IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 4 (Jul. - Aug. 2013), PP 33-36
www.iosrjournals.org

User Identity Verification Using Mouse Signature

B J Gorad, D.V Kodavade
[1](*Computer Science & Engineering, Sharad Institute of Technology College of Engineering, Ichalkaranji, Maharashtra, India)*
(Computer Science & Engineering, D.K.T.E Society's Textile & Engineering Institute, Ichalkaranji, Maharashtra, India)

Abstract : *Stealing Identity of the user is a crime in which hackers does the unauthorized activity under the stolen identity by using credentials such as passwords, usernames etc. User verification system provides security layer in addition to username and password by continuously validating the identity of the logged-on user based on their behavioral and physiological characteristics. We introduced a novel method that continuously verifies the user according to characteristics of their interaction with the mouse. The research contribution is in two parts. First, user signature is created according to the user's interaction with mouse while he is doing some predefined 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 part design hierarchy, to generate a user signature for the current session is discussed. The paper also discusses a decision making system to take decision about to continue the log in or log out from the system based on matching of his current signature and previously created signature. The system developed gives better verification accuracy by reducing the response time of the system.*

*Index Terms— LC **– Left click,** RC **– Right Click,** DC- **Double Click,** MM- **Mouse Move etc***

Submitted date 22 June 2013 **Accepted Date: 27 June 2013**

I. INTRODUCTION

Currently most computer Systems and online websites, identifies users by means of user names and passwords/ PINS. But normally hackers can easily steal the password with the help of so many techniques. 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 user's computer or by sending some links to that computer, Ex. Greetings or some images etc. if user clicks on that link key logger installs on that computer, it records every keystroke including passwords, usernames, screen shots after 5-5 minutes. Also they can send that hacked data to hackers without knowing to user.

The drawback of normal identification methods that only based on credentials lead 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. Authentication is performed once during the login while verification is performed continuously throughout the session. Identity Verification can be achieved by using one of the two techniques, either by Behavioral biometric system or 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.

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

II. RELEVANT LITERATURE

Most common behavioral biometric verification techniques are based on: (a) **mouse dynamics[1][2][3][4]**, which are derived from the user-mouse interaction and are the focus of this paper; (b) **keystroke dynamics[6][7][8]**, which are derived from the keyboard 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 evaluated using similar measurements.

III. PROPOSED MODEL

We propose a novel verification method which 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 [1].

The general block diagram of the proposed system is shown in fig. 1

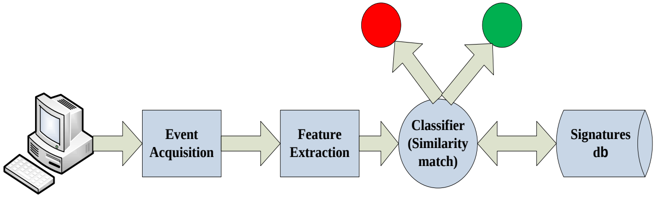

Fig.1 General Block diagram of proposed system

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 the user signature's.

In above diagram no 1 -
Green Signal- Authorized user
Red Signal – Unauthorized user/ Hacker

3.1. General architecture

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

-Event acquisition – captures the events generated by the various input devices used for the interaction (e.g. Keyboard, mouse) via their drivers, Events can be mouse move (MM), left down (LD), left up (LU), right down (RD), right up (RU), silence (S) etc.

-Feature extraction – High level features [1]can be extracted from that 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.

-Classifier – Consists of an inducer (e.g. Support Vector Machines, ANN, Random Forest Classifier etc.) that is used to build the user verification model to classify the signatures. During verification, the induced model is used to classify new samples acquired from the user. Any classifiers can be used depend on its availability and its knowledge [1].

-Signature database – A database is used to store the signature of user. If multiple users exist for system, then upon the entry of a username, signature of that user will retrieve for verification process [1].

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 for every session.

