Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.917 – 925

RESEARCH ARTICLE

AUTHENTICATION ENHANCEMENT BASED ON MOUSE AND KEYSTROKE FEATURES

Rohan V. Ponkshe[1], Prof. Vikrant Chole[2]

[1]M.Tech Scholar, Department Of Computer Science, GHRAET, Nagpur India

[2]Department Of Computer Science, GHRAET, Nagpur India

[1] rponkshe@rediffmail.com; [2] vikrantchole@raisoni.net

Abstract:- In this paper we introduced a new highly secured authentication method. This authentication method is based on keystroke and mouse movement along with the current username and password system. To identify the genuine user SVM algorithm is used. SVM analyzed the timing of keystroke and different click timings of mouse to differentiate genuine user from the imposter. This authentication method is implemented in MATLAB 2010. Analysis of results shows that, addition of keystroke and mouse dynamics as a security parameter along with username and password system provide high security as compared to the current authentication method.

I. Introduction

In current trade, most computer systems and online websites, identifies users by forcing them to enter the unique username and password or PINS. But there are many techniques nowadays by using which hackers can easily get username and password of a targeted user. Key loggers and phishing attack are some of those techniques. Drawback of this authentication system based on username and password lead to the introduction of authentication and verification technique based on physiological and behavioral biometric which are assume to be unique for each user and hard to steal.

Behavioral biometric includes characteristics of interaction of user and input devices such as mouse and keyboard, while physiological biometric uses human feature such as fingerprints and iris pattern which is unique to each individual. We are focusing on a behavioral biometric system because it does not require dedicated hardware as in physiological it requires. Obviously cost to implement this system is not more than physiological system.

Here, we introduced the hybrid approach in which both keystroke and pointing device movement acts as a characteristic to authenticate user along with username and password.

II. Keystroke Biometric

To increase the level of security in the authentication process, there is need to add more security parameters other than username and password. The most promising method nowadays is the typing style of the user which acts as the security parameter in combine with current authentication system.

The typing style of the genuine user is recorded in terms of the timings (i.e. Dwell Time and Flight Time). It is very tough for an intruder to crack username, password and the timing of genuine user.

A. Keystroke dynamics parameters:

1) ***Dwell time [6] [7]:*** It's the time interval between a key pressed until it is released (Press – Release). This calculates the time duration for which key holds by the user. The key hold time is the dwell time.
Dwell time is of the first key pressed is denoted by,

$$D1 = R1 – P1$$

2) ***Flight time [8] [6] [7] [9]:*** The time interval between a key press and the successive key press (Press – Press) is called as flight time. It's the consecutive press key time difference called as press time. The time difference between releases of two consecutive key releases is called as release-release time. The combination of the both the features terms as flight time.

$$D2 = P2- P1$$

$$D3 = R2- R1$$

Password of genuine user as well as the typing style of the user in terms the Dwell and Flight timing are input to the authentication system which makes it hard for the hacker to gain access of users account.

III. Mouse Dynamics

Mouse dynamics is a part of behavioral biometrics which can authenticate the user with the less amount cost. The handling of mouse is a parameter to the security in mouse dynamics. Mouse dynamics focuses on the usage of mouse while handling the system.

The mouse dynamics focuses on basic as well as advanced features. Single clicks and double clicks [10] are used gather the clicks related data. Data is stored and the other details of distance coverage also helpful to separate the legitimate user from hacker.

A. Features related to mouse dynamics:

1) ***Single Click statistics:*** It is the time interval between two consecutive single clicks.

2) ***Double click statistics:*** It is the time interval between two consecutive double clicks.

IV. Goals and Objectives

- To evolve a method for user authentication
- To establish user authentication with minimum hardware
- To provide high level of security to the users
- To achieve the authentication with minimal cost
- To carry performance analysis of suggested architecture.

V. Related Work

A. Keystroke dynamics:

In 2012, Pin Shen Teh et Al. [5] proposed the fusion of the two methods named as Gaussian Probability Density Function (GPD) and Direction Similarity Measure (DSM). Author performed two methods separately and formed fusion frameworks. The multiple layers multiple experts provided the best result with EER of 1.404%.

