ISSN No. 0976-5697

Volume 3, No. 4, July- August 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

User Authentication based on Keystroke Dynamics Using Backpropagation Network

Sarab M. Hameed*
Computer Science Department
College of Science
University of Baghdad, Iraq
sarab_majeed@yahoo.com

Mais M. Hobi
Computer Science Department
College of Science
University of Baghdad, Iraq
mais.shms@yahoo.com

Abstract: Computer systems and networks are being used in almost every aspect of our daily life; as a result the security threats to computers and networks have also increased significantly. Traditionally, password-based user authentication is widely used to authenticate legitimate user in the current system but this method has many loop holes such as password sharing, shoulder surfing, brute force attack, dictionary attack, guessing, phishing and many more.

The aim of this paper is to enhance the password authentication method by presenting a keystroke dynamics with back propagation neural network as a transparent layer of user authentication. Keystroke Dynamics is one of the famous and inexpensive behavioral biometric technologies, which identifies a user based on the analysis of his/her typing rhythm.

This paper utilizes keystroke features including dwell time (DT), flight time (FT), up-up time (UUT), and a mixture of theses features as keystroke representation. The back propagation neural network is trained with the mean of keystroke timing information for each character of password. These times are used to discriminate between the authentic users and impostors.

Results of the experiments demonstrate that the backpropagation network with UUT features comparable to combination of DT and FT. Also, the results of backpropagation with combination of DT, FT and UUT provide low False Alarm Rate (FAR) and False Reject Rate (FRR) and high accuracy.

Keywords: Back propagtion, Biometrics, Dwell Time, Flight Time, Keystroke Dynamics, Neural Network, Up-Up Time, User Authentication.

I. INTRODUCTION

The number of computer user's has increased rapidly and so too has the use of internet applications such as e-commerce, online banking services, web mail, and blogs. All internet applications require the user to use an authentication scheme to make sure only the genuine individual can login to the application [1-3].

User authentication is the process of verifying claimed identity. This is done for the purpose of performing trusted communications between parties for computing applications. User authentication is categorized into three classes including knowledge based, object or Token based, and biometric based as shown in figure (1) [4].

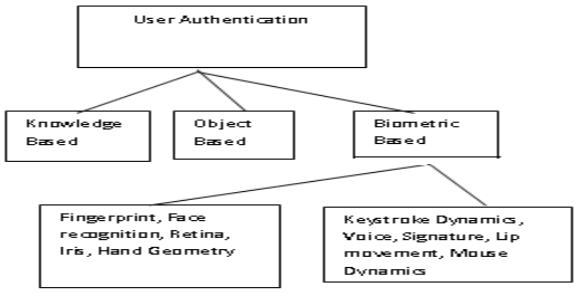

Figure 1: User Authentication Classification

The knowledge-based authentication is based on something one knows and is characterized by secrecy. The object-based authentication relies on something one has and is characterized by possession. The Biometric-based user authentication is based on something you are and depends on behavioral and/or physiological characteristics of individuals. In knowledge-based and object-based approaches, passwords and tokens can be forgotten, lost or stolen. Biometrical mechanism is the strongest way to authenticate people, that is, to verify their identity[5].

Because biometric characteristics are unique to each person and could not be stolen, lost or forgotten.[6]

However, they usually require expensive hardware to support the dedicated function.

Biometrics can be divided into two categories, physiological and behavioral. The first category contains the features that are physically related to a person, for example, fingerprint, DNA, retina, iris pattern, facial, palm print, and hand geometry. The second category contains features that people have learned to do in a stable manner. Examples in this category are walking (gait), writing a signature, lip movement, mouse dynamic, voice and typing on a keyboard (keystroke dynamics).

The authentication via keystroke is based on the idea that each user has a keystroke latency pattern which is different from others [7]. There are two types of keystroke dynamics.

The first one is the static keystroke dynamics in which the data that is typed is fixed and also the time this information is typed in is fixed during login time.

The second one is continuous keystroke dynamics which authenticates individuals independently of what they are typing on the keyboard and the typing characteristics are analyzed during a complete session.

