Keystroke Dynamic Authentication in Mobile Cloud Computing

Mahnoush Babaeizadeh
Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Skudai 81310, Johor, Malaysia

Majid Bakhtiari
Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Skudai 81310, Johor,Malaysia

Mohd Aizaini Maarof
Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Skudai 81310, Johor,Malaysia

ABSTRACT

One of the important challenges in Mobile Cloud Computing (MCC) is related to the authentication of users. There is increasing demand for suitable authentication method for accessing to the shared information via the Internet through Cloud Service Provider (CSP). Personal identification number is the most common mechanism for authentication in mobile devices; however it is not secure way for authenticating users. This work presents a method of authentication which able to identify users based on Keystroke Dynamic Authentication (KDA). Furthermore, keystrokes duration is considered as an attribute for measuring keystrokes of mobile's users. This paper proposed strong method of authentication in the password authentication scheme by combining it with keystroke authentication, which is a type of behavioral biometric mechanism. Experimental results show, the proposed method can work 97.014% correctly, due to the keystroke duration of each user depends on their behavioral characteristic and it can be measured up to milliseconds. On the other hand, if unauthorized person knows the username and password of legal user can not gain access rights because of difference between their keystroke duration. Therefore, it is hard for an attacker to pretend as an owner, and this method enhances the security of authentication in MCC

Keywords

Keystroke authentication, Mobile cloud computing, Biometric authentication, Security and privacy

1. INTRODUCTION

One of the important challenges in MCC [21, 22] is security and privacy [41]. Furthermore, authentication plays an important role in preserving security and privacy of mobile communication especially in wide spread networks such as MCC [37, 38, 40]. It helps to protect shared information from unauthorized persons. In other words, an authentication mechanism determines how user identified and verified to access to sensitive information [42]. Verification of user's identity is the most important goal behind an authentication. PIN is adopted as the only security mechanism for mobile devices. It is obvious that, PIN (something the user knows) is not very secure mechanism for authenticating users because of its limitation, as well as it is difficult to confirm that the demand is from the rightful owner [17, 44].

Strong method of authentication should cover one or several various factors of identification to improve security. These factors are i) something we know; ii) something we have; iii) something we are.

Therefore, biometric authentication [11, 13] is a strong authentication mechanism by providing the factor what we are and what we know [28]. In addition, it is able to identify users based on their unique characteristic [35], and it is more reliable, because it is so difficult for user to pretend as other user by using physical or behavioral biometric authentication.

Keystroke authentication is a type of behavioral biometric authentication. Keystroke based authentication can categorize in two folds, Keystroke Static Authentication (KSA), as well as KDA. Keystroke static authentication can identify keystroke of users only at particular times, for example the time that user wants to login. This is a huge drawback of KSA; due to system can use by anyone once the user is authenticated at login [36]. Majority of the researches have focused on KSA using inter-keystroke latency mechanism [9]. Static authentication provides more strong and robust user authentication than simple password or PIN; however it cannot keep continuous security.

KDA continuously observes the style of typing of the users throughout the whole stage of interaction even after a successful login. In other words, the typing patterns of users are constantly analyzed and when they do not match accessing of users will block [9, 34]. The main goal of KDA is recognizing mobile users by identifying and analyzing their unique feature for authentication such as typing pressure, keystroke duration, typing error, and latency of keystrokes [9].

KDA has some advantages rather than other types of biometric authentication. These advantages are i) Contrasting other biometric methods, KDA does not need any additional tools, therefore it causes to decrease price, ii) High acceptability between mobile users due to it is natural for everybody to type a password for authentication purposes, iii) preserving privacy and security of users because it is based on behavioral characteristic of users, iv) It could not be forgotten, stolen or lost [28, 32].

This paper is organized as follows: Section 2 discusses the various researches related to biometric authentication, as well as keystroke base authentication. Explanation about the proposed method is in Section 3. Experimental results obtained from applying KDA in CSP using Android application development bring in Section 4; finally the conclusions are given in Section 5.

2. LITERATURE REVIEW

Biometric authentication [9, 13] is an authentication mechanism that identify users base on measuring their unique characteristic. In other words, biometric authentication is base on verifying personal attributes of users [11]. Furthermore, biometric authentication has some benefit as compared to other techniques [14]. These benefits are i) biometric characteristics are uniquely individual (something you are); ii) non-transferable to others; iii) impossible to forget or lose; iv) difficult to reproduce; v) usable with or without the knowledge; vi) complicate to alter or modify.

