ENHANCED AUTHENTICATION FOR WEB-BASED SECURITY USING KEYSTROKE DYNAMICS

Siti Rahayu Selamat[1], Teh Teck Guan[2] and Robiah Yusof[1]

[1]Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
[2]Infineon Technologies Melaka, Batu Berendam, Melaka, Malaysia

ABSTRACT

Current password authentication system was proven not secure enough to protect the information from intruders. However, various research has been done and the results show the value of FRR still low and the value of FAR still high. Thus, one of the methods suggests, is enhancing the current system using keystroke dynamics. Keystroke dynamics is a type of biometric authentication that does not require any special hardware, easy to use as the same routine as normal password authentication. Therefore, this research proposed an authentication system using keystroke dynamics to prevent the system from intruders. A system is developed that consist of two parts which are enrolment and verification. Then, a prototype is developed for testing process that consists of 3 main modules, namely Enrolment, Client/Server Connection and, Verification and Retraining. Based on the testing, the system proved that the keystroke dynamic authentication system was able to implement in client/server environment and shows the value of EER is low that indicates it provide a better system authentication. In future, the system can be improved by enhancing the security, performance, and user interface.

KEYWORDS

Authentication, Web-based, Biometric, Keystroke Dynamics.

1. INTRODUCTION

Nowadays, more and more sensitive data have been stored and processed by computer systems. Thus, there is a need to increase the security of the system to secure the important data. Normal authentication systems at present are not full proof. Common methods to break the current authentication system, including brute force attack, password dictionary and etc. Most of the current systems only have one-layer protection, in which is the password for those online systems [1]. Thus, if the password has been stolen it means the system is at risk to be breached. In addition, the most common way to enforce authentication is by password, personal identification number (PIN) or another predetermined passcode [2] [3] [4]. Before a user want to perform any intended activity online, he/she is required to enter his/her username and credentials. Unfortunately, it also has many flaws which make it vulnerable to hacking [5] [6] although a normal username/password access control effective to a certain extent.

However, a good password hard to hack must have certain rules. Example: include at least eight characters, some of which capital letters and special characters. Regrettably, hard-to-hack passwords are also hard-to-remember. Subsequently, many users choose passwords that relate to their private lives. As a result, this will open to an opportunity of a hacker to penetrate into their system. This situation becomes worse as the tendencies of users to write their password is very high as one of the methods for remembering their password. This action causes their password

DOI: 10.5121/ijnsa.2020.12401

can be intercepted by intruders. The use of the same password for different purposes on the websites is also leading to the probability of the right password guessed by an attacker is high. Thus, a hacker revealing users' passwords from a non-secure website will gain access to many of the websites that the user has access to. Hacker is hacking into some of the user's bank websites, may incur money lost to the user. Due to these drawbacks, password-based user authentication methods provide only partial protection against hackers or intruders.

In order to counter these types of problems, they need to be complemented by additional authentication. One of the methods that been suggested is implementing a biometric authentication such as physiological and behavioral biometrics [7]. Biometric Authentication is a type of authentication method that uses the human characteristics to identify the user. It is hard to forge human characteristics compare to forge password or ID card, therefore it will enhance the system security with to identify the user biometrically. Thus, this paper proposes Keystroke Dynamic authentication as it is one of the most common and low cost behavioral biometrics in the market now.

The paper is organized as follows: Section 2 provides a review of related work in the field. Section 3 describes the methodology followed in conducting this research. Section 4 presents the proposed system and the reporting results are presented and discussed in Section 5. Followed by conclusion in Section 6.

2. RELATED WORKS

2.1. Biometric taxonomy

There are two distinct meanings for biometric. Bio means living creature and Metric meaning the standard of measure an object quantitatively. Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. Thus, biometrics can be defined as the science and technology of measuring and statistically analyzing biological data. Physiological characteristics are based on measurements of data derived from direct measurement of a part of the human body. Fingerprints, hand geometry, and retina, iris, and facial images are leading physiological biometrics [2]. Behavioral characteristics are based on an action taken by a person [8]. Behavioral biometrics are based on measurements of data derived from an action, and indirectly measure characteristics of the human body [9]. Signatures, voice recordings (which also has a physiological component), and keystroke rhythms are leading behavioral biometric technologies [10]. Thus, biometric characteristics can be divided into two different categories, physiological and behavioral as shown in Figure 1.

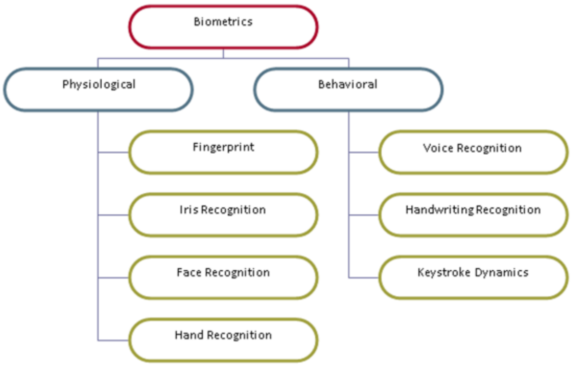


Figure 1. Taxonomy of biometric

Based on Figure 1, physiological are related to the actual body shape of the user, for example fingerprint, iris recognition, face recognition and hand recognition [11]. Behavioral are related to the behavioral of the user for example handwriting recognition, keystroke dynamic and voice recognition.