Although the password approach is the most widely used, as well as being the simplest and least expensive tool, it has loopholes because people tend to choose as passwords such easy-to-guess words and/or numbers as the names of family members, birthdays, phone numbers, addresses, etc. The result is a security failure. Some other means should be devised which replaces or consolidates the password approach [8].

This paper looks at keystroke dynamics as a method for authentication to consolidate the password approach. Keystroke dynamic is a process of analyzing keyboard typing characteristics or keyboard typing rhythms by

monitoring keyboard inputs. In other words, the system verifies how a person types.

This paper is organized as follows. Section 2 presents related work. Section 3 illustrates the features of keystroke dynamics and the features that are used in the proposed approach. Section 4 demonstrates how the data was collected. Section 5 presents the proposed approach. Finally the results and the conclusion are given in sections 6 and 7 respectively.

II. RELATED WORK

This section reviews some of the related work in area of keystroke dynamics. One of the most primitive studies done on keystroke dynamics had been done by Gaines and Lisowski [9]. The experiment involved six professional secretaries at the Rand Corporation as subjects. Each was asked to type three passages, consisted of 300-400 words each, and at two different sessions separated by 4 months. The time between each pair of successive keystrokes was calculated and recorded from the experiment, and the test statistical tool was used to check the hypothesis that two populations have the similar average and standard deviation. It was insufficient to make an accurate judgment due to a small number of users involved. It was also inapplicable in real cases because of the large length of the text required as input.

Joyce and Gupta [10], a mean reference feature was computed from eight sets of the users' keystroke patterns consisted of username, password, first name, and last name. They computed the norm of difference between the test keystroke feature and mean reference feature, which were used to determine if a user was legitimate based on a predefined threshold. The experiment involved 33 users.

Monrose et al. [11] asserted that keystroke recognition based on fixed-text is more desirable than free-text. This is because there are several factors such as uncontrolled environmental parameters, unconstrained inputs, and uncooperative user, which impose restriction on the usage of free-text recognition. Keystroke data were collected from a population of 63 users over a period of 11 months. The keystroke feature extracted was keystroke duration and keystroke latency.

Cho et al. [12] was employed a neural network to distinguish between legitimate user and imposter. The extracted keystroke features keystroke are duration and keystroke latency, also the experiment involved 21 users Dowland et al. [13] collected the typing samples of five users by monitoring their regular computer activities, without any particular constraints being imposed on them such as asking users to type predefined set of words. They selected the features (2-graphs only) that occurred least number of times across the collected typing samples. They use keystroke latency which is the elapsed time between the release of the first key and the press of the second key. They build user profiles by computing the mean and standard deviation of 2-graphs latency.

D'Souza [14] proposed a simple statistical method on identifying user based on their typing dynamics. The experiment involved ten subjects, each user was required to repeatedly provide their username, password and a predefine phrase of text for ten times. The duration of each key press and the time duration between each different key press were considered. The author computed the mean and standard deviation of the collected keystroke features as template.

Joshi [15] used a neural network to classify legitimate user and attacker. The extract duration feature was used and employed 43 users in their experiment.

III. KEYSTROKE DYNAMICS FEATURES

There are several different features which can be extracted when the user presses keys on as listed below [16] [17]:

a. Dwell time (DT) or Duration: The time interval between a key pressed until it is released.
b. Flight time (FT) or latency: The time interval between a key release and the successive key press.
c. Up-Up time (UUT): The time interval between a key release and the successive key release.
d. Down-down time (DDT): the time interval between two successive key presses.
e. Pressure of keystroke used when hitting keys while typing.
f. Finger placement the place where the finger is placed on the key or even the angel of the finger when pressing the key (in this case a camera is required).
g. Finger choice which finger is used for which key of the keyboard.
h. Difficulties of typing text.
i. Frequency of word errors.
j. Typing rate.

However, not all kinds of the above mentioned features are useful and widely used. In order to measure keystroke pressure, a special type of pressure sensitive keyboard needs to be used. However, frequency of word errors, typing rate, and difficulties of typing text is only useful on long text. Since user will be providing only username, password and a fixed text phrase, the three aforementioned features are not suitable to be utilized because the length of those inputs are rather short in most cases.