As shown in Figure 1, biometric authentication can categorize in two types. These types are physical biometric and behavioral biometric [11, 32]. Physiological biometric relies on something the users are. It performs authentication base on physical characteristics such as facial features [18- 20], palm prints [23, 24, 26], retina patterns [39, 13], finger print [13, 25], iris pattern [20], as well as hand geometry [13, 27]. In other words, physiological biometrics is based on measurements and data derived from direct measurement of a part of the human body. Behavioral biometrics is based on the user's behavior and authentication may occur perfectly such as signature, keystroke dynamics [43] and voice. Furthermore, voice can considered as physiological biometric. One advantages of behavioral biometrics are that they can be applied in a transparent and continuous authentication system [13, 15].

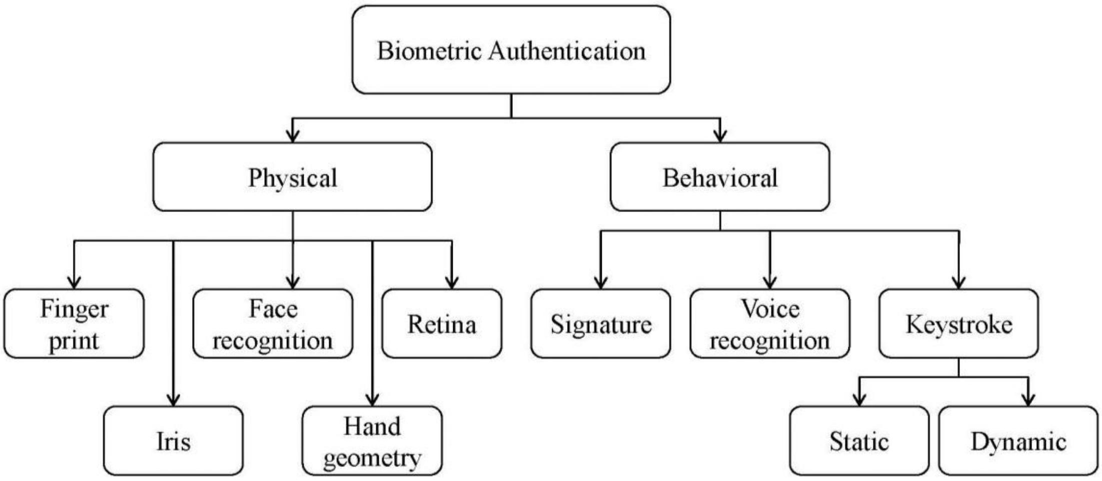


Fig1: Classification of biometric authentication

Keystroke dynamic authentication (KDA) is a type of behavioral biometric authentication which developed in the late 19th century. It is based on style of each person's typing on a keyboard, as well as it can identify the user based on their habitual typing pattern. Keystroke dynamics implies on the process of measuring human's typing rhythm on digital devices such as mobile devices [9]. In other words, it is not important what you type; the important point is how you type. Furthermore, keystroke technology can be easily integrated with existing technology environments and processes [30].

In [10], Yu et al. proposed the solutions to enhance identity verification by applying an SVM novelty detector, proposing GAe-SVM, as well as an ensemble creation based on characteristic selection. After that, Bartlow et al. [4] developed a web application to use keystrokes dynamics by incorporating shift-key patterns. It helps to achieved 14% FRR.

Clarke et al. [6] improved biometric authentication by using keystrokes analysis. They utilize telephone number and text message obtained from mobile phone for authenticate users. They compare performance of different type of biometric techniques. Their results show that, hand geometry identification with 1.5% EER has lowest performance and vein mechanism has highest performance with 5% EER. Hyoung and Sungzoon [5] proposed the retraining framework to enhance authentication accuracy. Minetti et al. founded a positional dependence of the relationship between the applied force and the resulting down stroke speed due to the different hammer mass to be accelerated [29].

In [8], Kang et al. enhanced quality of data obtained from keystrokes of users by using artificial rhythms and cues. Artificial rhythms cause increasing the uniqueness, as well as raising the stability. Briggs and Olivier [16] recommended creating “biometric daemons” for authenticating users. This method is based on learning user's behavior.

Hwang et al. [1] utilized artificial rhythms to overwhelm problems resulting from short PIN length. Through the experiment involving human subjects, they decreased the error from 13% to 4%. They measured performance in terms of Equal Error Rate (EER). Giot et al. [28] presented comparative research on various method of keystroke dynamic on keyboard. Moreover, they considered the operational constraints of use for collaborative systems.

Karnan et al. provides over view on biometric authentication. In fact, they do research on well-known approaches used in keystroke dynamics in the last two decades [11]. Chang et al. proposed a method of authentication that is combination of neural network technique and password keystroke features to produce a long-lived private key dynamically. This method improved security of long-lived private key. In fact, it decreased the likelihood of accessing the private by unauthorized person [7].

