International Journal of Emerging Engineering Research and Technology
Volume 3, Issue 3, March 2015, PP 1-5
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Direct Indirect Human Computer Interaction Based Biometrics

Sachin Takmare, Miss. Pranjali Bhosale[1], Miss. Pooja Ganghi[2], Miss. Priyanka Shinde[3], Miss. Rutuja Waskar[4],

Assistant Professor, Department of Computer Science and Engineering, BVCOEK, Shivaji University, Kolhapur
[1, 2, 3, 4]Department of Computer Science and Engineering, BVCOEK, Shivaji University, Kolhapur

ABSTRACT

Data security is much more important issue now a day; because hacker's are much more intelligent. Identity theft is a crime in which hackers does the unauthorized activity. Hackers can steal the identity of user by using credential things such as password, username. User verification technique provide security to the user in terms if their username and password or also by continuously validating the identity of logged-on user and Continuous verification done through users behavioral and physiological characteristics. We introduce one method that does continuous verification of user according to the interaction with mouse. Their search contribution is in three parts. First, user verification is based on result of individual mouse action and the methods which aggregate mouse action. Second we propose hierarchy of mouse action in which features are extracted. Last, we take decision about to continue the log in or log out the logged user.

Keywords: Authentication, verification, biometric system, input devices

INTRODUCTION

Currently in all systems user verification has done through the credential lead like the username password. It's fixed to every user to use the password and username for their authentication. So hackers can use so many techniques to hack the password of particular user. Some of the techniques are phishing attacks, key logger and so on. Also sometimes a user's computer remains unlocked at that time hackers can install the key logger in users computer or sends some links to user computer, Ex. Greetings or some images etc. if user clicks on that link key logger automatically installs on that computer, it records every key stroke including passwords, usernames of user also the screen shots after 5-5 minutes. Finally, they can send that hacked data to hackers without knowing to user.

The drawback of normal identification methods that only based on credentials lead means username, password, personal identification number (PIN). To the introduction of user authentication and verification techniques that are based on behavioral and physiological biometrics which are assumed to be unique to each other and hard to steal. Once Authentication is performed during the login while verification is performed continuously throughout the session. Identity Verification can be achieved by using one of the two techniques, First by Behavioral biometricsystem and second by Physiological Biometric system.

The behavioral biometric feature includes characteristics of interaction of user and input devices such as mouse and keyboard. And physiological biometric use the human feature that is unique to individuals. For Examples: fingerprints, iris patterns, face, blinking patterns, lip movement, gait/stride, voice/speech, signature/handwriting etc. physiological biometric system uses the various devices for verification of user but this devices are expensive. Also it is not possible to carry those devices always with us. Although fingerprint verification is becoming widespread in laptops, but it is still not popular enough and it cannot be used in web applications. Furthermore, fingerprints can be copied. Behavioral biometrics, on the other hand, do not require special designated hardware since they use common devices such as the mouse and keyboard

Also in case of temporal aspect of behavioral biometric system it may be different depending on the time of particular day in which it can be captured. This makes very harder to intercepts and also harder to produce result at a given accuracy. Furthermore, several challenges, which still need to be

**Address for correspondence*

priyajshinde17@gmail.com

overcome in order to make this approach fully operational. Consequently, behavioral biometrics was ignored to a certain extent for user verification in the past. So we propose a novel user continuous verification technique based on behavioral biometrics of the user's mouse activity when he is performing his daily computer activity.

Also if the signature of user is not getting matched with existing signature then as per its matching percentage different puzzles and questions are displayed. This puzzle has different levels with some time limit. If user cannot solve within time then pc automatically shut down.sSimilarly, it also captures the pc handling way of user and store it and then it is used for further verification.

Thus, systems utilizing biometric user verification require a hacker who wants to infiltrate the system not only to steal the credentials of the user but also to mimic the user's behavioral and/or physiological biometrics making identity thefts much harder. We are focused to implement a behavioral biometric system because it does not require dedicated hardware's as in physiological it requires. Obviously cost to implement this system is not more than physiological system.

RELEVANT LITERATURE

Most common behavioral biometric verification techniques are based on:

(a) Mouse dynamics, which are derived from the user-mouse interaction and are the focus of this paper.

(b) Key stroke dynamics, which are derived from the key board activity; and

(c) Software interaction, which rely on features extracted from the interaction of a user with a specific software tool (somewhat our system falls in this category also).

Behavioral methods can also be characterized according to the learning approach that they employ. Explicit learning methods monitor user activity while performing a predefined task such as playing a memory game, this method falls in this category. Implicit learning techniques, on the other hand, monitor the user during general day-to-day computer activity rather than during the performance of a specific task–Explicit and implicit methods are also referred to as static and dynamic methods, [1], respectively. Implicit learning is considered more challenging due to high inconsistency owed to the variety of the performed tasks, mood changes and other influential factors. Nevertheless, it is the best way to learn unique user behavior characteristics such as frequently performed actions. Since biometric-based verification systems are a special case of classifiers, their performance is evaluating during similar measurements.

