Volume : 4 | Issue : 11 | November 2015 • ISSN No 2277 - 8179

Research Paper

Enhanced Click dynamics to Ensure User Authentication and Detection of Cyber Attacks

Computer Science

KEYWORDS : Biometric, Click dynamics, Cyber attacks, Graphical password, Authentication, anytime algorithm

M.Uma — Ph.D Research Scholar, Department of Computer Science Avinashilingam Institute for Home Science and Higher Education for women Coimbatore.

Dr.G.Padmavathi — Professor and Head, Department of Computer Science Avinashilingam Institute for Home Science and Higher Education for women Coimbatore.

ABSTRACT

Recently biometric sought more attention in the field of research and development. Mouse dynamics otherwise known as click dynamics is a biometric system which plays a predominant role in the field of network security. In this paper, enhanced click dynamics is introduced to ensure user authentication. The unknown cyber attack detection process is developed using biometric system. In this research work "anytime algorithm" is integrated along with existing method to increase the accuracy in detecting the unauthorized user i.e., cyber attacks. To evaluate the accuracy in detecting the unknown cyber attacks by the proposed method the experiments were conducted with few performance metrics namely False Acceptance Rate, False Rejection Rate, Authentication time and Attack Detection rate. The experiments were conducted for 24 participants. The proposed method is developed using JAVA 1.7 as front end and mysql as back end.

1. Introduction

Click dynamics is used in the field of network security due to its unique nature of capturing the mouse operations of the individual user. The mouse operations can be captured in various forms like general movements, drag and drop, point and click but it does not require any specific hardware component [3]. By capturing the mouse movements, it will record the following details the type of action, the traveled distance, in pixels, the elapsed time in seconds, and the movement direction. All the actions captured of the mouse operations for every user login at the time of registration will be stored in a database for future reference. The mouse operation distances are measured using various algorithms like Levenshtein distance, Manhattan distance, dynamic time wrapping. The user re-authentication system [4] is also developed which is an application independent, continual, non-intrusive, fast and easily deployable. Apart from that, mouse-to-keystroke dynamics, interaction and Interaction Quotient (IQ) is also measured. Anytime algorithm is a similarity measurement algorithm used nowadays for more accuracy. While using anytime algorithm [9] mean squared differences and Mutual information are used to measure the similarity. To measure the distance these algorithms are used. Anytime algorithm gives more accuracy in measuring the distance than existing methods and also helps in reducing computational time.

2. Related Works

Some of the related works of the proposed method are discussed in this section

Bassam Sayed et.al (2013), introduces a new framework for static authentication for mouse dynamics. Vector quantization neural network classifier is used to capture the gestures in this research work. The evaluation of the proposed system is conducted for 39 users based on false acceptance ratio and false rejection ratio. Accuracy and validation is improved using the proposed system as this is the first method which provides the relatively accurate static authentication scheme.

Chao Shen et.al (2013) proposed a simple and efficient user authentication approach based on a fixed mouse-operation task. To get the accuracy and mouse behavior fine-grained characterization of every user traditional holistic feature and feature newly introduced in proposed system is also extracted. To increase the efficiency of the mouse feature space distance-measurement and eigen space-transformation techniques are used and for distance-based feature eigen space for the authentication one-class learning algorithm is applied. The dataset used is 5550 mouse-operation samples from 37 subjects. Authentication time is also analyzed based on false-acceptance rate and false-rejection rate is also calculated to ensure the efficiency of the proposed system.

Cheng-Jung Tsai et.al (2012), in their research work clicking and pressing the mouse button is captured based on the time. Down-Up, Down-Down, Up-Down, Up-Up and Down-Up2 are the five features analyzed and experimentation is done with 25 users. Imitate sample and non-imitate samples are used for to extract those five features for 25 users. The weight scores are calculated using three statistical methods. False Acceptance Rate, False Rejection Rate, Average False Rate and Equal Error Rate are the four performance metrics used to evaluate the proposed system. And concluded that the system proposed increasing the portability and the same system can be applied in electronic devices. To improve the security level this system can also be used as a standby identifiable factor of the keystroke-dynamics based authentication. Finally, they have declared that error rate of the system is high and given future scope as reducing the error rate.