Bours [12] experimented with the new idea of continuous keystroke dynamics. This authentication mechanism can continuously monitor the typing behavior of a user and verify that the request is from the legal user. Furthermore, Wang et al. proposed a new user authentication approach by using keystroke dynamic method. The novel method has two stages. These stages are tanning and authentication. Training stage contains set of feature vector are generated from keystroke characteristics of valid user that successfully authentications. Authentication stage consists of, current keystroke feature vector of the set orthogonal bases. It has better performance in term of False Acceptance Rate (FAR) and False Rejection Rate (FRR). This method of authentication can apply in any password base system [2].

In [3], Chang et al. proposed a new graphical based password KDA system for identifying users in touch screen mobile devices. In addition, they applied pressure feature in their system. The results obtained from experiment of graphical-based password KDA system shown, this method cause to develop EER to 12.2%. Moreover, using pressure and time features in this system helps to decrease EER to 6.9%. Therefore, this system is suitable for low-power mobile devices. Teh et al. provides a survey on keystroke dynamics biometrics authentication. It covers research performed during the last three decades, as well as proposing some future works in this approach [9].

Nauman et al. [31] proposed a protocol for keystroke dynamics analysis which allows web-based applications to make use of remote attestation and delegated keystroke analysis. Moreover, they presented a prototype implementation of their protocol using Android operating system. Bhatt and Santhanam have presented a survey paper that explained about the researches work on keystroke dynamics, as well as they discussed advantages and disadvantages of these researches [34].

3. THE PROPOSED METHOD

Introduction motivated the KDA and advantages of it. This section presents the proposed method in MCC. MCC is an infrastructure where both data processing and data storage occur outside of mobile set [21]. Therefore, the mobile device does not require powerful Control Processing Unit (CPU) and memory capacity.

In this paper, Google drive (CSP) is considered as data storage. As mentioned before the proposed method is based on keystroke authentication. It is a type of behavioral biometric authentication. There are different parameters for measuring keystrokes of mobile users; keystroke duration is considered as an attribute to measure keystrokes of uses.

As shown in Figure 2, this method is multi-factor authentication. It uses username/ password as well as keystrokes authentication to identify users. The process is shown that in first time login, user has to insert username/ password to login to the application, after inserting password the application can measure keystrokes duration. Finally, all the values (username, password, keystrokes duration) will send to CSP and store in to the data storage.

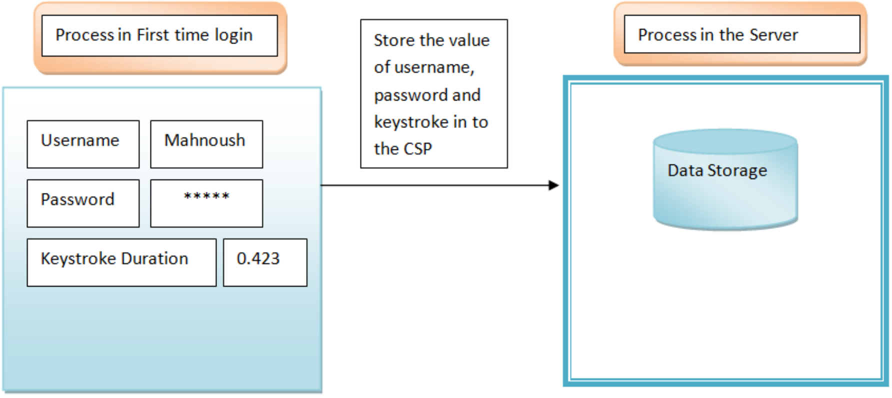

Process in First time login
Username
Mahnoush
Password
*****
Keystroke Duration
0.423
Store the value of username, password and keystroke in to the CSP
Process in the Server
Data Storage

Fig2: Process of sending values obtained from mobile device to CSP

After storing the values obtained from mobile device, as shown in Figure 3 inserted values have to compare with the stored values for the next login. There are different cloud servers such as Drop box, Amazon, Sky Drive, Box, as well as Google drive which provide different types of cloud computing services (Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)). In this paper Google Drive is used as an IaaS.

Figure 4 shows pseudo code of the proposed method. In proposed method, fixed username and password are defined for the first time login. Moreover, there is a constant parameter which is related to the limitation of login attempt. At most user can three times attempt to login to the application otherwise they will block. Furthermore, after successfully login, pseudo-random session ID will create and store in database. It means that, user is login until session expires. It helps to continuously check validity of user.