In 2009, Pilsung Kang et al. [1] proposed a nearest neighbor based novelty approach with the help of convex hull. Author checked the approach with 13 novelty detectors for a real world application in which keystroke is used. The outcome showed promising results with the updating strategy of keystroke.

In 2007, Kenneth Revett [2] used probabilistic neural network on 50 users to obtain FAR of 4% and FRR of 4%. The advantage of this method is to work with missing and mixed data. The future work included permutation and combination on attribute selection.

B. Mouse dynamics:

Feher et al. [3] proposed a novel verification method based on observing each individual mouse action performed by the user. The basic actions are left click, right click, mouse move sequence and drag-and-drop action. The amount of time required for computation got reduced as compared to histogram method. The method produced EER of 8.53%.

Author described a new behavioral biometric system based on the pointing device. Using statistical pattern recognition system, author developed classifier based on user interaction which accepts the user if he satisfies the threshold. Parson density estimation and a unimodal distribution are used as statistical model. Author used memory game to collect the pointing device feature and testing showed that mouse can be used for authentication purpose. [4]

VI. Implementation

The keystroke and mouse system is part of advanced security level of security. The username-password system shows a low level security for the hacker. We have implemented the system by extracting the parameters from the keystroke and mouse. The dwell and flight time parameters are extracted from the keystroke and the combination of dwell and flight time shows the higher accuracy than the individual one.

To improve the results we have checked the mouse dynamics. The use of single clicks and double clicks are also added. The double clicks show the improved results than the single click. We have provided username password system to the user. Every user has to enter the username and password into the system. After that he has to enter passphrase of fix length for the 5 times, this event captures the keystrokes of the user and from that Dwell time and Flight time are calculated.

The mouse dynamics is provided with the task. The mouse dynamics shows the single and double clicks statistics. The mouse double clicks show better results.

We have used SVM (support vector machines). SVM is generally used for image processing. The use of algorithm is done for the separation of imposter and genuine user. The SVM takes care of the user's security and provides the best outcome. We have tested the system for 40 users using keystroke and mouse.

VII. Result And Analysis

We have done experimentation of users for the results and analysis. The Following parameters come in to the picture.

A. For Dwell and Flight time (FAR):

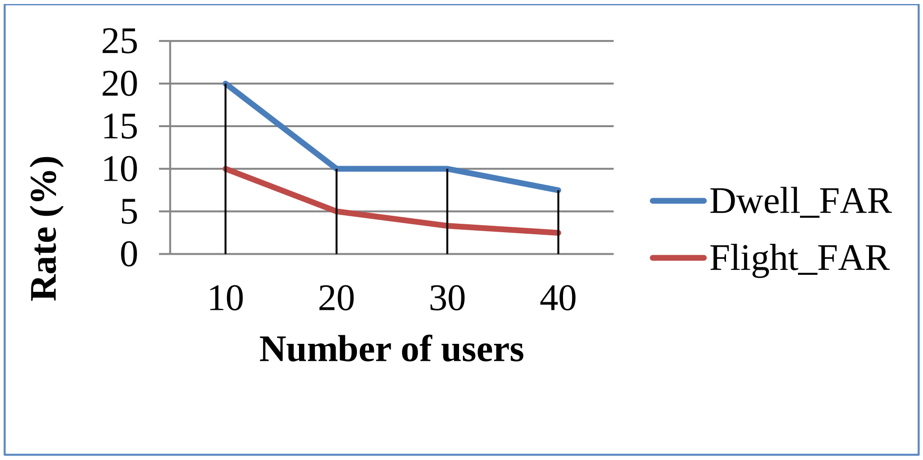

Figure1. Comparisons of Dwell and Flight Time FAR

The figure 1 shows the comparison between Dwell and Flight time FAR for the number of users. X-axis shows number of users. Y-axis shows the rate of accuracy. As the number of users increase, Flight time FAR shows better results in all cases. Hence we can suggest that Flight time FAR works better than Dwell time FAR.