Existing work in the literature of static keystroke dynamics authentication as mention in section two focuses on DT or FT or a mixture of DT and FT. This paper studies the first three types of keystroke dynamics features namely DT, FT, and UUT and analyzes each of the performance separately. Also, a combination of two features namely DT and FT and a combination of DT, FT and UUT features are used and these performances are analyzed. Figure 2 depicts DT, FT, and UUT features.

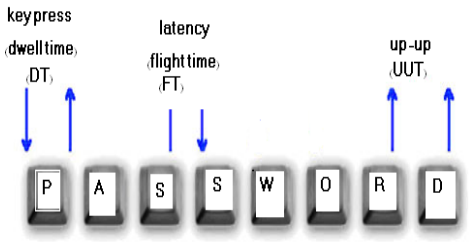

Figure 2: DT, FT, UUT Representation

IV. DATA COLLECTION

The keyboard property was set to enable the proposed keystroke dynamics authentication system to distinguish between two classes of users legal and illegal.

The data was collected from a students and staff of University of Baghdad/college of science. A total of 17 users participated in the experiment. The participated users are divided into two groups: the first group contains 6 users as authentic users while a second group contains 11 users' impostors.

Initially, each participant had to register the determined password during a login session. All participants were requested to enter the same password since the objective was to determine whether the proposed approach could identify and differentiate a particular user from the rest. Note that the participants were not informed of the data collection and analysis approach.

During the data collection phase, a user typed the password "*computer*" for 25 times during three weeks because there is a chance that when the user types continuously the same password again and again the typing speed may increase. Thus, a database of 17 user profiles, where each profile contained number of samples of keystroke features (timing vector) was measured in milliseconds. The password "*computer*" considered weak because of the relative ease with which a third party can guess them or find them via dictionary attacks.

On the other hand, a second password "*comp.84-rl*" was chosen which satisfies the password selection criteria, i.e., at 10 characters in length combining symbols, numbers, and letters. The participants were asked to practice typing the password beforehand. Moreover, the user typed the password "*comp.84-rl*" for 25 times during three weeks. Accordingly, a second database of 17 user profiles was obtained. These two databases where the first contains weak password "*computer*" and the other contains strong password "*comp.84-rl*" were used to evaluate the proposed keystroke dynamics.

The length of the timing vector is different and depending on the length of the password and the type of feature used. For example, a password "*computer*" which contains eight characters will result in eight DT, seven FT and seven UUT. Generally, a password with n character will yield n number of DT and n - 1 number for FT and UUT. So the timing vector length for combination of DT and FT is equal to $n \times (n-1)$ and the timing vector of combination of three features is equal to $n \times 2(n-1)$.

V. THE PROPOSED KEYSTROKE DYNAMICS AUTHENTICATION

The authentication via keystroke is based on the idea that each user posse's unique typing dynamics, this paper proposes a keystroke dynamics user authentication by exploiting back propagation neural network algorithm. The following subsections will explain the basic steps of this proposal.

A. Preprocessing:

Preprocessing step is done to obtain single template for each user that enable the proposed keystroke dynamics with neural network to distinguish between legitimate user and imposter one, with minimum rate of error.

First, compute the mean of timing vector for each user. Then, normalize the timing vector for each features using equation (1).

$$newIP = \frac{(oldIP - \min)}{(\max - \min)} \quad \ldots(1)$$

Where

$oldIP$: The mean of timing vector for each user.

$\min$: Minimum value in the time vector of each user

$\max$: Maximum value in the timing vector of each user.

B. Backpropagation Neural Network:

Classification is to find the best class that is closest to the classified pattern. Back propagation neural network algorithm is used to classify the features in classification phase. A backpropagtion neural network is a form of supervised learning for Multi-Layer Perceptron (MLP). The MLP network consists of several "layers" of neurons; typically an input layer, hidden layers, and an output layer. Input layers take the input and distribute it to the layers hidden. These hidden layers do all the necessary computation and output the results to the output layer, which forwards the data to the user as shown in figure (3).