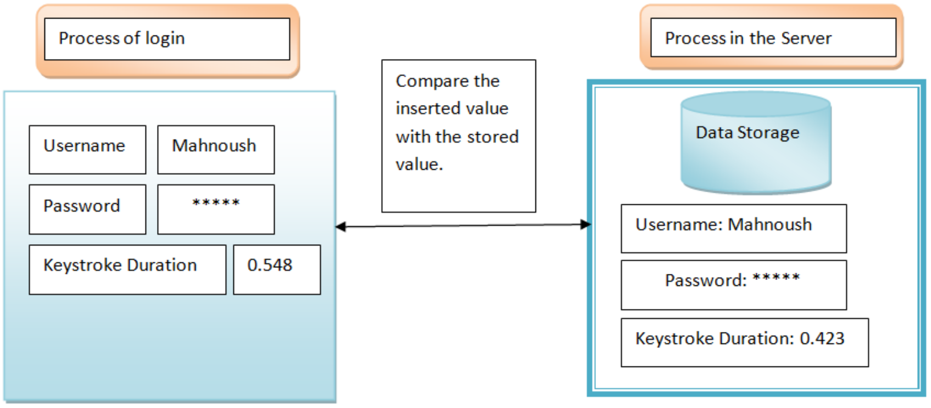


Fig3: Process of comparing values in mobile device with CSP

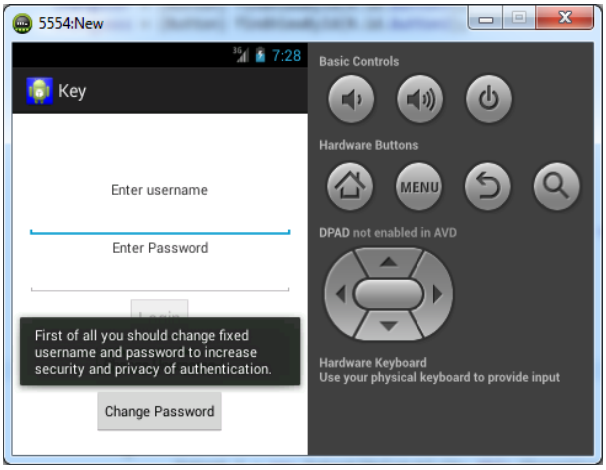
```
Count=0
if First time run then
    //Change password
    Insert old password
        if password is incorrect then
            Output ("Password is incorrect")
            Exit
        else
            Insert new password
            Insert confirm password
            Measure keystrokes duration
                if password match then
                    Output (" Password is changed")
                    Store new password in CSP
                    Store keystrokes duration in CSP
                else
                    Output ("Password is not match")
                    Exit
                end if
        end if
else
    if like to change username then
        //change username
        Insert old password
            if password is correct then
                Insert new username
                Output ("Username is changed")
                Store new username in CSP
            else
                Output ("password is incorrect")
            end if
    else
        //login to the application
        Insert username
            if username matches with the stored value then
                Insert password
                Measure keystrokes duration

                    if keystrokes duration is in the range of stored value then
                        Output ("Successfully login")
                        Create pseudo-random session ID
                        Store session ID on database
                            if session exists on database then
                                User is logged in
                                Count= Count+1
                            else
                                Output ("login again")
                            end if
                            if  count>=3 then
                            Block user
                            else
                            Allow to login again
                            Count= Count+1
                            end if
                    else
                        Output ("You cannot login")
                    end if
            else
                Output ("You cannot login")
            end if
    end if
end if
```

Fig4: Psoudo code of proposed method

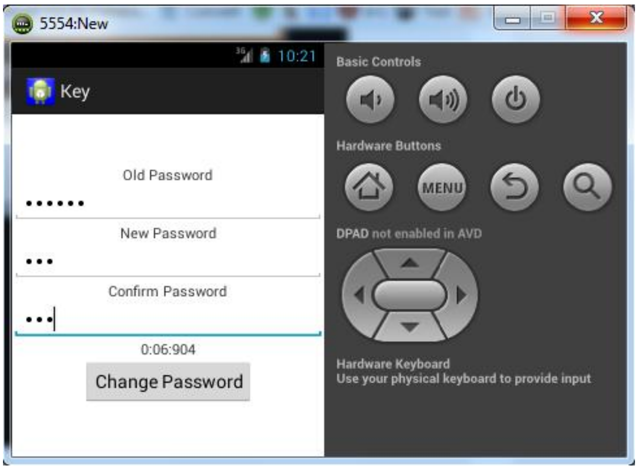
As shown in Figure 5, when user wants to run an application for the first time login button is inactive. They have to change fix password and may username to allow login to the application. In the time users change their password keystroke duration can measure. As mentioned before values of username, password, as well as keystroke duration will store in to the CSP.

Figure 6 shows the process of changing password. For changing password, user should insert old password. If old password is match, user can insert new password. After that, they should insert confirm password. In the time user inserts confirmation of password, keystroke duration of them will measure. An important point is that, this method is more accurate because it capable to calculate the keystrokes duration up to milliseconds. At last, new password and value of keystroke duration send to CSP and store.



First of all you should change fixed username and password to increase security and privacy of authentication.