B. For Dwell and Flight time (FRR):

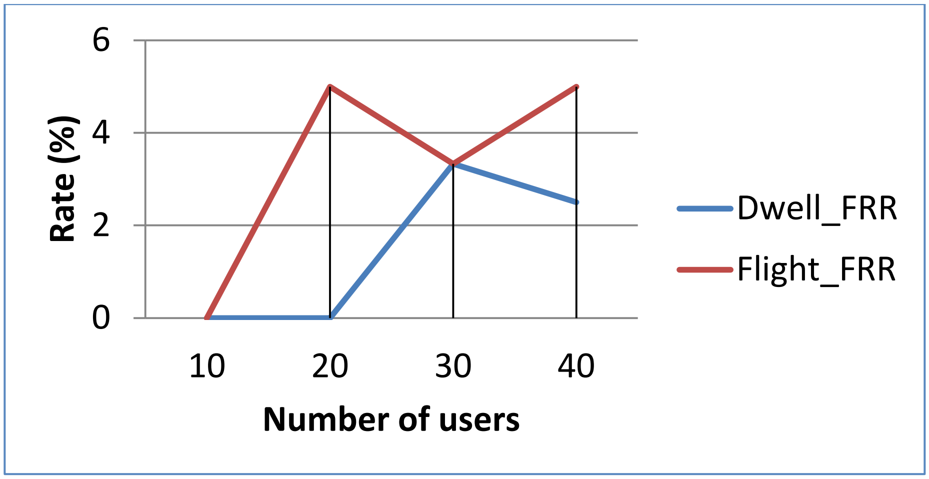

Figure2. Comparisons of Dwell and Flight Time FRR

The figure 2 shows the comparison between Dwell and Flight time FRR for the number of users. X-axis shows number of users. Y-axis shows the rate of accuracy. As the number of users increase, dwell time FRR shows better results in all cases. Hence we can suggest that Flight time FRR works better than Dwell time FRR. If we consider Dwell and flight time including FAR and FRR, flight time works better than Dwell time.

C. Combination of Dwell & flight time (FAR):

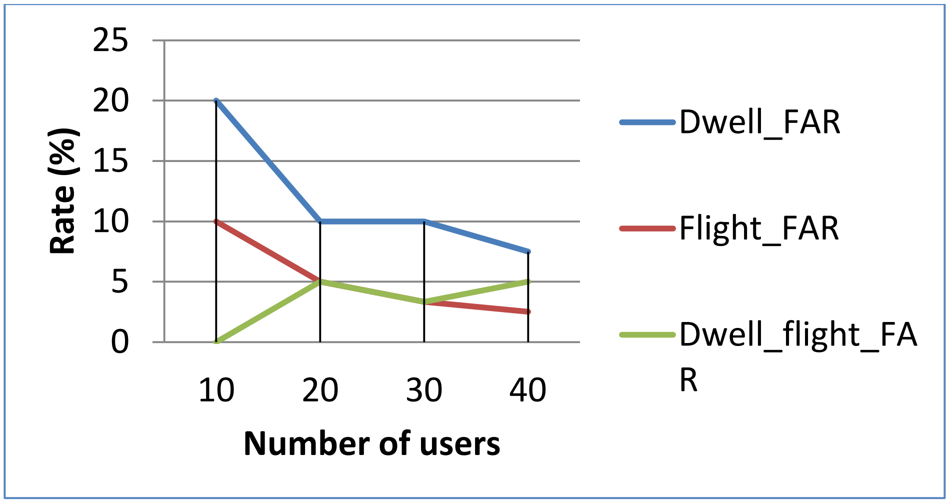

Figure3. Comparisons of Dwell and Flight Time FRR

The figure 3 shows the comparison between Dwell and Flight time FRR for the number of users. X-axis shows number of users. Y-axis shows the rate of accuracy. As the number of users increase, the combination of Dwell and Flight time shows worst result than individual one. It's due to combination of both the parameters, dwell time and flight time. The idea of combining dwell and flight does not give us the improved results.