Biometrics are becoming the foundation of highly secure security identification solutions. It is becoming apparent as the number of security breaches and fraud increases. Currently, biometrics can be found in most at many places including Government Sector, Law and Enforcement, Commercial Sector, Banking Sector, and etc.

Biometrics can operate online or offline depending on the needs of the application. For an online system, it requires recognizing the user and respond immediately. It must use a fully automated system with a live scanner. On the other hand, the offline system doesn't require immediate recognition and it can use a semi-automated system with an offline scanner.

2.2. Keystroke dynamics

Keystroke Dynamics is a type of biometrics authentication. It existed more than 100 years ago where the world uses telegraph to communicate in long-distance, with telegram operators have developed their typing rhythm which can identify. During World War II where military messages were transmitted through Morse code, military intelligence uses this method to distinguish ally from enemy. However, the field of keystroke dynamics is still an emerging field, where most of the challenges need to be overcome for it to become an effective biometric [10].

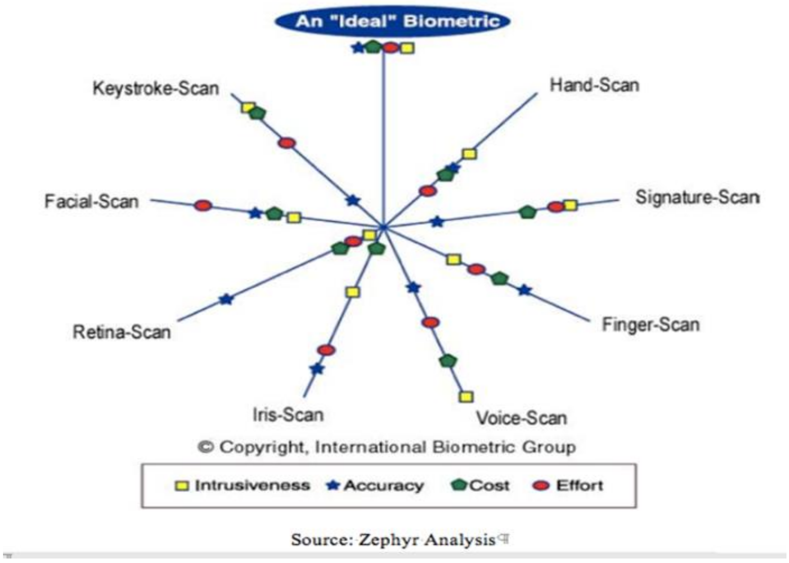
Keystroke Dynamics doesn't require additional hardware to be installed, thus is ready to be used in every computer system [11] [12]. The system will record the typing rhythm when the user key in their username and password [13]. To have a clear comparison with other users, it is strongly suggested to include a standard phrase field whenever the user login through the system. The additional field will increase the security of the system.

The measurement of keystroke timing can be categorized as two, the Dwell Time and the Flight Time [14]. Dwell Time measures the time between key down and next key up. Flight time measure the timing between the key down of a key and the successive key down or the key up of a key and the successive key up. The timing measurement is important as it is the feature that use for comparison.

Similar to other Biometrics Authentication methods, the Keystroke Dynamics authentication system consists of an enrolment part and also a verification part [1]. The enrolment part will register and record the typing rhythm of the new users [1]. The verification part will verify the user by comparing the user's login data with reference data stored in the system's database and updating the existing keystroke template in the database with successful login data to increase the accuracy of the system.

2.3. Keystroke dynamics analysis

Web-based Keystroke dynamics authentication system is designed for secure online systems such as online banking, e-commerce portal, social media and, etc. The system is easy to use and suitable for all different types of the online system. Zephyr chart from the International Biometric Group described the biometric characteristics that can be compared based on several factors namely ease-of-use, cost, accuracy, and intrusiveness as shown in Figure 2.



© Copyright, International Biometric Group

Source: Zephyr Analysis

Figure 2. Biometric Zephyr analysis [http://biometrics.pbworks.com]

In Figure 2, the relative capabilities of each characteristic are represented using symbols. All symbols on the edge represent a perfect biometric system and the symbols that closely to the "center" of the Zephyr chart is considered as a poor biometric system [15]. Thus, based on this chart, four main aspects namely, intrusiveness, accuracy, cost and, effort is focus in the proposed system.

3. METHODOLOGY

In this research, there are six main processes involved as shown in in Figure 3.

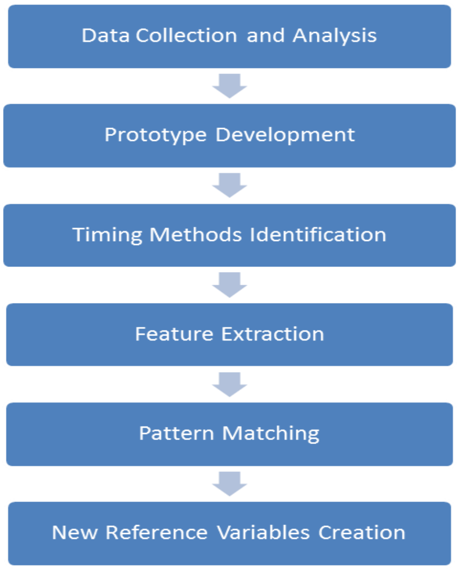

Data Collection and Analysis
Prototype Development
Timing Methods Identification
Feature Extraction
Pattern Matching
New Reference Variables Creation

Figure 3. Proposed Method

3.1. Data collection and analysis

In this research, the data are collected in a real environment. 10 sets of data are collected that involved with 5 selected users. The users are randomly selected.