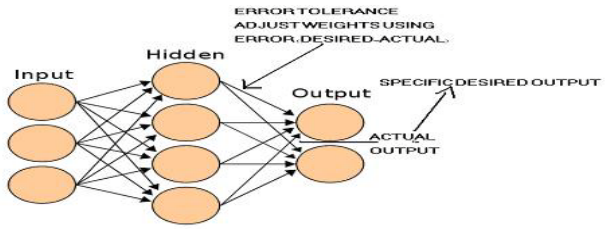

Figure 3: Structure of Backpropagation Network

Error data at the output layer is backpropagated to earlier ones, allowing incoming weights to these layers to be updated. The back propagation algorithm has been widely used as a learning algorithm in feed forward multilayer neural networks [18].

To train the neural network, a set of timing vectors from each user class was required. These timing vectors are collected for each user and stored in databases as mentioned in section 4. The timing vector are averaged and normalized to form a set of patterns that will be used to train the network. The number of patterns is 17. Training consists of taking a timing vector as an input, comparing the current output with the target output, and adjusting the weight values according to the backpropagation training algorithm. When the error of the training vector set is reduced to a pre-defined threshold which is the total summed squared error less than or equal to threshold, training is stopped. Figure 4 depicts the proposed keystroke dynamics with backpropagation algorithm.

VI. EXPERIMENTAL RESULTS

This section investigates the performance of the proposed keystroke dynamics against the most popular features DT and FT for satisfying user authentication based on keystroke dynamics.

Three experiments are performed independently on the two passwords (*computer* and *comp.84-rl*) using backpropagation to distinguish between authentic users and impostors with the parameters adjusted as follows:

a. Number of input layer nodes (*IN*) depends on the password length and the feature(s) that are used plus 1 node as bias as shown in table 1.

b. Number of hidden layer nodes (*HN*) is set to $2 * IN + 1$.
c. Number of output layer nodes (*ON*) is set to 1 since the output is either authentic users or impostors
d. Learning rate (η) is set to 0.1
e. Momentum (α) is set to 0.9

Table 1: Number of Nodes in Input Layer

Password	*Feature(s)*	*Input layer Nodes*
computer	DT	9
	FT	8
	UUT	8
	DT and FT	16
	DT, FT, and UUT	23
comp.84-rl	DT	11
	FT	10
	UUT	10
	DT and FT	20
	DT, FT, and UUT	29

In the first experiment, the proposed approach was tested on the same patterns that neural net was trained on.

The second experiment deals with test the proposed keystroke dynamic online. This experiment includes computing the selected feature(s) for each key he/she typed then concern preprocessing on the computed vector time and finally test the approach.

The testing involves when the user types the password of first trial and when the users type the password three trial.

The third experiment tests the proposed approach on the patterns that the net was not trained on.

To evaluate the performance of the proposed keystroke dynamics, three metrics are used including the false rejection rate (FRR) (i.e. the rate at which users are rejected when they could be authenticated), false acceptance rate (FAR) (i.e. the rate at which users are accepted when they should be rejected) and accuracy (i.e. the proportion of true results in the population). Table 2 and 3 illustrates the results of the proposed keystroke dynamics when each user types two passwords "*computer*" and "*comp.84-rl*".

Table 2: FRR, FAR and Accuracy of proposed Keystroke Dynamics for "*computer*" Password

Feature (s)	**Metric**	**Exp 1**	**Exp2**		**Exp3**	
			One Trail	**Three Trail**	**One Trail**	**Three Trail**
DT	FRR%	0	16	44	0	0
	FAR%	0	19	18	20	26
	Accuracy%	100	88	72	80	73
FT	FRR%	0	0	5	0	0
	FAR%	0	27	12	20	20
	Accuracy%	100	82	90	80	80
UUT	FRR%	0	0	0	0	0
	FAR%	0	18	18	20	33
	Accuracy%	100	88	88	80	86
Combine FT and DT	FRR%	0	16	22	0	0
	FAR%	0	9	30	0	0
	Accuracy%	100	88	90	100	93
Combine DT, FT and UUT	FRR%	0	0	5	0	0
	FAR%	0	9	3	0	6
	Accuracy%	100	94	96	100	93

