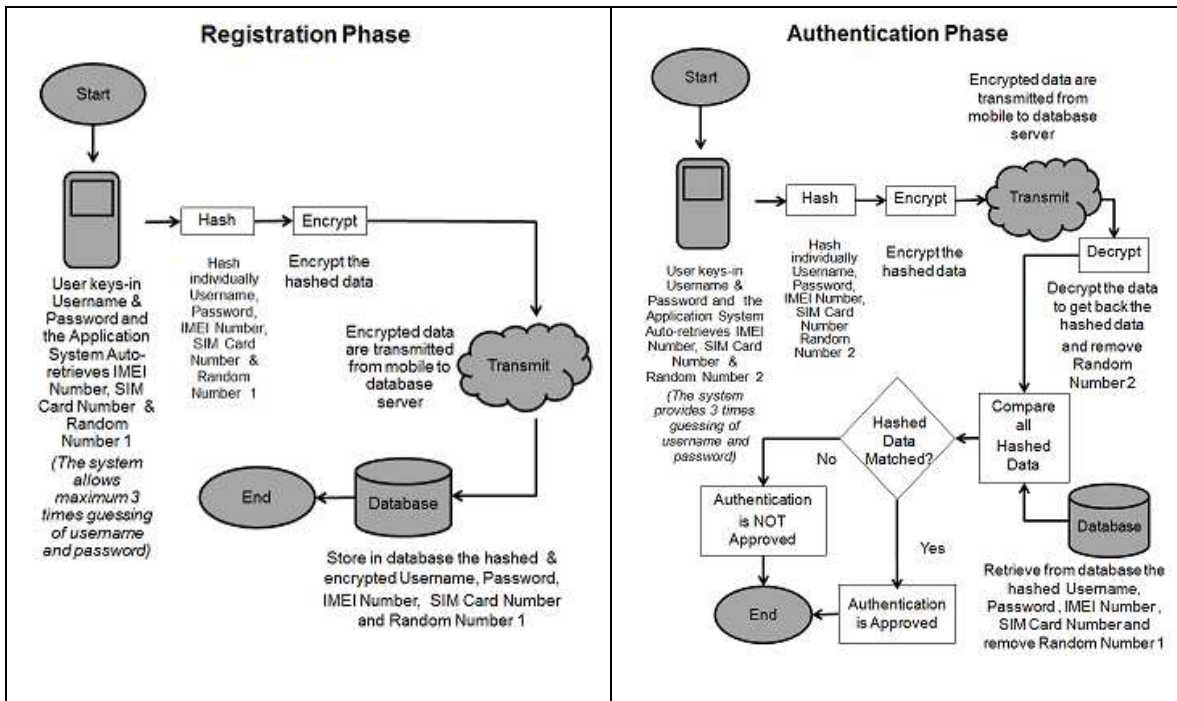


Figure 1(A) : Registration Phase

Figure 1(B) : Authentication Phase

The proposed system basically maintains the normal protection practices as being applied in other mobile apps such as the strict selections or filtrations of usernames and passwords. As such, the number of characters of each username and password is allowed to be between 8 to 12 and in

alphanumeric form. This filtration process which include the system denial after three failure attempts to guess username and password with their alert messages are as demonstrated in a diagram as in Figure 2. The user guidance of such

filtration is indicated on the mobile screen as shown in Figure 3.