D. For combination of Dwell & flight time (FRR):

The figure 4 shows the comparison between Dwell, Flight and combination of dwell and flight time FAR for the number of users. X-axis shows number of users. Y-axis shows the rate of accuracy. As the number of users increase, the combination of Dwell and Flight time shows better result than individual one.

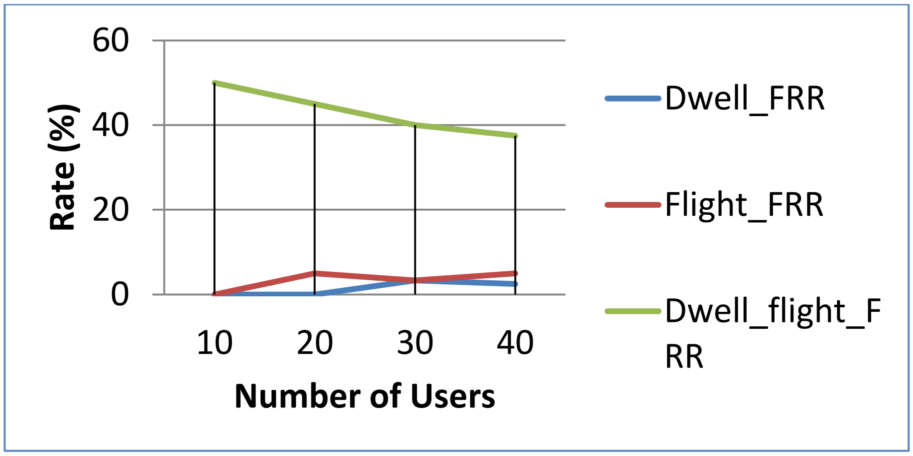

Figure4. Comparisons of Dwell and Flight Time FRR

E. Comparison of Single and Double click (FAR):

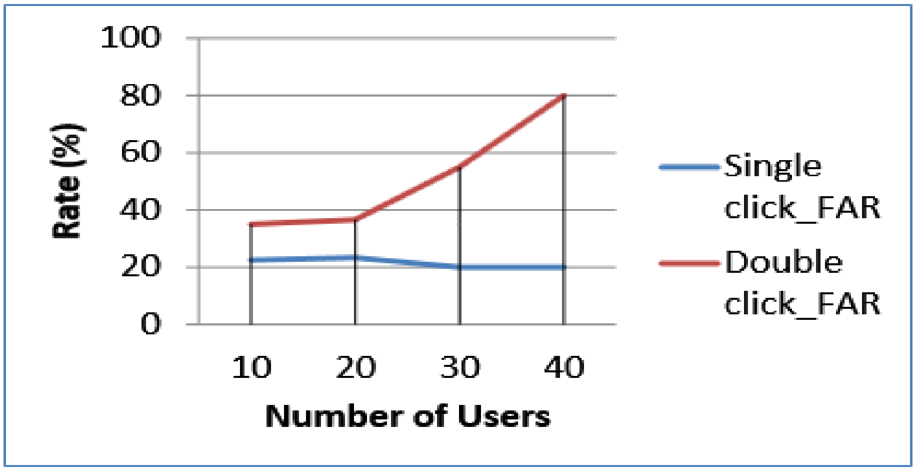

Figure5.Comparison of Single and Double click (FAR)

The figure 5 shows the comparison between Single and double time FAR for the number of users. X-axis shows number of users. Y-axis shows the rate of accuracy. As the number of users increase, Single click shows the better accuracy when we consider FAR.

F. Comparison of Single and Double click (FRR):

The figure 6 shows the comparison between Single and double time FRR for the number of users. X-axis shows number of users. Y-axis shows the rate of accuracy. As the number of users increase, single click FRR shows better results than double click.