In the following, we list current available user verification systems along with their performance evaluation

MOUSE BASED METHOD

Authentication methods identify users at login based on a predetermined sequence of mouse operation that the user needs to follows. During training, the sequence is repeated several times by every user. Features are extracted from each sequence and are used to characterize the user. During authentication, the user is required to follow the same sequence. Continuous verification, on the other hand, repeatedly reconfirms the user's identity throughout the entire session using all mouse activity rather than a predetermined sequence. One of the popular methods is Histogram Based user identification. In this paper we propose a continuous verification method and it is based on mouse movement.

A biometric-based user verification system is essentially a pattern recognition system that acquires biometric data from an individual, extracts a feature set to establish a unique user signature and constructs a verification model to classify (Similarity Match) between user signature.

OTHER BEHAVIORAL BIOMETRICS SYSTEM

Alternative approaches to user verification utilize keyboard dynamics and software interaction characteristics. Keyboard dynamics features include, for example, latency between consecutive keystrokes, flight time, dwell time – all based on the key down/press/up events. Keyboard-based methods are divided into methods that analyze the user behavior during an initial login attempt and methods that continuously verify the user throughout the session. The former typically construct classification models according to feature vectors that are extracted while the users type a predefined text (such as a password) while the latter extract feature vectors from free text that the users type .

PROPOSED MODEL

We propose such verification method that verifies a user based on each individual mouse action. This method requires the aggregation of dozens of mouse coordinates and its activities before accurate verification can be performed. Verification of each individual mouse action increases the accuracy while reducing the time that is needed to verify the identity of the user since the fewer actions are required to achieve a specific accuracy level, as compared to the histogram- based approach which is explained in the general block diagram of the proposed system is shown in fig. 1

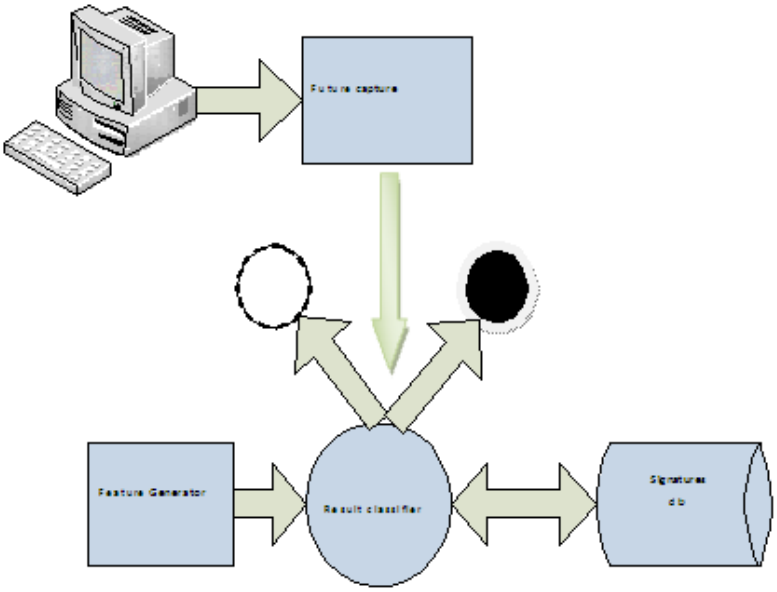

Fig1. *General Block diagram of proposed system*

In Above fig:

White Signal- Authorized User.

Black Signal- Unauthorized User/Hackers.

Fig.1 depicts the architecture of a behavioral biometric user verification system. Such systems include the following components:

Event capture: it captures events generated from input devices and then it is used for further interaction (e.g. Keyboard mouse). Events can be mouse move (MM), left down (LD), left up (LU), right down (RD), right up (RU), silence (S) etc.

Features generator: it generate high level features which are extracted from the appropriate events and the signature will be constructed which characterizes the behavioral biometrics of the user, The features may include Mouse Move Sequence (MMS), Left Click(LC),Right Click(RC) etc.

Result classifier: it used for classification of signature. During verification it can classify new samples acquired from the user. Any classifiers can be used depend on its availability and its knowledge.

Signature database: A database issued to store the signature of user. If multiple users exist for system, then up on the entry of username, signature of that user will retrieve for verification process.

In the database, the signature will consist number of mouse moves; number of left clicks, number of right clicks number of silence along with time intervals and aggregation of mouse Co-ordinates.

Same type of signature will be created forever session.

As shown in fig.2, if the matching percentage of signature is less than 100 then different puzzle are displayed. These puzzles are displayed according to user signature matching percentage criteria.

This puzzle has three different levels if the percentage of user is more than 90 then simple puzzle and questions are displayed. If percentage of user more than 80 then in that case medium level of hard puzzle and questions are displayed. If the percentage of user more than 60 then hard levels puzzles are displayed and hard questions also.

If the percentage is below 60 then at this movement pc automatically shut down.

