USER IDENTITY PREDICTION BY MOUSE GESTURE DYNAMICS THROUGH ANN

[1]ABHAY A. JADHAV, [2]J. V. MEGHA

[1,2]Department of Information Technology, SGGSIE & T, Nanded (MS), India
E-mail: jabhay4@gmail.com meghavjon@gmail.com

Abstract- we propose an approach for the user authorization system during login based on the Signature drawn from mouse movement. The scenario presented here is that the system can successfully and easily identify user behavior based on its behavioral model. Our implemented system uses Artificial Neural Network approach to train user behavior and verify user sign pattern for authentication of user to system. In this biometric scenario we have two parts, In First phase, the user signature is created as per the user's interaction with mouse while he is doing some activity such as, drawing any alphabet or his signature on canvas application and it gets stored in a database and used for verification purpose. In the second phase we have designed hierarchy, to generate a user signature for the verification purpose with signature stored in database. Our experimental results work on ten user signatures drawn for Authorization of user. Each user has to store five various signature patterns or sign variations and at a time of verification user has to draw his signature. If drawn signature matches with any of them, the user will be treated as Valid or Authorized User to system else fake user. We present the results of several experiments that we conducted to state our observations and suggest guidelines for evaluating future authentication approaches based on mouse Gesture dynamics by ANN.

Keywords- Mouse Dynamics, Behavioral Biometrics, Ann, Human Computer Interaction, User Re-Authentication, Anomaly Detection.

I. INTRODUCTION

The primary intension of developing such behavioral system is to provide more secure authentication system and along with reduce user effort to remembering password. The psychological studies shown that graphical things/password are easily captured and remembered as compare to textual things like password. So again for highly secure purpose we used to select lengthier and more complex password, so again here complexity increases for end user to remember such things. The main objective of developing such system is to make use of Behavioral or physiological characteristics of human being for the verification of Authorized user. In recent years of computer technology many Biometric system has been used for identification of human from figure printing devices to voice recognition and Eye retina recognition. Mainly for verification of user can be done by two techniques one is Physiological Biometric system in which psychological constraints can be used like figure prints, eye retina ,voice recognition which are unique in world. On the other hand behavioral biometric uses feature like user interaction activity with system using keyboard and mouse devices.

The mouse dynamics biometric is a behavioral biometric technology that extracts and analyzes the movement characteristics of the mouse input device when a computer user interacts with a graphical user interface for identification purposes. We present a new mouse dynamics analysis framework that uses mouse gesture dynamics for static authentication. We conduct an experimental evaluation of our framework with ten users.

II. RELATED WORK

Traditional Secure authentication systems uses periodically asking the user to authenticate via passwords, tokens and/or biometrics Or OTP i.e. One Time Password for re-authentication. However, repeated authentication is unvulnerable to the user, expensive, and often unreliable. Furthermore, it places the burden of the system's security on the end user and as such it is vulnerable to identity theft and authentication replay attacks.

Common behavioral biometric Authentication [8] Methods are mainly dependent on: (1) mouse movement, which depend on the user-mouse interaction with system (2) keystroke dynamics, which are derived from the keyboard events; and (3) software interactions, which are based on features extracted from the interaction of a user with a specific software system.

III. METHODS

In this section, we present an overview of our work and design of the system.

A. Proposed System Design

Proposed approach consists of two main phases, the Enrollment phase (Gesture creation module and Data acquisition and preparation module) and the Test phase (feature extraction and Classification) [7]. In the enrollment phase, we capture raw data and analyze it to extract the features which form the signature of the different users. Then we use these features to train a 2 neural network. The neural network will be used in the test phase to identify the user or verify his identity. Generally the enrollment phase consists of three steps. The first step is the raw mouse dynamics data capture. In this step the user draws the selected gestures and the raw mouse dynamics data get tagged and stored with his/her credentials. In the second stage the features get extracted from the raw mouse data and get combined to form the profile. In the third stage the profile is used to train a neural network. The neural network design is similar for all the users which allow us to store only the state of the neural network for each user as his/her reference signature. The challenge here lays in the signature and the neural network components. On one side, extracting features that form distinct signature for each user is a challenge. On the other side, the challenge would be how to design a neural network that when trained, would be capable of distinguishing between the users. Our approach to user authentication based on mouse gestures consists of presenting to the user one or several gestures drawn from an existing gesture set and asking him to replicate the gestures a certain number of times. The produced replications are then compared against templates produced by the user during the enrollment phase.