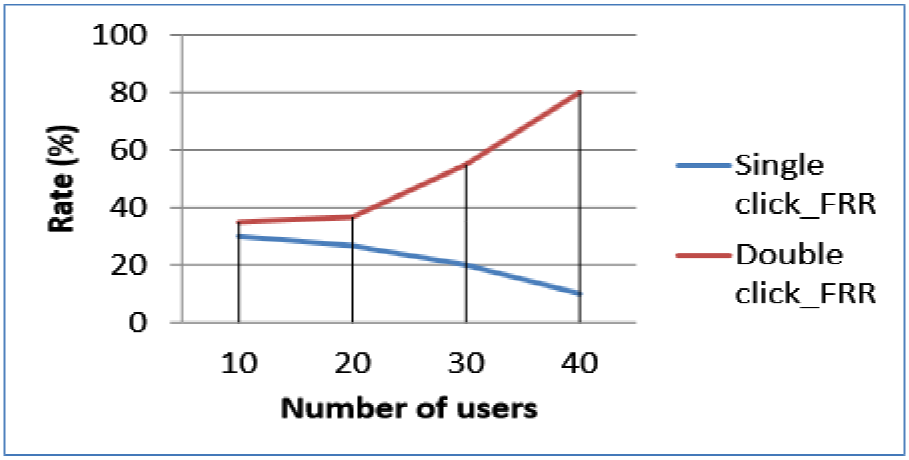

Figure6. Comparison of Single and Double click (FRR)

G. Fusion of keystroke and mouse (FAR):

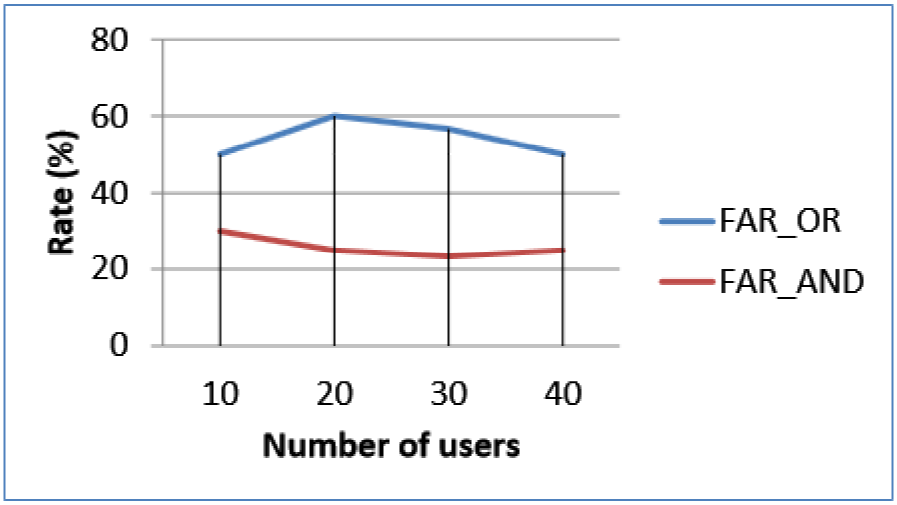

Figure7. Fusion of keystroke and Mouse (FAR)

The figure 7 shows the comparison between OR and 'AND' rule FAR for fusion of keystroke and mouse of number of users. X-axis shows number of users. Y-axis shows the rate of accuracy. 'AND' rule shows better accuracy in terms of FAR.

H. Fusion of keystroke and mouse (FRR):

The figure8 shows the comparison between OR and 'AND' rule FRR for fusion of keystroke and mouse of number of users. 'AND' rule shows better accuracy in terms of FRR. The fusion of keystroke and mouse using OR rule shows below 10% FAR and 'AND' rule shows 20-25% FRR