3.2. Development of Prototype

To verify the performance of the authentication using keystroke dynamics, a prototype of a web-based system is developed. The proposed system is utilized the Microsoft.NET framework, keyboard, and Microsoft IIS. It consists of 3 main modules, namely Enrolment, Client/Server Connection and, Verification, and Retraining.

3.3. Obtaining Keystroke Timing

In this research, several numbers of APIs related to time resolution are analyzed and imported to identify the method of obtaining the keystroke timing. Based on the analysis, several APIs from the combination of the .NET framework and Windows API are selected to obtain high-resolution timing. They are *Now(), Time()* and *Timer(), GetTickCount(), TimeGetTime()* and *QueryPerformanceCounter()* as summarized in Table 1.

Table 1. Comparison of Windows Timer API

Function	**Units**	**Resolution**
Now( ), Time( ), Timer( )	Seconds	1 second
GetTickCount( )	Milliseconds	Approx. 10ms
TimeGetTime( )	Milliseconds	Approx. 10ms
QueryPerformance-Counter( )	QueryPerformance-Frequency	< 1ms

Table 1 shows, API *Now(), Time(), Timer*(), *GetTickCount()* and *TimeGetTime()* have a minimum resolution up to 10 milliseconds, and *QueryPerformanceCounter()* has minimum resolution below 10 milliseconds. *QueryPerformanceCounter()* will able to update between each successive API call which is useful in high-resolution timing compared to other Windows APIs in which the update depends on the background tasks executed by the system.

3.4. Feature Extraction

There are many types of information that can be gathered in a single typing session, including the hold time of the keystroke, release time between keystroke, and also the pressure of the keystroke. The data that collected not only able to construct a digraph, but also suitable for a trigraph, and beyond. The data gathered can be termed as unigraph as it measures the time difference of pressing and release of a single key.

In this research, the collected data will be stored in text file format that allow future enhancement of the system by using MATLAB. Each user will have 3 different text files to store different data, which are: 1) <username> .UNS –User’s Username Typing Data, 2) <username> .UPS – User’s Password Typing Data, and 3) <username> .SNS –User’s Standard Phrase Typing Data. All files will be stored in the same format that will use comma (“,”) as delimiter for each data. The format for the text file is shown as Eq. (1).

<key>, <time for key down>, <key>, <time for key up>   Eq. (1)

The timing of each keystroke's key up and key down will be calculated using formula as shown in Eq. (2).

$$Time = Round\left(\frac{Tickcount}{Frequency} \times 10000\right) \qquad Eq.(2)$$

Where;

Tickcount - Processer's clock counter since the last time the computer was started

Frequency - Processer's frequency (Based on Processer's speed

The *Round* function and multiply by 10000 were applied in order calculate the time different between a range of 1 to 10000.

3.5. Pattern Matching

In this part, the login data are compared with the reference data. For each keystroke, the average and standard deviation for each keystroke are also compared. In this research, the pattern matching is used Down Up (DU) method as shown in Eq. (3).

$$T(K_i) = T_{up}(K_i) - T_{down}(K_i) \qquad Eq.(3)$$

Where;

$T_{i.up}(K_i)$ – Key Up time for keystroke K_i

$T_{i.down}(K_i)$ – Key Down time for keystroke K_i

After gathering all the information, the system will calculate the average, standard deviation, number of samples, and also the sum of the square root of the total hold time and save it in the reference variable files. These values were calculated to speed up the process of identifying the user as the user reference template will grow. The average, standard deviation, and sum of the square root of total hold time value for each keystroke will be counted using Eq. (4), Eq. (5) and Eq. (6) respectively.

$$\mu_{K_i} = \sum_{j=1}^{n} T_j\ (K_i) \qquad Eq.(4)$$

$$T^2(K_i) = \sum_{j=1}^{n} [T_j(K_i)^2] \qquad Eq.(5)$$

$$\sigma_{K_i} = \sqrt{\frac{T^2(K_i)}{n} - \left(\mu_{K_i}\right)^2} \qquad Eq.(6)$$

Where;

$K_i - keystroke$

$T_j(K_i) - The\ time\ interval\ when\ a\ key\ remains\ pressed$

$n - The\ numbers\ of\ samples$

When the user login to the system, the system will then compare the login data with the reference data by using the Gaussian function as shown in Eq. (7).

$$D_{K_i} = 1 \times e^{-\frac{\left[T^2\,(K_i) - \mu_{K_i}\right]}{\sigma_{K_i}}} \qquad Eq. (7)$$

Where;

$K_i - keystroke$

$T_j(K_i) - The\ time\ interval\ when\ a\ key\ remains\ pressed$

$n - The\ numbers\ of\ samples$

$\mu_{K_i} - Keystroke\ reference\ data\ average$

$\sigma_{K_i} - Keystroke\ reference\ data\ standard\ deviation$

If the D_{K_i} is less than or equal $(\leq)$ to the threshold value (τ) that set in the system, the system will recognize the user is authenticated and proceed to allow the user to access the system, else it will reject the user request.