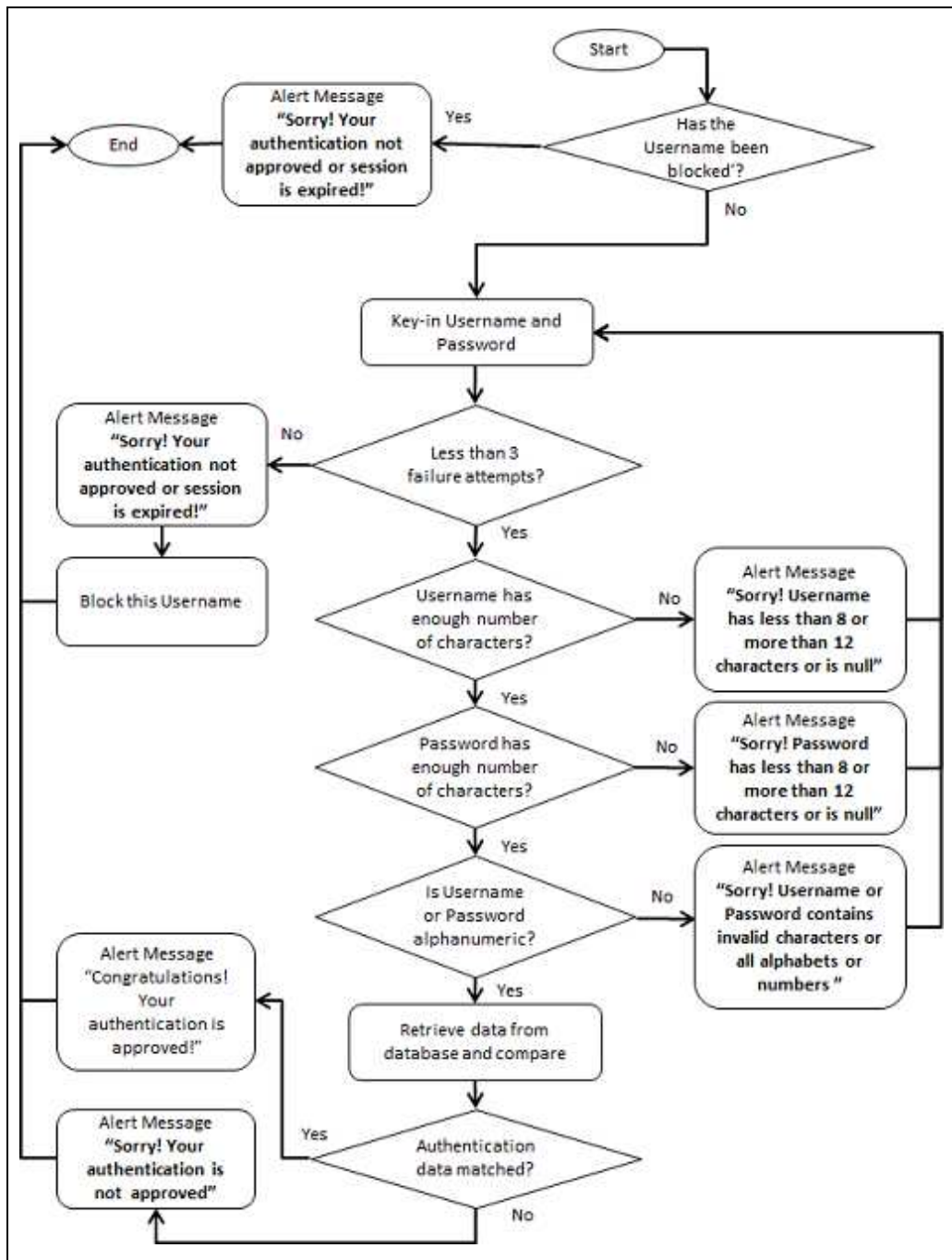
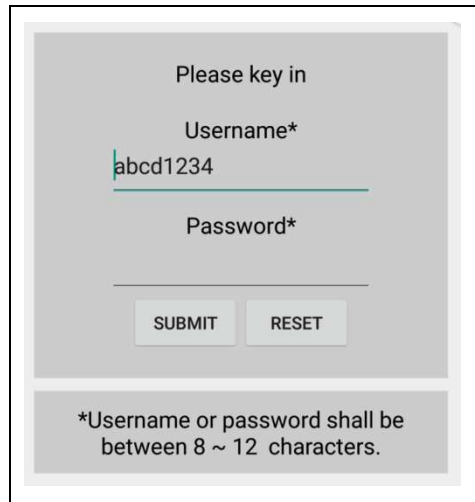


Figure 2: Sample Of Authentication Process



Please key in

Username*

abcd1234

Password*

SUBMIT RESET

*Username or password shall be between 8 ~ 12 characters.

Figure 3: User Authentication With Guidance Of Input Characters

4. EVALUATION METHODOLOGY

Since there are two dimensions of improvements being introduced in this proposal as per Table 1, there are four possible combinations

of performances need to be evaluated. A mobile apps has been developed for each combination and each mobile apps is named as Type 1A, 1B, 2A and 2B as summarize in Table 2.

Table 1: Existing Vs. Proposed Authentication System

Type	Elements of Authentication	Cipher Text Protection
Existing Authentication System	Username Password IMEI Number SIM Card Number	Encryption only
Proposed Authentication System	Username Password IMEI Number SIM Card Number Random Number Time	Encryption & Hash



Table 2: Differences Of Type 1A, Type 1B, Type 2A And Type 2B

Type	Elements of Authentication	Cipher Text Protection
Type 1A	Username Password IMEI Number SIM Card Number	Encryption & Hashing
Type 1B	Username Password IMEI Number SIM Card Number	Encryption only
Type 2A	Username Password IMEI Number SIM Card Number Random Number Time	Encryption & Hashing
Type 2B	Username Password IMEI Number SIM Card Number Random Number Time	Encryption only