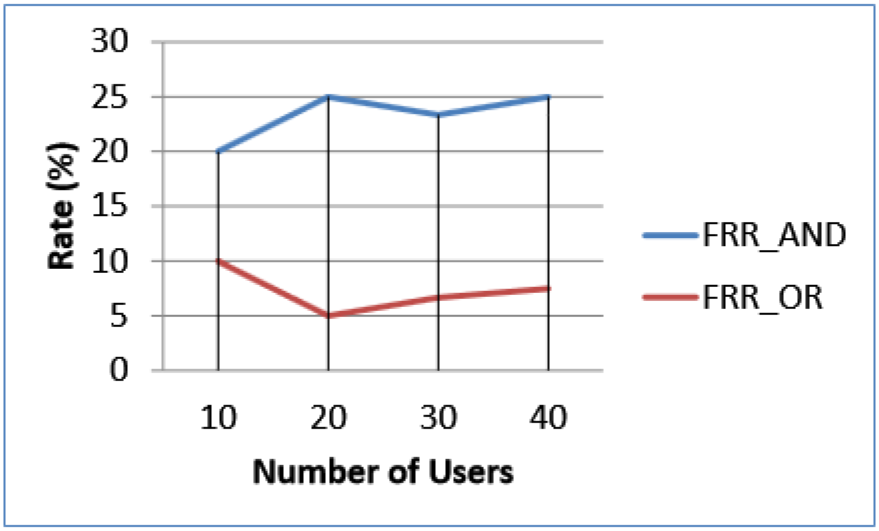

Figure8. Fusion of keystroke and Mouse (FRR)

Conclusion:

The keystroke and mouse features are combined and provides a high level security using keystroke parameters called as dwell and flight time. These keystroke parameters are combined with the mouse parameters to provide high level of security. The combination of dwell and flight time with single click shows better results. The accuracy of combination of keystroke and mouse authentication shows more than 85%. The future scope includes the identification of other parameters and the use of another algorithm to improvise the level of security and implementation of keystroke on touch screen system (LAPTOP, ATM) and use of pressure keyboard.

REFERENCES

[1] Pilsung Kang and Sungzoon Cho, "*A hybrid novelty score and its use in keystroke dynamics-based user authentication*", Pattern Recognition Volume 42, Issue 11, pp. 3115–3127, November 2009

[2] Kenneth Revett, Florin Gorunescu, Marina Gorunescu, Marius Ene, Sérgio Tenreiro de Magalhães and Henrique M. Dinis Santos, "*A machine learning approach to keystroke dynamics based user authentication*", Int. J. Electronic Security and Digital Forensics, Vol. 1, No. 1, pp. 55-70, 2007

[3] Feher C, Elovici Y, Moskovitch R, Rokach L, Schclar A, "*user Identity verification via mouse dynamics",* Information Sciences, Volume 201, pp. 19-36, 2012

[4] Hugo Gamboa, Ana Fred, "*A behavioral biometric system based on human-computer interaction*", Proc. SPIE 5404, Biometric Technology for Human Identification, 381, August 25, 2004

[5] Pin Shen Teh, Andrew Beng Jin Teoh, Connie Tee and Thian Song Ong, 2012, "*Keystroke dynamics in password authentication enhancement*", Expert Systems with Applications, Volume 38, Issue 12, pp. 8618–8628, December 2012

[6] Lisa M. Vizer, Lina Zhou, Andrew Sears, "*Automated stress detection using key stroke and linguistic features: An exploratory study*", ELSEVIER, Int. Human-ComputerStudies68, pp 880–886, 2009

[7] John A. Robinson, Vicky M. Liang, J. A. Michael Chambers, and Christine L. MacKenzie, "*Computer User Verification Using Login String Keystroke Dynamics*", IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, Vol. 28, No. 2, March 1998

[8] H.-R. Lv and W. Y. Wang, "*Biologic Verification Based on Pressure Sensor Keyboards and Classifier Fusion Techniques*", Consumer Electronics, IEEE Transactions on (Volume: 52, Issue: 3), pp 1058 - 1063, Aug. 2006

[9] Chao Shen, ZhongminCai, Xiaohong Guan, Youtian Du and Roy A. Maxion, "*User Authentication through Mouse Dynamics*", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013

[10] Patrick Bours, "*Continuous keystroke dynamics: A different perspective towards biometric evaluation*", Information Security Technical Report Volume 17, Issues 1–2, pp. 36–43, February 2012