3.6. New Reference Variables Creation

In creating the new reference variable, an algorithm known as a retraining algorithm is used. Therefore, the new variables can be calculated by going through line by line in the user reference template. However, as the template is growing each time the user successfully login, the performance of the system will slow down as there is more data that need to be processed. Thus, new formulas to improve the processing time on calculating the new reference variables were derived by utilizing the current reference variables as presented in Eq. (8) to Eq. (11).

$$\mu_{K_i.New} = \frac{\left(\mu_{K_i.Old} \times n_{old}\right) + T_j(K_i)}{n_{old} + 1} \qquad Eq. (8)$$

$$T^2(K_i)_{New} = T^2(K_i)_{Old} + T_j(K_i)^2 \qquad Eq. (9)$$

$$\sigma_{K_i.New} = \sqrt{\frac{T^2(K_i)_{New}}{n_{old} + 1} - \left(\mu_{K_i.New}\right)^2} \qquad Eq. (10)$$

$$n_{new} = n_{old} + 1 \qquad Eq. (11)$$

Where:

$K_i - keystroke$

$\mu_{K_i.Old} - The\ current\ reference\ average$

$T^2(K_i)_{Old} - The\ current\ sum\ of\ square\ root\ of\ total\ hold\ time$

$T_j(K_i) - The\ time\ interval\ when\ a\ key\ remains\ pressed$

$n - The\ numbers\ of\ samples$

$\mu_{K_i} - Keystroke\ reference\ data\ average$

$\sigma_{K_i} - Keystroke\ reference\ data\ standard\ deviation$

$n_{old} - The\ total\ numbers\ of\ reference\ samples$

By using Eq. (8) to Eq. (11), the new reference variable can be calculated in a faster way that indirectly improved the performance of the system.

4. PROPOSED WEB-BASED KEYSTROKE DYNAMICS

Keystroke dynamics is one of the biometric techniques and it is more secure than a normal password authentication system. Implementation of keystroke dynamics will not affect the current workflow of the password authentication system. The front-end operation will be just the same as the normal password authentication system, with the difference is the backend process where the system will analyze the typing rhythm of the users when he/she entering the username and password. Apart from that, the implementation cost is lower than other biometric authentication methods as it doesn't have to purchase additional hardware except for keyboard, the cost is mainly focusing on software implementation. Time consumption for training users to use the system is minimal as the system is easy to use.

In this paper, a web-based system is developed that consists of two parts which are enrolment and verification. Thus, it will utilize several technologies including ASP.Net and VB.Net. The system consists of three main modules that are, a) Enrolment, b) Verification and retraining, and c) Client/Server Connection.

The functions in the Enrolment module are registering new users and performing data collection of user typing patterns. In this part, the user typing time is recorded and a reference template is created. Then, the verification part will take place in which the match of the similarity between the login and the reference template will be verified based on the threshold set to grant the user accessing the system. While, in the Verification and retraining module, the user is verified and the user's reference template is updated. In this part, the match of the similarity between the login and the reference template will be verified based on the threshold set to grant the user accessing the system. Finally, in the Client/Server Connection module, a communication medium between the client and server is created.

4.1. System Architecture

The architecture of the proposed system that include the main components which are client and Keystroke Dynamic Server is depicted in Figure 4.

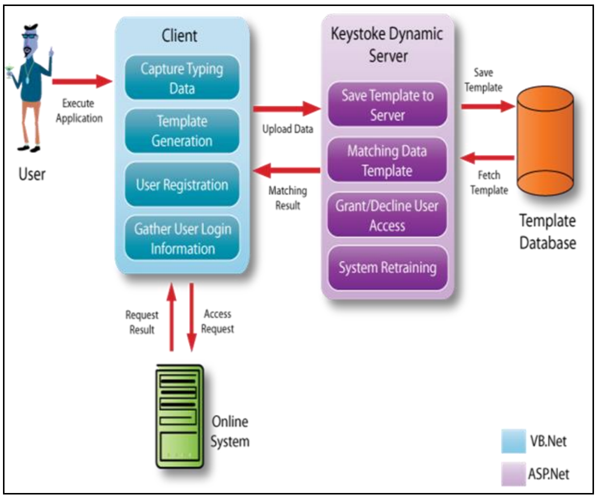


Figure 4. Architecture of Web-based Keystroke Dynamic System

Figure 4 depicts the system architecture for Keystroke Dynamic for the Online system. It is a Client-Server connection. A user or client needs to type his/her username and password to access the system. During this process on the client-side, the system will capture the pattern of the user's typing. Then, this pattern will be sent to the Keystroke Dynamic Server to be verified using the matching algorithm and verify. Once the result is matched (positive), the user is granted to enter the system. The overall processes involved in the proposed system are represented using a flow chart as shown in Figure 5.

