Authenticating Login session using Mouse biometric with AES Encryption

Shruthi G., Shilpa S.G., Geeta S. Hukkerimath
Department of Computer Science, VTU, Bangalore
shruthigmysore@gmail.com, shilpasg.06@gmail.com,blh_geeta@gmail.com

ABSTRACT- The mouse biometric is a behavioural 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. In this paper, we present a new method for Authenticating login session Using Mouse Biometrics. Mouse dynamics are defined by the characteristics which are acquired by analyzing the inputs a user performs by a pointing device. These characteristics are then combined to form the *factors* which are stored in the user profile. Factors are encrypted using AES Algorithm. During Login session, comparing the current input stream with the previously stored user profile, mouse dynamics can detect anomalies in the user's behavior and stop intrusions while they are happening.The paper proposes mouse based authentication, the application of behavioural biometrics for authentication as a safeguard against unauthorized users gaining access to a computer.

Keywords: biometric authentication, computer security, identity verification, mouse dynamics.

I.INTRODUCTION

User authentication is the process verifying claimed identity. The authentication is accomplished by matching some short-form indicator of identity, such as a shared secret that has been prearranged during enrollment or registration for authorized users. This is done for the purpose of performing trusted communications between parties for computing applications.

Conventionally, user authentication is categorized into three classes:

- Knowledge - based,
- Object or Token - based,
- Biometric - based.

The knowledge-based authentication is based on something one knows and is characterized by secrecy. The examples of knowledge-based authenticators are commonly known passwords and PIN codes. Passwords are the simplest form of user authentication. The object-based authentication relies on something one has and is characterized by possession. Traditional keys to the doors can be assigned to the object based category.

A new category of biometrics that is gaining in popularity is referred to in the literature as behaviometrics (for behavioral biometrics), where analysis focuses on studying the user's behavior while he interacts with a computing system for the purpose of identification [4]–[6]. One interesting example of behaviometrics is mouse dynamics biometrics [5]–[8]. The following Figure 1. Shows the different classification of biometric methods.

Mouse dynamics biometric recognition involves extracting the behavioral features related to the mouse movements and analyzing them to extract a signature, which is unique for every individual, and as such can be used to discriminate different individuals. The main strength of mouse dynamics biometric technology is in its ability to continuously monitor the legitimate and illegitimate users based on their sessional usage of a computer system. This is referred to as continuous authentication. Continuous authentication, or identity confirmation based on mouse dynamics, is very useful for continuous monitoring applications such as intrusion detection.

However, unlike traditional biometric systems, mouse dynamics biometric technology may face some challenges when applied to static authentication, which consists of checking the user's identity at login time. The key challenge is the data capture process, which requires more time to collect sufficient amount of mouse movements for accurate user identity verification [9] than can reasonably be tolerated, or afforded, in a realistic login process.

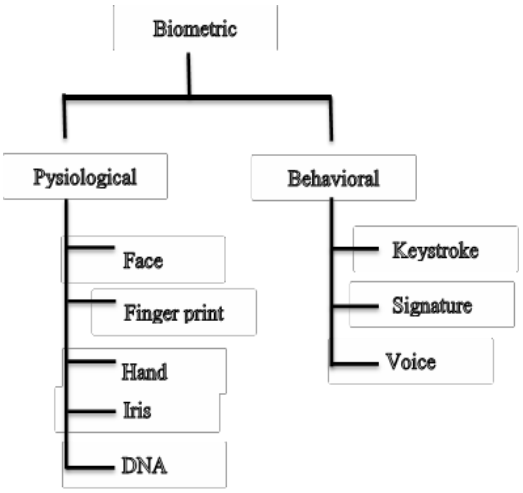

Fig 1. Classification of biometric

We tackle this challenge by proposing we present a new Design and Implementation for authenticating login session Using Mouse Biometrics that allows performing the authentication in a short time and as such may be used for static authentication (at login time). We use mouse gestures to achieve our goal. A mouse gesture results from the combination of computer mouse movements and clicks in a way that the software recognizes as a specific command. In our work, during the enrolment phase the user draws a set of gestures several times on a computer monitor using a mouse along with user details and password. We extract features from the captured gesture, analyse them, store it in database corresponding to particular user profile . In the verification phase, the user will be asked to replicate the gestures drawn by her in the enrolment phase along with password to test against her stored profile .Here we using both password and mouse dynamics for authentication. Even if the imposter get the password of a particular legitimate user he cannot login without knowing gesture .Again gesture depends on someone‘s behaviour .The system architecture is shown in fig 2. These features are usually unique for a person and cannot be stolen. In Authentication by mouse movements use of any additional hardware isn‘t required and no one can steal the mouse movements of a person. This is how Biometrics technologies are gaining popularity due to the reason that when used in conjunction with traditional methods of authentication they provide an extra level of security.