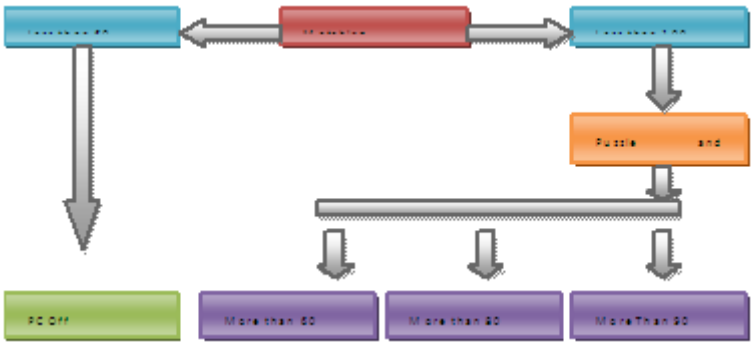

Fig2. *Signature Matching Criteria*

As Shown in Fig 2, if the signature is less than 100 then different levels of puzzles and questions displayed. These puzzles are displayed with some time limit. Because fix user solve puzzles within time limit, but unauthorized user take some time to solve these puzzles. Also similarly for questions authorized user answers all questions quickly, but unauthorized user takes some time.

Time limits are also given according to different levels. Simple level of puzzles and questions has 60 seconds. Medium level of puzzles and questions has 40 seconds. And finally, hard level of puzzles and questions has 30 seconds.

When authorized user logs on to computer its behavior gets captured and it stored on database. Every user has some fix pattern to handle pc, so these fix patterns get captured and then it is used for further verification.

If user log on to the computer then at that time system check whether user behavior pattern matching with existing stored pattern, if yes then continues else pc shut down.

In fig.3, user behavior classifications are displayed.

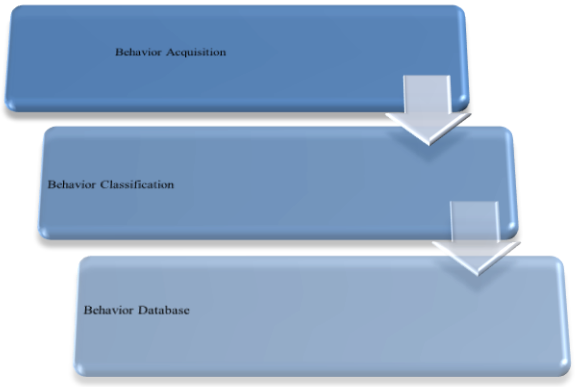

Fig3. *Behavior Classifier*

Behavior Acquisition: It captures user behavior of handling pc. Different users has different ways of handling pc. When user log on to pc it captures pc handling behavior of particular user.

Behavior Classification: it classifies behavior of user. During continues verification it classifies another behavior generated by user.

Behavior Database: Database used to store the behavior of users. It store different user's behavior of users this behavior further used for verification purpose.

CONCLUSION

Hence we can conclude that, User Verification System using mouse signature will give one more additional security layer in addition to the normal security layer. Obviously to infiltrate the computer system will be harder using this method because the hacker has not only to steal the credentials of authorized user but also he has to mimic the user's behavior, and it's normally impossible.

REFERENCES

A.A.E. Ahmed, I. Traore, "A new biometric technology based on mouse dynamics, IEEE Transactions on dependable and Secure Computing" 4 (3) (2007) 165–179.

P. Bours, C.J. Fullu, "A login system using mouse dynamics, in: Fifth International Conference on intelligent information hiding and multimedia sinal processing", 2009, pp. 1072–1077.

Lívia C. F. Araújo, Luiz H. R. Sucupira Jr., Miguel G. Lizárraga, Lee L. Ling, andJoão B. T. Yabu-Uti, "User authentication through Typing Biometrics Features,IEEETransactions on Signal Processing", Vol. 53, No. 2, February 2005

Clint Feher, Yuval Elovici, Robert Moskovitch, LiorRokach, AlonSchclar, "User identity verification via Mouse dynamics", Information Sciences 201 (2014) 19-36

R.V. Yampolskiy, V. Govindaraju, Behavioral biometrics: a survey and classification, International Journal of Biometrics 1 (1) (2008) 81–113.

H. Gamboa, A. Fred, An identity authentication system based on human computer interaction behavior, in: 3rd international Workshop on Pattern.

H. Gamboa, A. Fred, Behavioral biometric system based on human computer interaction, Proceedings of SPIE 5404 (2004) 381-392.

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

S. Deshpande, S. Chikkerur, V. Govindaraju, Accent classification in speech, Fourth IEEE Workshop on Automatic Identification Advanced Technologies, 17–18 October, 2005, pp. 139–143.

O. Hamdy, I. Traore, Homogeneous physio-behavioral visual and mouse-based biometric, ACM Transactions on Computer–Human Interaction 18(3) (2011) 1–30 (Article 12)

A. Jain, F. Griess, S. Connell, Online signature verification, Pattern Recognition 35 (12) (2002) 2963–2972.

K. Revett, H. Jahankhani, S.T. de Magalhes, H.M.D. Santos, A survey of user authentication based on mouse dynamics , in: Proceedings of 4th International Conference on Global E-Security, Communications in computer and information science , vol. 12, London, UK, June 2008, pp.210-219.