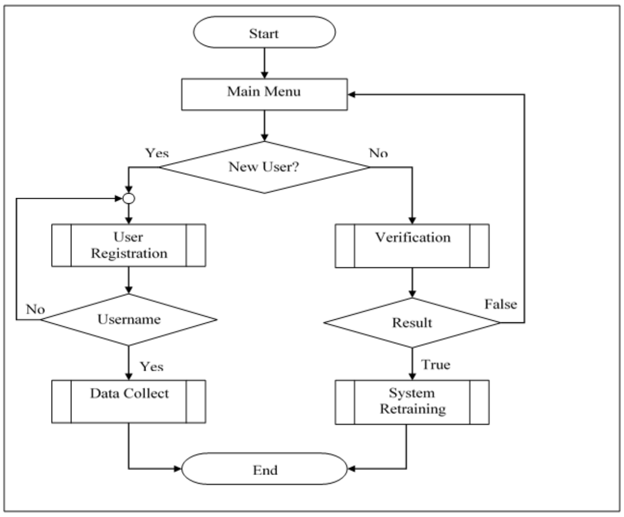


Figure 5. Flow of Web-based Keystroke Dynamic Process

Figure 5 shows the process flow of the keystroke dynamic prototype system. Mainly there are involve in two main parts. First, a user needs to register into the keystroke dynamic system if he/she is a new user. For new user, he/she need to key in his/her name, email, contact number, username, and password. Once he/she is successfully registered as a new user, he/she require to key-in his/her username, password, and standard phrase for 10 times to capture his/her keystroke dynamic typing data and reference template which to be stored in the server's database.

Second, a normal user which has registered can log in to the Keystroke Dynamic system which the username and password. The keystroke info will be captured and send from the client to the server. The verification process will be done on the server-side to verify the user keystroke dynamic info is matching with the username and password reference template. If his/her result is matched, then able to login to the web-based system. After that, the system will do the retraining process to recalculate the user reference template Otherwise, the result is negative which below the score limit, he/she will prompt that does not allow to proceed with the next step.

4.2. User Registration

In this prototype, a user is required to register into the system as shown in Figure 6.

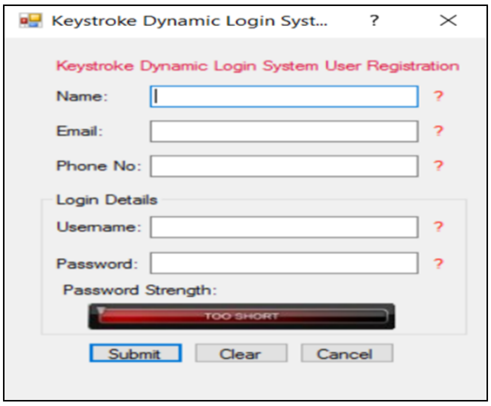


Figure 6. User Registration Interface

As shown in Figure 6, the user is required to enter their particulars including name, email, phone number, username, and also password. Email and phone numbers were collected as the system administrator able to contact the user. The window consists second part which is Login Details where requests the user to enter their preferred username and password as it will become the reference for the data collection and also check the availability of the username.

4.3. Keystroke Data Collection

During the registration, the data of keystroke are collected as shown in Figure 7. Figure 7 shows the keystroke data collection interface. In this interface, the user is given the reference text to be key-in that indicate by red-color text. The progress during the registration process is also shown in the interface using a progress bar to help the user in completing the process.

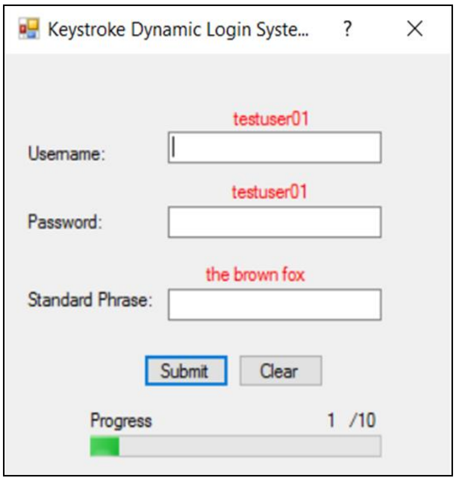


Figure 7. Keystroke Data Collection Interface

4.4. Login Process

After the registration is completed, the proposed application will collect the user typing rhythm and compile into a user template text file and upload it to the server. After successfully upload the files the application will then inform the user has been successfully registered. Then, the user is forwarded to the login page as shown in Figure 8.

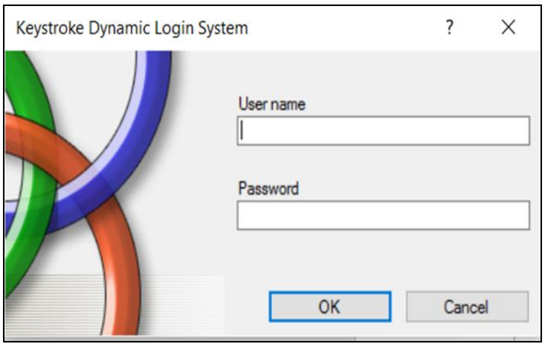


Figure 8. Login page

Figure 8 shows the login page. It looks the same as normal password authentication login page. The difference is the application not only will record down what the user has typed, but also will record down its typing activities which include what key has pressed, time when key pressed and time when key release. All this information is necessary in plot user's keystroke pattern.