The remainder of this paper is organized as follows. In Section II, we summarize and discuss related work. In Section III, we give an overview of mouse biometrics and present the design of our detection system. In Section IV,we present our experimental evaluation process and results. Section V, we give conclusions and summarize our future work.

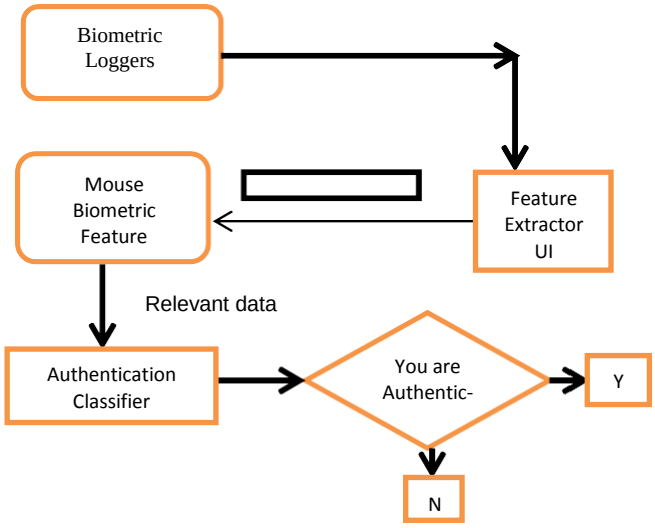

Fig 2 System architecture

II RELATED WORK

Behavioural biometrics first gained popularity with keystrokdynamics with mouse, work on password hardening in 1999 [7]. Later on, Ahmed and Traore [1] proposed an approach combining keystroke dynamics with mouse dynamics. Mouse dynamics for re-authentication have been previously studied as a standalone biometric by Pusara and Brodley [8]. Gamboa et al. [3] performed similar research by conducting an experiment to capture user interaction based on the mouse while playing a memory game. Fifty volunteers participated in the experiment. sequential forward selection technique based on the greedy algorithm was used to select the best single feature and then add one feature at a time to the feature vector. Gamboa et al. [3] showed that the equal error rate (EER) progressively tends to zero as more strokes are recorded. This means that the more interaction data the system records, the more accurate the system should be. But, as we commented earlier, it might be difficult to use such a method for static authentication at login time since the authors reported that the memory game took from 10–15 min to complete on average. so far only three papers in the literature, published by Syukri et al. [6] and Revett et al. [5], Bassam Sayed et.al[9] have targeted the use of mouse dynamics for static authentication. A system that may potentially be used for static authentication, proposed by Syukri et al. [5], utilizes signatures drawn using a mouse for user identification. The extracted features were analysed using geometric average means. The authors conducted two

experiments involving 21 users, in the first of which a static database was used, and in the second a dynamically updated database was used.

Revett et al. [6] proposed a new mouse dynamic analysis approach for static authentication, named mouse lock, which exploits the analogy of a safe, in which the numbers are replaced with graphic thumbnail images. To login, using a mouse, the user is required to click in a password that consists of five images. Bassam Sayed et.al[9] proposed a new mouse dynamics analysis framework that uses mouse gesture dynamics for static authentication. The captured gestures are analysed using a learning vector quantization neural network classifier. Here they combined gestures to get good result.

The main issues with the above works on mouse dynamic are that the minimum amount of data required to achieve meaningful user identification is impossible to obtain within the time constraint of a typical login process. As such, the proposed approaches may be used for user re authentication (after login) or for continuous authentication, but they may not be suitable for static authentication (at login time). And also in Bassam Sayed et.al[9] they have combined gestures to get good result again time consuming .

III. MOUSE GESTURE DETECTION AND ANALYSIS

In this section, we give an overview of mouse gestures and present the design of our gesture detection system.

A. Gesture Creation Module

The gesture creation module is a simple drawing application used to ask the participant to freely draw the gestures. It is used during both enrolment and login phase.

The main purpose of this module is to make the participant draw the gestures in his own way during enrolment and replicate them during login phase. Figure 3.shows example of drawing gesture having 8 data points gestures. It is important to note here that the gestures are not tied to any language and they do not necessarily have a meaning.