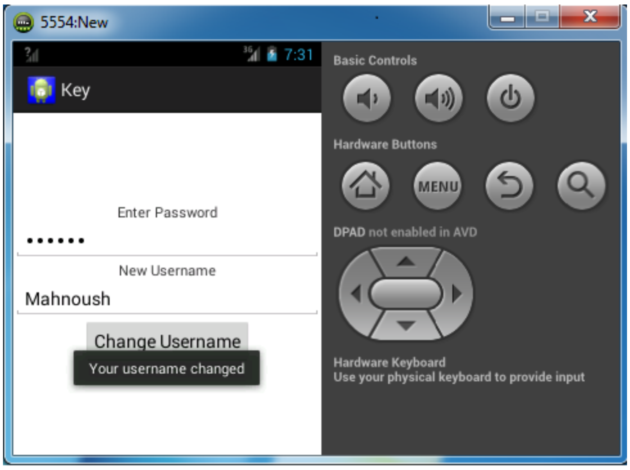
Fig5: First page of user interface



0:06:904

Fig6: Process of changing password

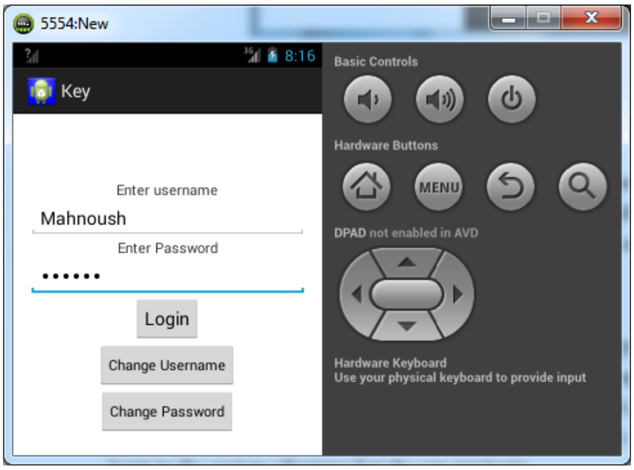
In addition, user should insert their password to allow to change username.Figure 7 shows process of changing username.However, it is not compolsary to change user name. When password and may be username changed, mobile user allows to login to the application. As shown in Figure 8, after inserting username and password by user, the application can compare inserted username, password, as well as keystrokes duration with stored values. If they match with each other user can login successfully.



Mahnoush

Your username changed

Fig7: changing username



Mahnoush

Fig8: login to the application

Moreover, session expiration time helps to expire the session of user and force them to login again. It helps to continuously monitor keystrokes duration of user through the whole stage of interaction even after successful login, as well as identifying unauthorized person after verification.

In practical situation keystrokes duration does not exactly equal with the stored value of keystrokes duration. Therefore, parameter ε is considered as tolerance. It means that keystrokes duration should be in range of defined tolerance to successfully login to the application, otherwise application do not allow user to login. Parameter ε defines based on keystrokes duration of user obtained in several times login to the application. For example, keystrokes duration of legal user when he changed his password is 4:048. In addition, ε is equal to one second. When user wants to login to the application, their keystrokes duration should be between 3:548 and 4:548 to successfully login to the application.

4. EXPERIMENTAL RESULT

In previous section explain proposed method of authentication in MCC. The purpose of this section is discussing about the performance of this method. Results obtained from communication with Google drive. In this research asked some random people to cooperate in testing of the method. An important point is that, username and password of the mobile's owner were known by them.

In this experimental result, there are three important factors, username, password, as well as keystrokes duration. Moreover zero is considered for incorrect value and one for correct value of each factor. For example "000" means username and password and keystrokes duration are inserted incorrectly, "110" means username and password are inserted correctly however keystrokes duration is not in the range of keystrokes duration of mobile's owner.

In our experimental result keystrokes duration of owner was KD=4.679 milliseconds. Moreover, ε is equal to 0.529 milliseconds. Therefore, acceptable range of keystrokes duration is between KD- ε to KD+ ε.

Figure 8 shows various reasons of preventing unauthorized access. It is obvious that, the most important reason is relate to the situation that username and password are correct but keystrokes duration is not match with the stored value in CSP (110). It means that keystrokes duration can prevent unauthorized person to login to the application and access to the shared information in to the CSP. Due to, it is so difficult for unauthorized person or attackers to pretend as an owner.