Table 3: FRR, FAR and Accuracy of proposed Keystroke Dynamics for "*comp.84-rl*" Password

Feature(s)	*Metric*	*Exp1*	*Exp2*		*Exp3*	
			One Trail	*Three Trail*	*One Trail*	*Three Trail*
DT	FRR %	0	50	55	0	0
	FAR %	0	30	20	20	13
	Accuracy %	100	62	66	80	86
FT	FRR %	0	0	16	0	0
	FAR%	0	20	26	0	6
	Accuracy%	100	87	77	100	93
UUT	FRR%	0	0	16	0	0
	FAR%	0	10	20	0	86
	Accuracy%	100	93	81	100	93
Combine FT and DT	FRR%	0	0	16	0	0
	FAR%	0	10	20	0	6
	Accuracy%	100	93	81	100	93
Combine DT, FT and UUT	FRR%	0	0	16	0	0
	FAR%	0	10	16	0	6
	Accuracy%	100	93	83	100	93

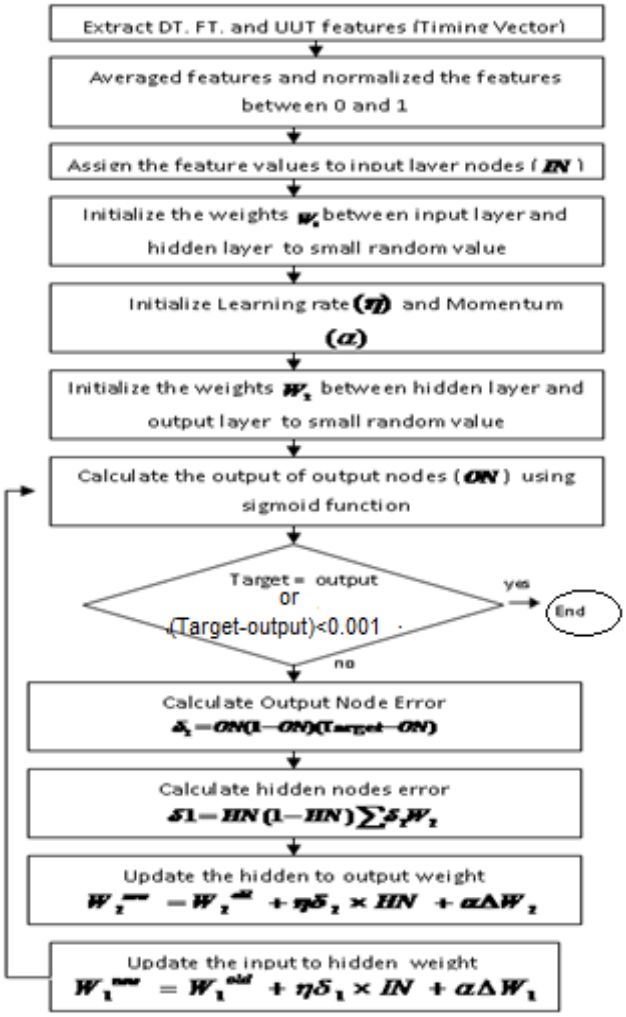

Figure 4: Keystroke Dynamics with Backpropagation Network

VII. CONCLUSIONS

The primary goal of the proposed keystroke dynamics is to prevent intruders from impersonating legitimate users (a low FAR is desired), while also ensuring that legitimate users are not rejected (a low FRR is also desired) and the accuracy of the system is high. This paper extracted the DT,

FT and UUT features from participate users. The backpropagation neural network was applied on different features namely DT, FT, UUT, combination of DT and FT, and combination of DT, FT and UUT to analysis the performance of these features.

The tested results demonstrate that the UUT gives better FAR, FRR and accuracy than DT and FT features. Also, UUT result is equal to the combination DT and FT features result because UUT features includes these features implicitly. On the other hand the result of combination of DT,FT and UUT features is best among the results. So, the testing results demonstrated that the backpropagation neural network was able to determine weights that distinguish the authentic users and impostors with low FAR, low FRR and high accuracy when using the features UUT and the combination of DT, FT, and UUT.