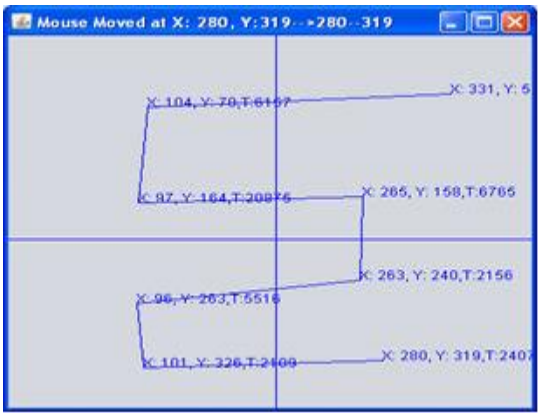

Fig. 3 shows example of drawing gesture having 8 data points gestures .

B. Data Acquisition Module

The data acquisition component loads the gestures, created initially by the user using the gesture creation module. It is used during both enrolment and login phase .The main use is to extract features from the gesture. The data acquisition module records the user interaction while drawing the gesture. The raw data collected from the drawing area consist of the horizontal coordinate (x-axis), vertical coordinate (y-axis), and records the elapsed time t in milliseconds starting from the origin of the gesture. Given gesture can be defined as a sequence of data points and each data point can be represented by a triple <x,y,l > consisting of the X-coordinate, Y-coordinate, and Number of points(clicks) l .The elapsed time in milliseconds starting from the origin of the gesture. During Enrolment phase, for each user, the program creates a directory that will contain the user replications for the different gestures. Each gesture must be replicated a specific number of times (e.g., 10 times). The user has to wait 3 s between consecutive replications. The idea behind this waiting time is to prevent the user from drawing the gesture too fast. The module asks the user to release the mouse between each successful replication during the wait time. We assumed that the wait time and mouse release will force the users to maintain their normal behaviour each time they replicate the gesture.

C. User Registration Module (Enrolment Module)

Registration Module records the user personal information along with gesture, here user supposed to draw gesture n times, the gestures are drawn using gesture creation module. 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 tied to any language and they do not necessarily have a meaning.

They can be any drawing that can be produced in a uni-stroke. Also, this module serves as a practice step for the participants to get familiar with the idea of drawing mouse gestures.

After gestures creation, using the data acquisition the features are extracted from the each gesture replica and stored in Feature data base along with the personal information and user name. All information stored in database are encrypted by using AES Encryption. The below Figure 4 shows extraction of features set from all replicas during enrolment phase.

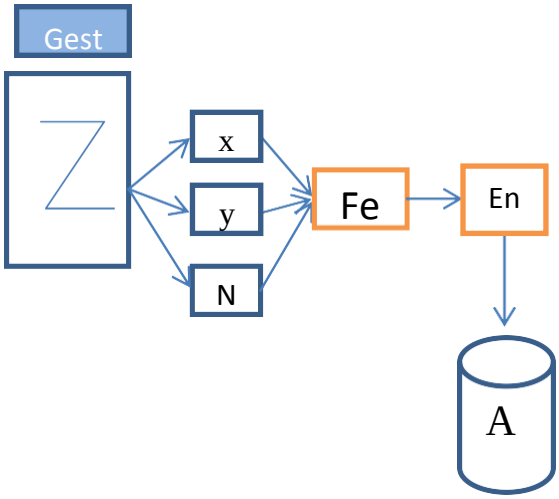

Fig .4 shows the extraction of feature set during login phase.

D. Login Module

In this module, user who is claiming an identity will be asked to replicate gesture he already sketched in the enrolment phase along with user name. Here also by using data acquisition module the features are extracted from the gesture and stored in the authentication data base. The information of the login user is encrypted by using AES Encryption. The idea behind Encryption for login information is just to provide extra security.

E. Authentication Classifier Module

This is the main module which tests the authentication of user. This module decides, given user is legitimate or imposter. For a given user, it exports features gesture replication recorded during the enrolment phase from the feature database and decodes it.

Again it exports the feature of gesture recorded during login phase from authentication database and decodes it. The comparison of gesture in terms of feature takes place .The feature recoded during login phase is compared with each feature recorded during enrolment phase. Before comparison we have to consider few things. Generally humans can not draw the same gesture with the same exact detail twice under the same conditions. This will result in some variability in the replicas produced by the same individual for the same gesture. We have to minimize the effect of variation .This minimization is accomplished by using range normalization. For each point recorded coordinates given the relaxation of +20 and -20 units .The idea behind this is user can‘t draw the gesture exactly with same position for all points, instead we given the space for each point .user can draw the gesture within that space for ach point.

AS specified each feature recorded during login phase is compared with features of all replicas during enrolment phase. First it compares with number of points (clicks) ,then it compares with x,y coordinates considering range relaxation. While comparing coordinates, it takes first point coordinate form login gesture and compares with same point coordinates of all gesture replicas. At least, in any one of the gesture in replicas the coordinate should match. The comparison is repeated for all the points in gesture .The decision depend on the total matching count of all the points in gesture. The matching count should be greater than or equal to Number of points in the gesture .