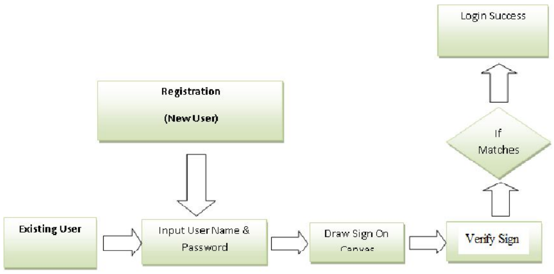


Figure 1: System Architecture

As shown in figure 1, first we take input from user by using mouse and create the mouse gesture for number of times (five times for this case)for system training and then perform data acquisition and then extract the feature for converting the impure gesture to pure gesture. Second is the classification module in which neural network performs the task to take the input, process the data and provide the result. The generated result by neural network is then stored in the relational database with specific user identity.

For the data collected, we design the gesture data acquisition and analysis framework. Our framework consists of mainly four modules [1]-[2]:

1) Gesture creation module;
2) Data acquisition and preparation module;
3) feature extraction module;
4) Classification module.

1) Gesture Creation

In the gesture creation module, we have provided canvas as a drawing application used to ask the user to freely draw a five set of signature. The main purpose of this module is to make the participant draw the gestures in his own way to replicate them later on. It is important to note here that the gestures are not bounded to any language. They neither need to be only alphabets or numbers nor are they required to have a meaning. They can be any drawing that can be produced in a single stroke.

2) Data Acquisition and Preparation

The initial two phases of data acquisition and preparation involves loading the gestures created by the user using some canvas control gesture creation module and presenting them to the user to replicate. The data acquisition module records the user interaction while drawing the gesture. It preprocesses the collected raw data from the computer mouse in such a way that some noise patterns are ignored or dropped. This is required since the data produced by the pointing devices is usually jagged and irregular as user may have drawn sign in its own handwriting style. After preprocessing the raw data, two types of normalizations are applied to the input data. The first is center normalization and the second is size normalization. The Center normalization which will calculate the input node values of network by converting image to Matrix vector and it shifts the gesture to the center of the drawing area as implemented in the gesture creation module. The Size normalization used to normalize the size so that the final size of the gesture is equal to the size of the template gesture in order to compare the two gestures.

3) Feature Extraction

Feature extraction deals with extracting the information of the boundary of a handwritten signature [9]. This is done by scanning the sign image until the boundary pixel is found. The searching follows according to the clockwise direction. For any pixel p of canvas, the set of all foreground pixels connected to it will be scanned, (so called connected component containing p).Once a black pixel of sign is detected, it checks for another new black pixel and so on. The tracing follows the boundary automatically.

When the first pixel is found, the program will be assigned the coordinates of that position i.e. x and y coordinate of region to indicate that this is an origin of the boundary of drawn sign which will be assigned for neural network node. The new found pixel will be assigned as a new reference point and starts the eight-neighbor searching. In this way, the coordinates of the initial point are varied according to the position. As the tracer moves along the boundary of the image, the corresponding coordinates will be stored in an array for the computation of Fourier Descriptors. During this feature extraction phase or boundary tracing process, the program will always check the condition whether the first coordinates of the boundary are equal to the last coordinates. Once it is obtained; means the whole 3 boundary has been traced and boundary tracing process is completed

4) Classification Module

For the classification of the gestures, we first tried the principal component analysis technique on sample data, yielding poor performance. We also explored the use of the feed-forward back propagation multi layer perceptions network. Though the training step using this type of neural network is effective but it is somewhat time consuming.

Modular Neural Network Design:

A monolithic neural network is considered as an unstructured black box that does not have the flexibility and modularity to solve a subset of certain problems [10]. Neural network is proven to be one of its major performance limiting characteristics. The modular neural network design addresses this limitation by introducing more flexibility and structure in the neural network architecture.