There are two possible tests that can be performed to evaluate the effectiveness of each of the mobile apps. The tests are known as Functionality Test and Vulnerability Test. The Functionality Test is performed to ensure the system is executing as per expectations without any bugs or errors whereas the Vulnerability Test is done to check the possible system penetration by intruders. An independent testing body known as CyberSecurity Malaysia has been appointed to carry out the tests to demonstrate the impartiality of the results obtained. Besides, the appointed testing body is also supported by the Malaysian Ministry of Science and Technology (MOSTI) and have the best experts and skills as well as tools to test such systems. The details of tests to be conducted for each Functionality Test and Vulnerability Test are described below:

a) Functionality Test

There are three areas that this test is focusing. First is the security management that is to confirm that the system is able to create new users and properly manage the username and password. Second is the time session to confirm that the system is denial after three times of failure attempts to key in correct username and password. Third is the identification and authentication to

find out whether the registered usernames and passwords are authenticable.

b) Vulnerability Test

Four standard tools are being used to test the possible penetration by unauthorized parties. They are known as Cain and Abel, Wireshark, Wi.cap. Network Sniffer and BlueStacks. These tools are selected for testing due to several reasons. Firstly, they meet the common criteria requirements and are publicly available. Secondly, they are able to provide quick access to common features and command and thirdly, they fulfill the ISO 17025 requirements where the tests need to be repeated several times until the same results are obtained. How each tools works are explained here:

(i) Cain and Abel

It has a function call APR (ARP Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. It has a function to analyse encrypted protocols such as SSH-1 and HTTPS and contains filters to capture credentials from a wide range of authentication mechanisms, decoders and some not so common utilities related to network and system security. This application is an open source and publicly



available. It also has the capability to analyze encrypted protocols such as SSH-1 and HTTPS and contains filters to capture credentials from a wide range of authentication mechanisms. This function can determine whether crucial information such as username and password can be obtained or not.

(ii) Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, software analysis, development of communication protocol and education. Wireshark lets the user put network interface controllers that support promiscuous mode into that mode, so they can see all traffic visible on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic. This application is an open source and publicly available. It has the capability to monitor network traffic and network sniffing. This function can determine whether crucial information transferred by the TOE such as username and password can be obtained or not.

(iii) Wi.cap. Network Sniffer

Wi.cap demo is a Mobile network packet sniffer that has the capability to monitor network traffic. This application is a demo version and publicly available. Wi.cap has the capability to monitor network traffic and network sniffing. Similar to Cain and Abel, this function can determine whether crucial information such as username and password can be obtained or not.

(iv) BlueStacks

BlueStacks is an Application Player/software emulator for Android applications to run on Windows PCs and Macintosh computers. BlueStacks emulates some of the basic functions of an Android device. There are certainly some Android application that aren't available for Windows, and BlueStacks makes it possible to run them. This application is an open source and publicly available. Testers normally use BlueStacks to execute the testing system in a vulnerable environment (root) and try to sniff/capture the crucial information such as username and password [14][15][16][17][18][19][20][21].

In short, the above tools are used to sniff the crucial information such as username and

password from the network communication between mobiles and cloud servers and to identify whether the data are in encrypted or plain-text form. They are also used to identify whether the website being used is in 'http' or 'https' type of link. The connection is considered as more secured if the wireless communication is done using 'https' link.

5. RESULTS AND DISCUSSION

This section summarizes the results and discussions related to the Functionality Test and Vulnerability Test as provided by CyberSecurity Malaysia.

a) Functionality Test

Every type of test done are marked with the following marking formula:

Pass => [Number of test pass / number of tests done] x 100% >= 50%

Fail => [Number of test pass / number of tests done] x 100% <50%

Examples of functionality test done are to evaluate whether the same username can be registered repeatedly within each system Types 1A, 1B, 2A and 2B, to evaluate whether the same username can registered again across different system types, to evaluate whether the system is able to register username and password between 8 to 12 alphanumeric characters, etc.

The results show that all the test done are Pass. This indicates that the system is well operating as per planned with no system bugs or errors.

b) Vulnerability Test

The test is done to evaluate if there are any flaws or weaknesses that can allow the penetration and exploitations by intruders during its operation. The authentication system is considered as weak if the user authenticating data are possible to be sniffed. The sniffing is possible if the authenticating data are in plain-text form and if they are not communicated between mobiles and servers using 'https' link. Interestingly, even though the network used in this study is not in 'https' connection, the intruders are not able to retrieve or sniff the data because the authenticating data have been strengthened with the increase number of elements from four to six numbers and are already being hashed and encrypted. Even

though the system is already being strengthened using the proposed enhancements, the testing body has recommended that the sensitivity of usernames and passwords be increased by using upper case and lower case letters, include more than one numerical digits, use special characters, increase the number of characters to be between 8 and 15 and hide the password when typing it. Besides, the session clock out could also be considered to make the authenticating system stronger.