Harini Jagadeesan and Michael S. Hsiao (2009) proposed a user re-authentication system which is application independent, continual, non-intrusive, fast and easily deployable based on user behavioral biometrics of keyboard and mouse operations. Mouse-to-keyboard interaction ratio and interaction quotient is proposed to extract the attributes of the user. The behavior of the user will be captured every time and it will be with the existing behavior which is stored already. The accuracy and application independency of the proposed is improved comparatively. The performance metrics sensitivity, specificity, false acceptance rate, false rejection rate and accuracy are used to evaluate the proposed system.

Ahmed Awad et.al (2007) introduced a new technique to capture the mouse behavioral characteristics of the user using artificial neural network. The first experiments are conducted for 22 participants, mouse movements have been collected randomly for 284 hours, 45 sessions for every user and 998 sessions for entire users. The second experiments were conducted for 7 participants. The proposed system is evaluated using the performance metrics such as receiver operating characteristic (ROC), confusion matrix, false acceptance rate and false rejection rate.

Adam Weiss et.al (2007) focused a detailed study on data collection, feature metrics, and classification. New software was developed for capturing the data capture, feature extraction, creation of user profile and classification of patterns. Leave-one out method of next Nearest Neighbor is used for implementation

and the success rate achieved is 92%. Experimentation is done with five users for 25 sample data to train and test the software developed.

Ross A.J. Everitt and Peter W. McOwan (2003) introduced a new concept for security using biometric authentication. Proposed is a novel which combines two different biometric to make sure that the system provides authenticity. The experimentation is conducted for 41 participants and the data collected is trained using back propagation algorithm and stored for future verification. False acceptance rate, false rejection rate, latency time and hold time are the performance metrics used to evaluate the system developed. Concluded that better results is achieved for FAR and FRR by the proposed system and suggested that the system can be applied to heterogeneous networks.

3. Proposed Methodology

The overview of the proposed methodology is discussed in detail in this section. The proposed methodology consists of four phases. The four phases of the proposed methodology are discussed below:

3.1. Steps Involved in Proposed Method

The four processing steps involved of the proposed method are discussed below

Step.1 Initiate user login using graphical password

The users are expected to execute the graphical password to login to access the database

Step.2 calculate distance measurements of capturing mouse operation

The mouse operation of every user is measured using integrated Manhattan distance with dynamic time wrapping.

Manhattan distance [31] (MD) calculates the sum of difference in every dimension of each vector. It is otherwise known as L_1 distance. If u= (x_1, x_2,... *Xian*) and v= (y_1, y_2,... y_n) are two vectors in n dimension. Then MD (u, v) will be calculated using the following equation.

$$MD(u,v) = |x_1 - y_1| + |x_2 - y_2| + \dots + |x_n - y_n| = \sum_{i=1}^{n} |X_i - Y_i|$$

Step.3 Measure operations similarity based on anytime algorithm

The similarity of the mouse operation of every user is compared by calculating mean square difference and measure information similarity of Anytime algorithm.

Anytime algorithm is used to measure similarity of the mouse operations, that can be achieved using function as D(φ), D(φ,p) as parameters and p as percentage of pixels. Mean square difference is measured using the following equation:

$$D_{MSD}(\varphi, p) = -\frac{1}{\lfloor pN \rfloor} \sum_{i=1}^{\lfloor pN \rfloor} \left(R(x_i) - T(W(x_i, \varphi))\right)^2$$

D_{MSD} --->Average of the negative mean squared differences in intensity between pixels

N ---> total number of pixels
p ---> percentage of pixels
R ---> Random Order

Step.4 Authenticate user and permit data access

After executing the anytime algorithm for user authentication, the authorized users will be permitted for data access from database.

3.2. Flow Diagram of the Proposed Method

The flow diagram of the proposed method is given in figure.1.