The reasons of unsuccessfully login are as following:

(i) Username and password are correct; however keystrokes duration is not correct

(ii) Username and keystrokes duration are correct, but password is incorrect

(iii) Username is correct, but password and keystrokes duration are incorrect

(iv) Username, password, and keystrokes duration are correct

(v) Username, password, as well as keystrokes duration are incorrect

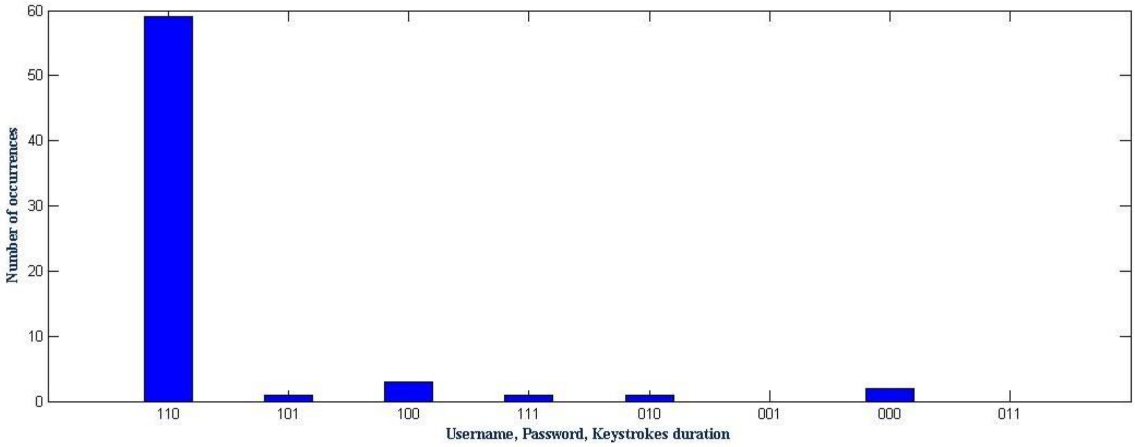


Fig8: Reasons of preventing unauthorized access

Figure 9 shows acceptable and unacceptable range of keystrokes duration. There are two black point that put in the acceptable range. It means that in these tests the method work incorrecty. One of them occurred, when username was correct, password was incorect, keystrokes duration was correct. Another one related to the situation that username, password as well as keystrokes duration was correct.

As shown in Figure 10 the proposed method of authentication can works 97.014% correctly. It means that, this method can 97.014% prevent from unauthorized login and access to shared information in cloud server.