However, due to some constraints including time, etc., several weaknesses are not yet being tackled at the moment such as the prevention of unintended data leakage, broken cryptography, lack of binary protection and verifying mobile application permission. Even though these problems are not related to the proposed techniques of enhancing user authentication but more on the way of writing the algorithms, it is hope that this problems could also be rectified in the near future to ensure the proposed protection achieve the highest security and confidence levels.

6. CONCLUSION

A technique is proposed to strengthen the user authentication in mobile apps that deals with highly confidential and sensitive data. It is to ensure that such data could not be sniffed or stolen by any unauthorized personnel during its transmission between mobiles and database servers. The enhancement is proposed in the multi-factor elements of user authentication and the data ciphering technique. Four types of mobile apps developed and each are tested in terms of functionality and vulnerability by an independent testing body. Results indicate that the proposed enhancement is effective to make the user authentication stronger with several improvement recommended to increase the sensitivity of username and password as well as the use of session's lock out timer. Thus, it is concluded that even though the objective to improve the apps protection has been achieved, there are still some improvements to be considered in the future work of this study. Besides, the problems related to unintended data leakage, broken cryptography, lack of binary protection and verifying mobile application permission which are not yet tackled will also need to be improved in our future work.

7. ACKNOWLEDGEMENT

This work is financially and technically supported by Universiti Putra Malaysia, SIRIM Berhad and CyberSecurity Malaysia.

REFERENCES:

- [1] Sanou, B. (2015). *The World in 2015*. Retrieved from ICT Facts and Figures: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>
- [2] Shen, G. C.-C. (2015). Users' Adoption of Mobile Applications: Product Type and Message Framing's Moderating Effect. *Journal of Business Research*, 2317-2321.
- [3] 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.
- [4] Fenu, G., & Pau, P. L. (2015). An Analysis of Features and Tendencies in Mobile Banking Apps. *Procedia Computer Science* (pp. 26-33). Cagliari, Italy: ScienceDirect.
- [5] Helf, C., & Hlavacs, H. (2015). Apps for life change: Critical review and solution directions. *Entertainment Computing*, <http://dx.doi.org/10.1016/j.entcom.2015.07.001>.
- [6] Mallat, N., Rossi, M., Tuunainen, V. K., & Oorni, A. (2009). The Impact of Use Context on Mobile Services Acceptance: The Case of Mobile Ticketing. *Information and Management*, 190-195.
- [7] Schierz, P. G., Schilke, O., & Wirtz, B. W. (2010). Understanding Consumer Acceptance of Mobile Payment Services: An Empirical Analysis. *Electronic Commerce Research and Applications*, 209-216.
- [8] 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*, 129-142.
- [9] Gordon, M., & Sankaranarayanan, S. (2010). Biometric Security Mechanism in Mobile Payments. *IEEE*.
- [10] Mohamed, K; Sidi, F.; Jabar, M.A; Ishak, I. (2016). Protecting Wireless Data Transmission in Mobile Application System Using Digital Watermarking Technique. *Journal of Theoretical and Applied*



- Information Technology*, Vol. 83, No. 1, (pp. 52-63).
- [11] Krishna, B. M., Madhumati, G. I., Ganesh, M. S., Bhargav, Y., Krishna, V. M., & Kumar, O. M. (2015). Biometric Based Industrial Machine Access Control System Using FPGA. *Journal of Theoretical and Applied Information Technology*, 76-82.
- [12] 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.
- [13] 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.
- [14] <https://en.wikipedia.org/wiki/Wireshark>
- [15] <https://wiki.wireshark.org/>
- [16] <http://resources.infosecinstitute.com/password-cracking-using-cain-abel/>
- [17] [https://en.wikipedia.org/wiki/Cain_and_Abel_\(software\)](https://en.wikipedia.org/wiki/Cain_and_Abel_(software))
- [18] <https://play.google.com/store/apps/details?id=com.evbadroid.wicapdemo>
- [19] <http://forum.xda-developers.com/showthread.php?t=2589947>
- [20] <https://en.wikipedia.org/wiki/BlueStacks>
- [21] <http://liliputing.com/2011/10/bluestacks-lets-android-apps-run-on-a-windows-pc.html>