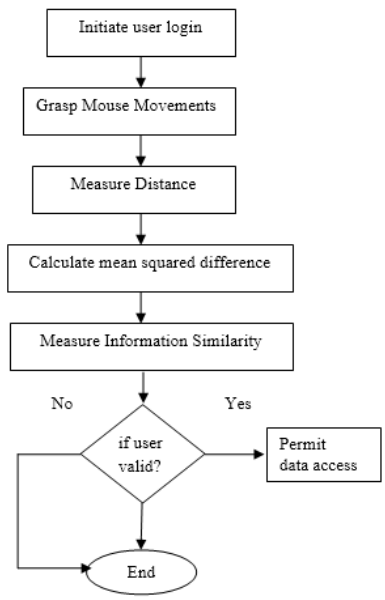

Figure.1 Flow diagram of the proposed method

Table.1 Proposed Algorithm

Initialize server for each user logging in execute graphical password capture mouse operation distance measurement measure similarity using anytime algorithm ensure user authentication if user authorized permit to access data end if end

4. Experiments and Results

The experimentation was conducted randomly for 24 participants.

4.1. Performance Metrics

The performance metrics used to evaluate the proposed method are:

False Acceptance Rate

The false acceptance rate is a fraction of negative entry or unauthorized user was incorrectly identified as positive entry or unauthorized user and it will be calculated using the following formula:

$$FAR = \frac{number\ of\ false\ rejections}{number\ of\ client\ accesses}$$

False Rejection Rate

The false rejection rate is a fraction of positive entry or unauthorized user that was correctly identified as negative entry or unauthorized user and it will be calculated using the following formula:

$$FRR = \frac{number\ of\ false\ acceptances}{number\ of\ client\ accesses}$$

5. Conclusion

The method proposed here enhances the click dynamics for user authentication. The concepts of graphical password, one class

classifier, Manhattan distance with dynamic time wrapping and anytime algorithm is used to increase the accuracy in user authentication. The accomplishment of the proposed method is evaluated in terms of performance metrics like false acceptance rate, false rejection rate, authentication time and attack detection rate to predict its efficiency in defending against cyber attacks.

Acknowledgement

This work is supported by Department of Science and Technology, Government of India under Women Scientist Scheme (WOS-A).

Table.2 Comparative Results of FAR, FRR and Authentication time

No. of Mouse Operations	False Acceptance Rate (%)		False Rejection Rate (%)		Authentication Time(seconds)	
	Existing Method	Proposed Method	Existing Method	Proposed Method	Existing Method	Proposed Method
25	5.7	4.6	4.3	3.6	9.0	8.7
50	6.7	5.8	4.7	3.8	8.9	8.6
75	7.7	6.4	5.7	4.6	8.9	8.4
100	8.2	6.5	6.7	5.2	8.7	8.1

Table.3 Attack Detection Ratio

Attack Types	Existing Method	Proposed Method	% of Improvement
Active Attacks	68%	71.5%	3.5%
Passive Attacks	71%	73%	2%

REFERENCE

[1]. Ross A.J. Everitt and Peter W. McOwan, "Java-Based Internet Biometric Authentication System" IEEE Transactions on pattern analysis and analysis and machine intelligence, Vol. 25, No. 9, 2003, pp. 1166 – 1172. [2]. Adam Weiss et al., "Mouse Movements Biometric Identification: A Feasibility Study" Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 4th, 2007, pp.C2.1-C2.8. [3]. Ahmed Awad E. Ahmed and Issa Traore, "A New Biometric Technology Based on Mouse Dynamics" IEEE Transactions on dependable and secure computing, Vol. 4, No.3, 2007, pp.165 – 179. [4]. Harini Jagadeesan and Michael S. Hsiao, "A Novel Approach to Design of User Re-Authentication Systems" IEEE, 2009, pp.1-6. [5]. Nan Zheng et al., "An Efficient User Verification System via Mouse Movements" CCS'11, ACM. [6]. Cheng-Jung Tsai et al., " An Approach for user authentication on non-keyboard devices using mouse click characteristics and statistical-based classification" International Journal of Innovative Computing, Information and Control ICIC International c 2012 ISSN 1349-4198 Volume 8, Number 11, 2012, pp.7875 – 7886. [7]. Bassam Sayed et al., "Biometric Authentication Using Mouse Gesture Dynamics" IEEE Systems Journal, 2013, pp.1 – 13. [8]. Chao Shen et al., "User Authentication through Mouse Dynamics" IEEE Transactions on Information forensics and security, Vol.8, No.1, 2013, pp. 16 – 30. [9]. Rupert Brooks et al., "Anytime similarity measures for faster alignment" Computer Vision and Image Understanding 110 (2008) 378–389, Elsevier, 2007, pp.378 – 389.