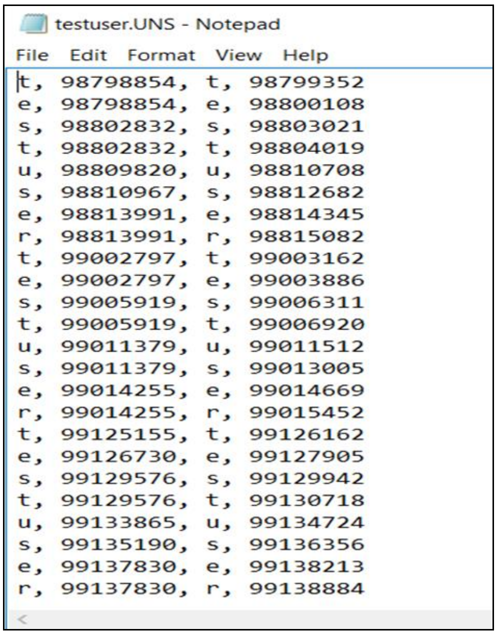
After the user click on the "Ok" button after entering the username and password, the application will then compile the data gather during the user enter the details in a text file and upload it to the server. The server will analyze the file and calculate the average and standard deviation of the data and compare it with the reference data. If the difference between both less the acceptable range, then the system will approve the user login request.

5. Result And Discussion

Based on the prototype developed, the user typing time is recorded and a reference template is created. In this testing, only ten users are selected in the simulation and actual system environment by setting a similar situation for both environments. Then, the match of the similarity between the login and the reference template will be verified based on the threshold set to grant the user accessing the system. Therefore, the result is discussed based on the user enrolment, and the identification of threshold, False Acceptance Rate (FAR) and False Reject Rate (FRR).

5.1. User Enrolment

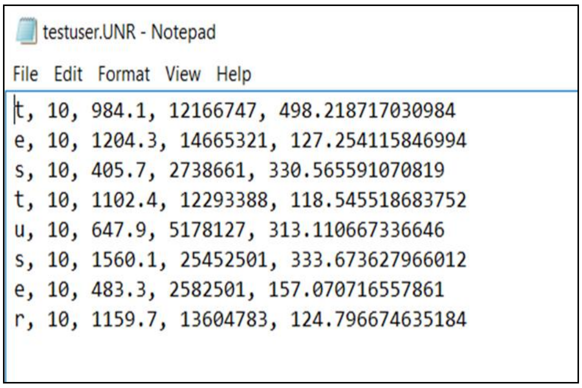
A template of a username and the username statistical values for a user is created as shown in Figure 9 and Figure10 respectively.



```
t, 98798854, t, 98799352
e, 98798854, e, 98800108
s, 98802832, s, 98803021
t, 98802832, t, 98804019
u, 98809820, u, 98810708
s, 98810967, s, 98812682
e, 98813991, e, 98814345
r, 98813991, r, 98815082
t, 99002797, t, 99003162
e, 99002797, e, 99003886
s, 99005919, s, 99006311
t, 99005919, t, 99006920
u, 99011379, u, 99011512
s, 99011379, s, 99013005
e, 99014255, e, 99014669
r, 99014255, r, 99015452
t, 99125155, t, 99126162
e, 99126730, e, 99127905
s, 99129576, s, 99129942
t, 99129576, t, 99130718
u, 99133865, u, 99134724
s, 99135190, s, 99136356
e, 99137830, e, 99138213
r, 99137830, r, 99138884
```

Figure 9. Enrolment - User data template

Figure 9 shows the template of the username for user "testuser". Each keystroke consists of one line where it records the keystroke, key pressed time of the keystroke, keystroke, and key release time of the keystroke.



```
t, 10, 984.1, 12166747, 498.218717030984
e, 10, 1204.3, 14665321, 127.254115846994
s, 10, 405.7, 2738661, 330.565591070819
t, 10, 1102.4, 12293388, 118.545518683752
u, 10, 647.9, 5178127, 313.110667336646
s, 10, 1560.1, 25452501, 333.673627966012
e, 10, 483.3, 2582501, 157.070716557861
r, 10, 1159.7, 13604783, 124.796674635184
```

Figure 10. Enrolment - User Reference Template

Figure 10 shows the template of the username statistical values for user "testuser". Each keystroke consists of one line where it records the keystroke, total sample, average time, square root of total hold time, and standard deviation. For password, the similar templates are also created which are template of the password for user "testuser" and the template of the password statistical values for user "testuser".

5.2. Threshold Identification

In order to get the threshold, several tests were conducted as a research to test the most suitable threshold value for this system by inputting the reference template which collected from the system into the MATLAB to perform the simulation. The testing will test all possible threshold values and will compute its False Acceptance Rate (FAR) and False Reject Rate (FRR). The result of the threshold identification is shown in Figure 11.