IV EXPERIMENTAL EVALUATION

We present, in this section, the experimental evaluation of the proposed framework. We start by describing the experimental conditions and procedures, and then present, analyse, and discuss the obtained results.

The main objective of our experiment was to be able to recognize individuals based on their mouse gestures. Ideally, the system should be able to recognize, with a high degree of accuracy, the behaviour of each user while replicating a specific gesture were involved in our experiment. So in our approach, we used the gestures having the combinations of angles, lines, curves. The main reasoning for this choice was, the more angles and curves the gesture has, the more it will require muscle tension and concentration from the users. This, in turn, imposes the intrinsic behaviour of the human motor control while drawing such gestures.

To show the efficiency of the proposed system ,two users user1 and user2 are asked to draw the same gesture the two replicas produced by user1 is

compared with replica produced by user2 as shown in below Figure 7.

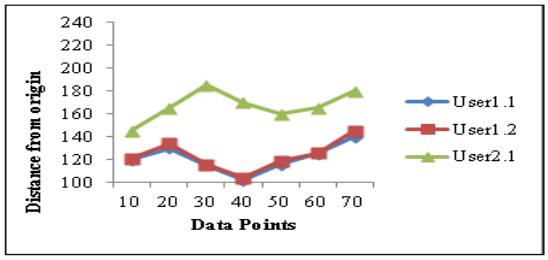

Fig..5 Comparing distance from original features of two replicas belonging to User 1 and one replica belonging to User 2 for the same gesture.

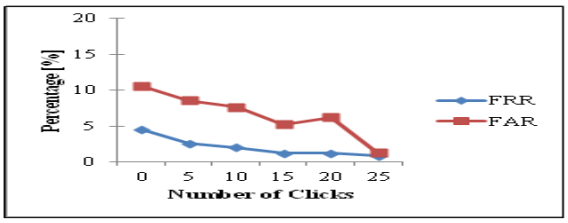

Fig .6 FAR and FRR of a Gesture

Even though both the user drawn the same gesture but replica produced by both user are different the more angles and curves the gesture has, the more it will require muscle tension and concentration from the users also as show in figure 8 False Acceptance Rate(FAR) and False Rejection Rate decreases for gesture having More Clicks. This, in turn, imposes the intrinsic behaviour of the human motor control while drawing such gesture.

V CONCLUSION AND FUTURE STUDY

In this paper, new Design and Implementation for authenticating login session Using Mouse Biometrics. Mouse dynamics are defined by the characteristics which are acquired by analysing the inputs a user performs by a pointing device. These characteristics are then combined to form the factors which are stored in the user profile. During Login session, comparing the current input stream with the previously stored user profile, mouse dynamics can detect anomalies in the user's behaviour and stop intrusions while they are happening. One of challenge faced by most of security system are protection against security attacks. Like many other biometric technologies, mouse dynamics can be the target of replay attacks. In our proposed system Such threats are mitigated by strengthening the protection of the biometric information using Encryption techniques.In future work, we intend to enhance the accuracy of our proposed scheme by revisiting various aspects. Since our proposed system is entirely software based, integration in a complex system environment .During comparison we give range Normalization (-20 and +20) units which may reduce by Using advanced software would allow addressing the interoperability challenges inherent in complex system environments. Mouse dynamics can also be the target of automated attacks, also referred to as generative attacks, where high quality forgeries can be generated automatically using a small set of genuine samples. We plan, in our future work, to strengthen our system by investigating the impact of generative attacks against it.

REFERENCES

[1] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti, ―Privacy-aware biometrics: design and implementation of a multimodal verification system,‖ in Proc. Annu. Comp. Sec. Apps. Conf., 2008, pp. 130–138.

[2] D. Lopresti, F. Monrose., and L. Ballard, ―Biometric authentication revisited: Understanding the impact of wolves in sheep‘s clothing,‖ in Proc. 15th USENIX Sec. Symp., 2006.

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

[5] 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, 2008, pp. 210–219.

[6] 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, 1998, pp. 403–414.

[7] C. Varenhorst. (2004). Passdoodles: A Lightweight Authentication Method [Online]. Available: http://people.csail.mit.edu/emax/ papers/varenhorst.pdf

[8] 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.

[9] Bassam Sayed Bassam Sayed, Issa Traor´e, Isaac Woungang, and Mohammad S. Obaidat, *Fellow, IEEE* l Biometric Authentication Using Mouse Gesture Dynamics.