IV. EXPERIMENTAL RESULTS

In this Scenario, We state the experimental Results of the proposed Work.

A. Things/Tools Used

All the participants used the same Dell PCs/laptop to enroll in our Testing Application. The hardware configuration of the PCs/laptop was an Intel Core 2 Duo processor clocked at 2 GHz, with 2GB of physical memory, running Microsoft Windows 7 configured with a resolution 1440×900 native screen resolution. All the participants used a Microsoft Explorer optical mouse to replicate the different gestures; even the same mouse pad was used during the experiment. The sampling rate was 125 Hz, which is the Microsoft Windows XP/Vista/7 OS default sampling rate for USB based mouse devices. The software involved in our experiments was already deployed on the laptop. The application, written in C# consists of a gesture creation tool and an enrollment tool. The gesture creation is used to create the gesture templates or sign and store them with the user credentials in a relational database. The Verification methods load the templates or sign from the database and allow the participant to enroll against them. The replications resulting from the enrollment are stored in the replications database.

B. Users:

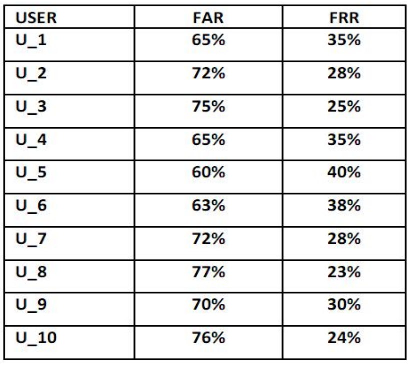
The main Aim of our experiment was to be able to recognize individuals identity to system based on their mouse signature. Ideally, the system should be able to recognize, with a high degree of accuracy, the behavior of each user while replicating a specific sign. To achieve such a goal, 10 people were involved in our testing scenario. We have chosen the participants from different backgrounds, like those who are using computer rarely or occasionally' and those who are professions user like university students and staffs, students engineers. Again we have some more users whose signatures were not in database .i.e. who are illegal or unauthorized user to system.

C. Method and Data

For the experimental results, all the participants used the same laptop to draw the same set of prechoosen gestures signature. The gestures replications along with the participating user credentials were stored in a user database as user id and name. There was only one requirement that was to draw such gestures in one stroke. The all participating user in the experiment was asked to draw sign in its own style like its own signature or any alphabetic character or numeric or non-alphabetic character. User can draw any sign or stroke unlike any English alphabets. The drawn sign gestures were included combinations of angles or curves, lines. Each of the ten impostors was asked to forge the (five) gesture templates of at least five legitimate users selected randomly from the above 10 legal users. Care was taken to ensure that each legal user would be targeted by exactly five different impostors. An impostor was shown a sample gesture for a given legitimate user and asked to forge it by providing five replicas.

D. Evaluation Process

We applied tested evaluation process 10 times for each of the five gestures sign involved in our testing experiment, and computed global FRR i.e. false rejection rate and FAR i.e. false acceptance rate. Each time one session was used as the test user identity exactly once and the remaining five drawing sessions were used to build the user profile or register user to system. The obtained results were averaged and depicted using receiver operating characteristic (ROC) curves in Figure 2. As we can see from the results, all the gestures are close to each other in performance. Some of the best operating point.



USER	FAR	FRR
U_1	65%	35%
U_2	72%	28%
U_3	75%	25%
U_4	65%	35%
U_5	60%	40%
U_6	63%	38%
U_7	72%	28%
U_8	77%	23%
U_9	70%	30%
U_10	76%	24%

Figure 2: User Wise FAR & FRR of 10 Users 4

CONCLUSION

From the proposed module implemented with the help of Artificial Neural Network, we conclude that, the behavioral biometric characteristics of human being can be used more efficiently for authentication of user to computer system as compared to password. To further enhance the security, one more security layer can be added to existing security mechanism. The most important advantage is offered by making the illegal access to the system more complicated, as the anonymous user has not only to steal the credentials of authorized user but also he has to mimic the user's behavior, and it's highly impossible.

REFERENCES

[1] Bassam Sayed, Issa Traor´e, Isaac Woungang, and Mohammad S. Obaidat, "Biometric Authentication Using MouseGesture Dynamics",IEEE systems journal, vol. 7, no. 2, June 2013.