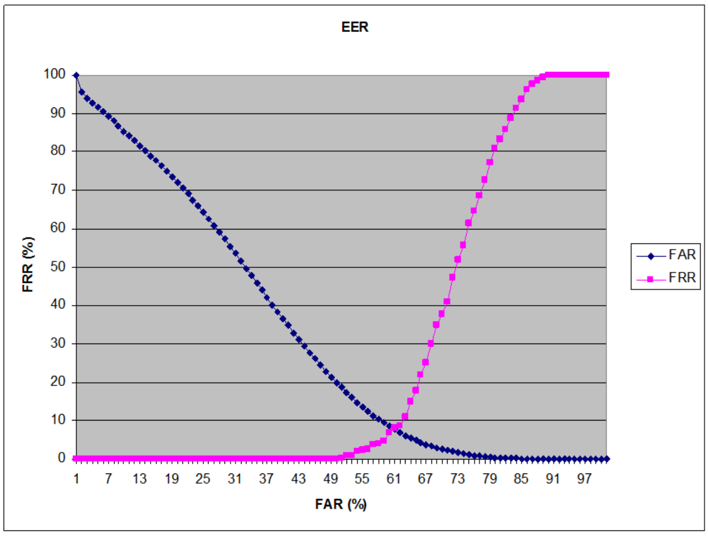
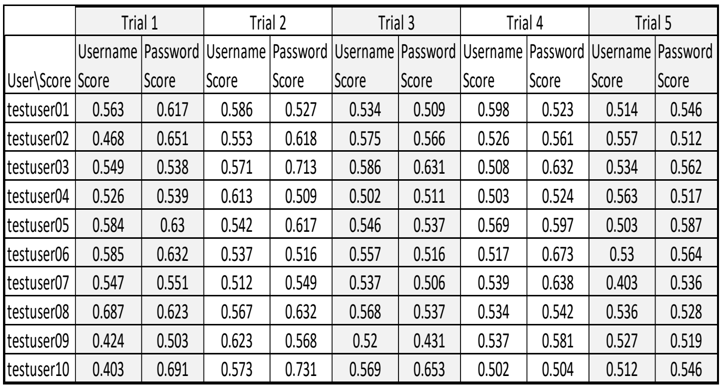


Figure 11. Result of the Threshold Identification

The result shows that the most efficient threshold is 0.56 with the most minimum equal rate which is 7.176%. The test is also done on the actual system by setting a similar situation as the simulation test. 10 sets of scores from 5 different users (testuser01- testuser10) are collected and the results show that the Username average score is 0.554 and the Password average score is 0.579. The details results are shown in Table 2.

Table 2. Actual Keystroke Dynamic (KD) Online System Result



	Trial 1		Trial 2		Trial 3		Trial 4		Trial 5	
User\Score	Username Score	Password Score	Username Score	Password Score	Username Score	Password Score	Username Score	Password Score	Username Score	Password Score
testuser01	0.563	0.617	0.586	0.527	0.534	0.509	0.598	0.523	0.514	0.546
testuser02	0.468	0.651	0.553	0.618	0.575	0.566	0.526	0.561	0.557	0.512
testuser03	0.549	0.538	0.571	0.713	0.586	0.631	0.508	0.632	0.534	0.562
testuser04	0.526	0.539	0.613	0.509	0.502	0.511	0.503	0.524	0.563	0.517
testuser05	0.584	0.63	0.542	0.617	0.546	0.537	0.569	0.597	0.503	0.587
testuser06	0.585	0.632	0.537	0.516	0.557	0.516	0.517	0.673	0.53	0.564
testuser07	0.547	0.551	0.512	0.549	0.537	0.506	0.539	0.638	0.403	0.536
testuser08	0.687	0.623	0.567	0.632	0.568	0.537	0.534	0.542	0.536	0.528
testuser09	0.424	0.503	0.623	0.568	0.52	0.431	0.537	0.581	0.527	0.519
testuser10	0.403	0.691	0.573	0.731	0.569	0.653	0.502	0.504	0.512	0.546

Table 2 shows that 10 sets of data collection of 10 users who have registered with the score when they are trying to access web-based system via the proposed Keystroke Dynamic system for verification. The score is captured and the graph is plotted as depicted in Figure 12.

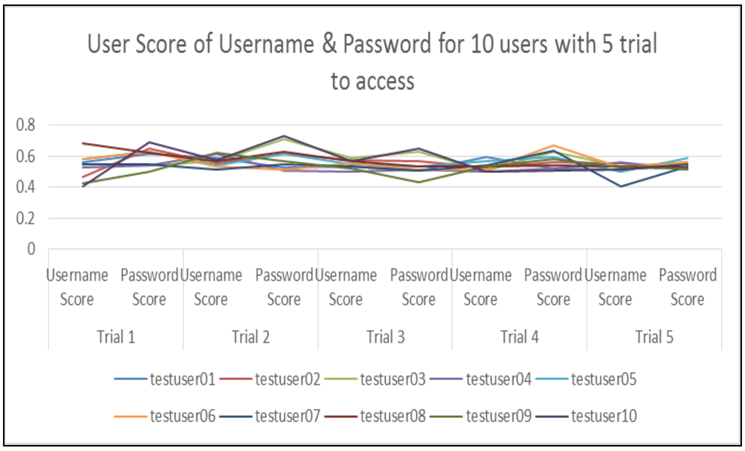


Figure 12. Graph of 10 users score of 5 trial access

Based on Figure 12, it shows that the actual testing result average score of the actual 5 users is around 0.5, which is slightly different from the simulation test result. However, it is significant due to several factors that possibly cause different results including the types of keyboard and the environment of data testing that influence user compatibility. However, the result shows that the keystroke dynamics authentication system is able to implement under a client/server environment.