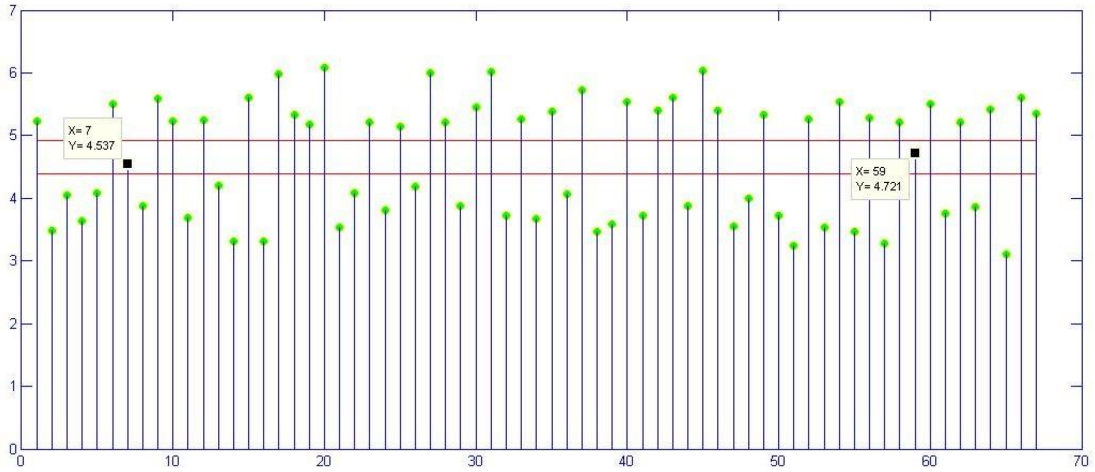


Fig9: Keystrokes duration

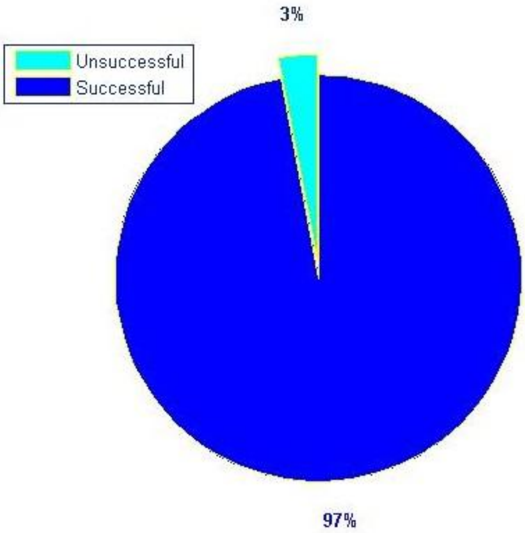


Fig10: Performance of the proposed application

5. CONCLUSION

This paper address using keystroke authentication in mobile communication. It has described a new biometric method based on measuring keystrokes duration. It helps to identify users based on their unique behavioral biometric and unlike the other biometric methods, Keystroke analysis does not require the aid of extra special tools, therefore it is cheaper than other type of biometric authentication methods. Experimental results show that this method can work 97.014% correctly in authenticating mobile's users, and it helps to improve the security and privacy of authentication in mobile communication. Some ideas of potential future investigation exist in this area; there are some other parameters for measuring keystrokes like as finger placement and applied pressure on the keys, and it is explained that performance metric can use for measuring keystrokes, this naturally bring the idea of improving KDA by measuring False Rejection Rate (FRR). It is percentage of attempts of wrongly recognizing a legitimate user as an imposter.

6. ACKNOWLEDGEMENT

The authors are thankful from Malaysia's Ministry of Higher Education (MOHE) and Research Management Center in Universiti Teknologi Malaysia (UTM) for their supports through research grant 01-01-06 SF1167.

7. REFERENCES

[1] Hwang, s., Sungzoon Ch., and Sunghoon P. 2009. Keystroke dynamics-based authentication for mobile devices. *Computers & Security* 28, no. 1: 85-93.

[2] Wang, Xu., Fangxia G., and Jian-feng M. 2012. User authentication via keystroke dynamics based on difference subspace and slope correlation degree. *Digital Signal Processing* 22, no. 5: 707-712.

[3] Chang, T., Cheng-Jung T., and Jyun-Hao L. 2012. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *Journal of Systems and Software* 85, no. 5: 1157-1165.

[4] Bartlow, N., and Bojan C. 2006. Evaluating the reliability of credential hardening through keystroke dynamics. In *Software Reliability Engineering, ISSRE'06. 17th International Symposium on*, pp. 117-126. IEEE.

[5] Lee, H., and Sungzoon Ch. 2007. Retraining a keystroke dynamics-based authenticator with impostor patterns." *Computers & Security* 26, no. 4: 300-310.

[6] Clarke, N. L., and Furnell S. M. 2007. Advanced user authentication for mobile devices. *computers & security* 26, no. 2: 109-119.

[7] Chang, T. 2012. Dynamically generate a long-lived private key based on password keystroke features and neural network." *Information Sciences* 211: 36-47.

[8] Kang, P., Sunghoon P., Seong-seob H., Hyoung-joo L., and Sungzoon Ch.2008. Improvement of keystroke data quality through artificial rhythms and cues. *Computers & Security* 27, no. 1: 3-11.

[9] Teh, P. Sh., Andrew B. J. T., and Shigang Y. 2013.A Survey of Keystroke Dynamics Biometrics. *The Scientific World Journal* 2013.

[10] Yu, E., and Sungzoon Ch. 2004. Keystroke dynamics identity verification—its problems and practical solutions." *Computers & Security* 23, no. 5 : 428-440.

[11] Karnan, M., Akila M., and Krishnaraj N.2011. Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing* 11, no. 2: 1565-1573.

[12] Bours, P. 2012. Continuous keystroke dynamics: A different perspective towards biometric evaluation. *Information Security Technical Report* 17, no. 1: 36-43.

[13] Bhattacharyya, D., Rahul R., Farkhod Alisherov A., and Minkyu Ch. 2009. Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology* 2, no. 3 :13-28.

[14] Hataichanok, S., Clarke, N. L., and Furnell, S. M. 2012. Multi-modal Behavioural Biometric Authentication for Mobile Devices. In *Information Security and Privacy Research*, pp. 465-474. Springer Berlin Heidelberg.

[15] Crawford, H., Karen R., and Tim, S. 2013. A Framework for Continuous, Transparent Mobile Device Authentication." *Computers & Security*.

[16] Briggs, P., Olivier, PL. 2008. Biometric daemons: authentication via electronic pets. In: Proceedings of conference on human factors in computing systems. ACM; p. 2423e32.

[17] Yi, H., Kim, S., Ma, G., and Yi, J. H. 2013. Elastic password authentication scheme using the Passcell-based virtual scroll wheel. *International Journal of Computer Mathematics*, (ahead-of-print), 1-11.

[18] Kochetkov, A. 2013. Cloud-based biometric services: just a matter of time." *Biometric Technology Today* 2013, no. 5: 8-11.

[19] Voth, D. 2003. Face recognition technology. *Intelligent Systems, IEEE* 18, no. 3 (): 4-7.

[20] Gomez-Barrero, M., Javier G., and Julian F. 2013. Efficient Software Attack to Multimodal Biometric Systems and its Application to Face and Iris Fusion. *Pattern Recognition Letters*.