[2] Chao Shen, Zhongmin Cai, Xiaohong Guan, Youtian Du, and Roy A. Maxion, "User Authentication Through Mouse Dynamics". IEEE transactions on information forensics and securityvol.8,NO. 1, Jan 2013.

[3] N. Zheng, A. Paloski, and H. Wang, "An efficient user verification system via mouse movements" in Proc. 18th ACM Conf. Comp. Commun. Sec., pp. 139–150, 2011.

[4] M. Obaidat and B. Sadoun, "Verification of comp. users using keystrokedynamics," IEEE Trans. Syst., Man, Cybern., vol. 27, no. 2, pp. 261–269, Apr. 1997.

[5] H. Gamboa and A. Fred, "A behavioral biometric system based on human-comp. inter," in Proc. Conf. Biometric Tech. Human Identification, vol. 5404, pp. 381–392, 2004.

[6] A. A. E. Ahmed and I. Traor´e, "A new biometric tech. based on mouse dynamics," IEEE Trans. Dependable Secure Comput., vol. 4, no. 3, pp. 165–179, Jul.–Sep. 2007.

[7] A. Nazar, I. Traor´e, and A. Ahmed, "Inverse biometrics for mouse dynamics," Int. J. Artif. Intell. Pattern Recognition, vol. 22, no. 3, pp. 461–495, May 2008.

[8] A. E. Ahmed and I. Traor´e, "A new biometric tech. based on mouse dynamics," IEEE Trans. Dependable Secure Comput., vol. 4, no. 3, pp. 165–179, Jul.–Sep. 2007.

[9] A. F. Syukri, E. Okamoto, and M. Mambo, "A user identification system using signature written with mouse," in Proc. 3rd Australasian Conf. Inform. Sec. Privacy, pp. 403–414, 1998.

[10] F. Azam, "Biologically inspired modular neural networks," Ph.D. dissertation,Virginia Polytechnic Instit. State Univ., Blacksburg, 2000.

[11] Z. Jorgensen, T. Yu, "On mouse dynamics as a behavioral biometric for authentication, in: Proceedings of the Sixth ACM Symposium on Information, Computer, and Communications Security" (AsiaCCS), March 2011.

[12] Saurabh Singh, Dr K V Arya, "Mouse Interaction based Authentication System by Classifying the Distance Traveled by the Mouse" International Journal of Computer Applications (0975 – 8887) Volume 17– No.1, March 2011.

[13] K. Revett, H. Jahankhani, S. de Magalhaes, and H. M. D. Santos, "A survey of user authentication based on mouse dynamics," in Proc. ICGeS, CCIS'12, pp. 210–219,2008.

[14] M. Pusara and C. E. Brodley, "User reauthentication via mouse movements," in Proc. ACM Workshop Visualization Data Mining Comp. Sec. (VizSEC/DMSEC), pp. 1–8, 2004.

[15] Clint Feher, Yuval Elovici, Robert Moskovitch, Lior Rokach, Alon Schclar, "User identity verification via mouse dynamics", Information Sciences 201 (2012) 19–36.

[16] S. Ross, "Peirce's criterion for the elimination of suspect experimental data," J. Eng. Tech., vol. 20, no. 2, 2003.

[17] T. Kohonen, Self-Organizing Maps (Springer Series in Information Sciences, vol. 30), 3rd ed. Berlin, Germany: Springer, 2001.

[18] M. Gamassi, M. Lazzaroni, M. Misino, V. Piuri, D. Sana, and F. Scotti, "Accuracy and performance of biometric systems", in Proc. Instrum. Meas. Tech. Conf., 2004, pp. 510–515.

[19] S. Bengio and J. Mariethoz, "A statistical significance test for person authentication," in Proc. Odyssey: Speaker Language Recognition Workshop, 2004.

[20] R. Biddle, S. Chiasson, and P. C. V. Oorschot, "Graphical passwords: Learning from the first twelve years," School Comp. Sci., Carleton Univ., Ottawa, ON, Canada, Tech. Rep. TR-11-01, Jan. 2011.

★★★