6. CONCLUSIONS

Keystroke dynamics have a strong behavioral basis which should be explored to the understanding of motor behavior during typing. Using these concepts, models could be built to better understand the processes involved in typing. An understanding of how different people or groups of people type may provide insight into patterns in biometric features such as age, gender, and environment. This might help in the development of better classifiers which could improve the accuracies of existing systems. Based on the result obtained, the performance of the authentication is robust and enhanced. Hence, it will improve the password authentication system in terms of security and performance-wise. In the future, some improvements can be done on the user template and the matching algorithm by encrypting the template and implementing more complex algorithms including fuzzy logic and Hidden Markov Models. Apart from that it also can include all timing calculation methods.

ACKNOWLEDGEMENTS

Thank you to the Research Group of Information Security Forensics and Computer Networking, Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Sarma, P., Yadav, A. K., and Barma, S. (2019). Keystroke Rhythm Analysis Based on Dynamics of Fingertips. In Machine Intelligence and Signal Analysis (pp. 555-567). Springer, Singapore.

[2] Schclar, A., Rokach, L., Abramson, A., and Elovici, Y. (2012). User authentication based on representative users. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42(6), 1669-1678.

[3] A. El-Saddik, M. Orozco, Y. Asfaw, S. Shirmohammadi, and A. Adler,“A novel biometric system for identification and verification of haptic users,” IEEE Trans. Instrum. Meas., vol. 56, no. 3, pp. 895–906, Jun. 2007.

[4] N. J. Grabham and N. M. White, “Validation of keypad user identity using a novel biometric technique,” J. Phys.: Conf. Ser., vol. 76, no. 1, pp. 012023-1–012023-6, 2007.

[5] A. Peacock, X. Ke, and M. Wilkerson, “Typing patterns: A key to user identification,” IEEE Security Privacy, vol. 2, no. 5, pp. 40–47, Sep./Oct. 2004.

[6] Leggett. J., Williams, G., Usnik, M. (1990) Dynamic identity verification via keystroke characteristics, International Journal of Man-Machine Studies, v35 p859-870.

[7] Sadikan, S. F. N., Ramli, A. A., and Fudzee, M. F. M. (2019, November). A survey paper on keystroke dynamics authentication for current applications. In AIP Conference Proceedings (Vol. 2173, No. 1, p. 020010). AIP Publishing LLC.

[8] Arun, V., and Sudhakar, R. (2019). User Behavioral Analysis Using Markov Chain and Steady-State in Tracer and Checker Model. Journal of Cyber Security and Mobility, 8(2), 277-294.

[9] Teh, P. S., Teoh, A. B. J., and Yue, S. (2013). A survey of keystroke dynamics biometrics. The Scientific World Journal, 2013.

[10] A. P. Rohit and L. R. Amar, “Keystroke dynamics for user authentication and identification by using typing rhythm.” International Journal of Computer Applications, Vol. 144, No. 9, 27–33, (2016).

[11] Banerjee, S. P., and Woodard, D. L. (2012). Biometric authentication and identification using keystroke dynamics: A survey. Journal of Pattern Recognition Research, 7(1), 116-139.

[12] Muliono, Y., Ham, H., and Darmawan, D. (2018). Keystroke dynamic classification using machine learning for password authorization. Procedia Computer Science, 135, 564-569.

[13] Kim, J., Kim, H., & Kang, P. (2018). Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection. Applied Soft Computing, 62, 1077-1087.

[14] Patil, R. A., and Renke, A. L. (2016). Keystroke dynamics for user authentication and identification by using typing rhythm. International Journal of Computer Applications, 144(9), 27-33.

[15] Khodaskar, H. V., and Mane, S. (2017). Human face detection & recognition using raspberry Pi. International Journal of Advanced Engineering, Management and Science, 1-2.

AUTHORS

Siti Rahayu Selamat is currently a lecturer at the Universiti Teknikal Malaysia Melaka, Malaysia. She received her Ph.D. Digital Forensics. Her research interests include network forensic, cyber terrorism, cyber violence extremism, intrusion detection, network security, and penetration testing. She is also a member of Information Security, Forensics and Networking (INSFORNET) research group, and actively doing research on malware, criminal behavior, and cyber violence extremism profiling.

The **Teck Guan** is a student Master in Computer Science (Internetworking) at the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia. His master project is authentication using biometrics technology. He is also interested in the area of network security. Currently, he was working as an executive in the IT department.

Robiah Yusof is currently a senior lecturer at the Universiti Teknikal Malaysia Melaka, Malaysia. She received her Ph.D. in Network Security from Universiti Teknikal Malaysia Melaka. Her Research interests include intrusion detection, malware, network security, and network forensic.