[21] Hoang D., Lee Ch., Niyato D., and Wang P. 2011. A survey of mobile cloud computing: architecture,

applications, and approaches. *Wireless Communications and Mobile Computing*.

[22] Fernando, N., Seng W. L., and Wenny R. 2013. Mobile cloud computing: A survey. *Future Generation Computer Systems* 29, no. 1 : 84-106.

[23] Lee, J. 2012. A novel biometric system based on palm vein image." *Pattern Recognition Letters* 33, no. 12:1520-1528.

[24] Wu, K., Jen-Chun L., Tsung-Ming L., Ko-Chin Ch., and Chien-Ping Ch. 2013. A secure palm vein recognition system. *Journal of Systems and Software* 86, no. 11: 2870-2876.

[25] Cao, K., Liaojun P., Jimin L., and Jie T. 2013. Fingerprint classification by a hierarchical classifier. *Pattern Recognition*.

[26] Kuang-Shyr, W., Lee, J., Chang, T., K., and Chang, Ch. 2013. A secure palm vein recognition system. *Journal of Systems and Software* 86, no. 11: 2870-2876.

[27] Guo, J., Chih-Hsien H., Yun-Fu L., Jie-Cyun Y., Mei-Hui Ch., and Thanh-Nam L. 2012. Contact-free hand geometry-based identification system. *Expert Systems with Applications* 39, no. 14 : 11728-11736.

[28] Giot, R., Mohamad E., and Christophe R. 2009. Keystroke dynamics authentication for collaborative systems. In *Collaborative Technologies and Systems, 2009. CTS'09. International Symposium on*, pp. 172-179. IEEE.

[29] Minetti, A. E., Luca P. A., and Tom M. 2007. Keystroke dynamics and timing: Accuracy, precision and difference between hands in pianist's performance. *Journal of biomechanics* 40, no. 16: 3738-3743.

[30] Pfost, J. 2007. The science behind keystroke dynamics. *Biometric Technology Today* 15, no. 2 : 7.

[31] Nauman, M., Tamleek A., and Azhar R. 2011. Using trusted computing for privacy preserving keystroke-based authentication in smartphones. *Telecommunication Systems* : 1-13.

[32] Bergadano, F., Gunetti, D., and Picardi C. 2002. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security (TISSEC)* 5, no. 4: 367-397.

[33] Guven, A., and Ibrahim S. 2003. Understanding users' keystroke patterns for computer access security. *Computers & Security* 22, no. 8: 695-706.

[34] Bhatt, Sh., and Santhanam, T. 2013. Keystroke dynamics for biometric authentication—A survey. In *Pattern Recognition, Informatics and Medical Engineering (PRIME), International Conference on*, pp. 17-23. IEEE.

[35] Araujo, L. C, Luiz, S. J., Miguel, G. L., Lee, L. L., and João B. T. Y. 2005. User authentication through typing biometrics features. *Signal Processing, IEEE Transactions on* 53, no. 2: 851-855.

[36] Choraś, M., and Piotr, M. 2007. Keystroke dynamics for biometric identification. In *Adaptive and Natural Computing Algorithms*, pp. 424-431. Springer Berlin Heidelberg.

[37] Pursani, M. P. J., and Ramteke, P. L. 2013. Mobile Cloud Computing. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 2, no. 4: pp-1512.

[38] Huang, D. 2011. Mobile cloud computing. *IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter* 6, no. 10: 27-31.

[39] Mariño, C., Manuel G. P., Marta P., María Carreira, J., and Gonzalez, F. 2006. Personal authentication using digital retinal images." *Pattern Analysis and Applications* 9, no. 1: 21-33.

[40] Guan, L., Xu K., Meina S., and Junde S. 2011. A survey of research on mobile cloud computing. In *Computer and Information Science (ICIS), IEEE/ACIS 10th International Conference on*, pp. 387-392. IEEE.

[41] Khan, A. N., Mat Kiah M. L., Samee U. Kh., and Madani S. A. 2012. Towards secure mobile cloud computing: A survey. *Future Generation Computer Systems*.

[42] Altinkemer, K., and Tawei W. 2011. Cost and benefit analysis of authentication systems. *Decision Support Systems* 51, no. 3: 394-404.

[43] Saevanee, H., Clarke, N. L., and Furnell, S. M. 2012. Multi-modal Behavioural Biometric Authentication for Mobile Devices. In *Information Security and Privacy Research* (pp. 465-474). Springer Berlin Heidelberg.

[44] Yang, S., and Bal, G. 2012. Balancing Security and Usability of Local Security Mechanisms for Mobile Devices. In *Information Security and Privacy Research* (pp. 327-338). Springer Berlin Heidelberg.