VIII. REFERENCES

[1]. A. Jain. and R. Jain , “Information Fusion in Biometrics", Pattern Recognition Letters, Vol. 24, No. 13, pp. 2115-2125, Elsevier, 2003.

[2]. U. Dieckmann and R.W. Frischholz "BioID: A Multimodal Biometric Identification Systems" IEEE Computer, Vol. 33, No. 2, pp. 64-68, 2000.

[3]. F. Monrose and A. D., Rubin "Keystroke Dynamics as a Biometric for Authentication" Future Generation Computing Systems (FGCS), Vol. 12, No. 12, pp. 351-359, 2000.

[4]. L. O’Gorman Comparing Passwords, Tokens, and Biometrics for User Authentication, Proceedings of the IEEE, Vol.91, No. 12, pp. 2019-2040, 2003.

[5]. S. Mandujano. and R. Soto “ Deterring password sharing: User Authentication via fuzzy c-means clustering applied to keystroke profiles, Proceedings of the ENC International Conference on Computer Science (ENC '04), pp. 181-187, ed. IEEE Computer Society, Colima, Mexico, September 2004.

[6]. L. C. F. Araújo, H. R. Luiz Sucupira Jr., Miguel G. Lizárrage, Lee L. Ling, and João B. T. Yabu-Uti, “User Authentication Through Typing Biometrics Features”, IEEE Transactions on Signal Processing, Vol. 53, No. 2, pp. 851-855, 2005.

[7]. G.A. Carpenter, M.A. Rubin and W.W. Streilein “ARTMAP-FD: Familiarity Discrimination Applied to Radar Target”, Proceeding of the International Conference on Neural Networks, pp. 1459–1464, 1997

[8]. D. Davis and W. Price, “Security for Computer Networks”, John Wiley & Sons, Inc., 1989.

[9]. R. Gaines, W. Lisowski, S. Press, N. Shapiro, “Authentication by keystroke timing: some preliminary results”, The Rand Report R-256-NSF. Rand Corporation, Santa Monica, 1980.

[10]. R. Joyce, G. Gupta, “Identity Authentication based On Keystroke Latencies”, Commun ACM Vol. 33, no. 2, pp. 168–176, 1990.

[11]. F. Monrose and A. D. Rubin “Keystroke Dynamics as a Biometric for Authentication”, Future Gener Compute Syst Vol. 16m No.4, pp. 351–359, 2000

[12]. S. Cho, C. Han, D. H. Hee and H. Il Kim, “Web based Keystroke Dynamics Identity Verification Using Neural Network”, Journal of organizational computing and electronic commerce, Vol. 10, No. 4, pp. 295-307, 2000.

[13]. P. Dowland, S. Furnell, and M. Papadaki, “Keystroke Analysis as a Method of Advanced User Authentication and Response”, Security in the Information Society: Visions and Perspectives, pp. 215, 2002

[14]. D. C. D’ Souza. “Typing Dynamics Biometric Authentication”, Bachelor engineering thesis, Faculty of Engineering and Physical Sciences, University of Queensland, Australia, 2002.

[15]. D. Shanmugapriya and G. Padmavathi “Virtual Key Force - A New Feature for Keystroke Dynamics”, International Journal of Engineering Science and technology, Vol. 13m No. 10, pp. 7738-7743, 2011.

[16]. P.S. Tee , T.S. Ong and, A. B. J. Teoh “A Multilayer Layer Fusion approach on Keystroke Dynamics”, Springer, Pattern Anal Applic, Vol. 14, pp. 23-36, 2011

[17]. H. Barghouthi “Keystroke Dynamics How Typing Characteristics Differ From One Application to Another”, Master of Science in Information Security, Gjøvik University College, Norway, 2007.

[18]. P. Mc Collum, “An Introduction to Back Propagation Neural Networks”, the Newsletter of the Seattle Robotics Society, 1997.