Data Flow Diagrams for proposed model:

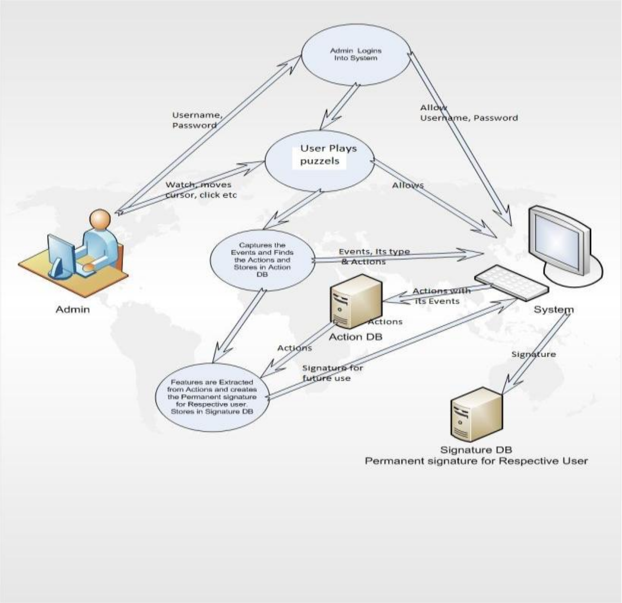
Admin Logins Into System
Username, Password
Allow Username, Password
User Plays puzzels
Watch, moves cursor, click etc
Allows
Captures the Events and Finds the Actions and Stores in Action DB
Events, Its type & Actions
Actions with Its Events
Admin
System
Actions
Action DB
Actions
Signature
Signature for future use
Features are Extracted from Actions and creates the Permanent signature for Respective user. Stores in Signature DB
Signature DB
Permanent signature for Respective User

Fig. 2 User Registration Process(Admin)

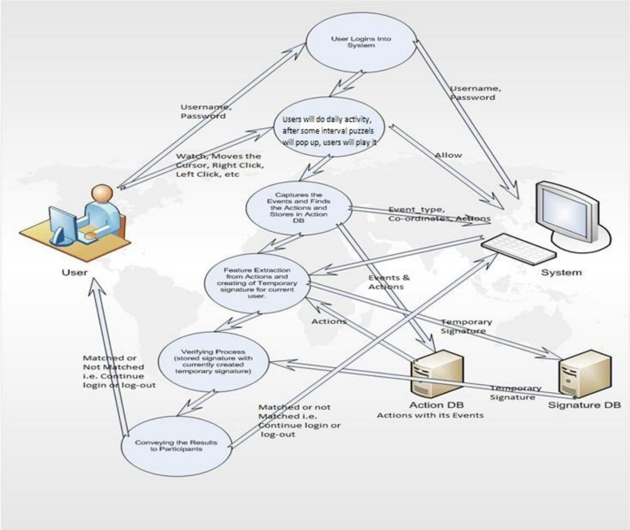
User Logins Into System
Username, Password
Username, Password
Users will do daily activity, after some interval puzzels will pop up, users will play it
Watch, Moves the Cursor, Right Click, Left Click, etc
Allow
Captures the Events and Finds the Actions and Stores in Action DB
Event_type, Co-ordinates, Actions
User
Feature Extraction from Actions and creating of Temporary signature for current user.
Events & Actions
System
Actions
Temporary Signature
Matched or Not Matched i.e. Continue login or log-out
Verifying Process (stored signature with currently created temporary signature)
Temporary Signature
Action DB
Actions with its Events
Signature DB
Matched or not Matched i.e. Continue login or log-out
Conveying the Results to Participants

Fig. 3 User Verification Process (Admin/ User)

In this proposed system, users have to register first. Registration is done at the start by opening the canvas and drawing an alphabet or sequence of alphabets, after saving it, it will be the signature for that respective user. Next time when user will start the system, obviously first he has to login into the system using credentials such as username and password. As usually users will enter his username and password which is already assigned to him, and he will do his daily activity. During his daily activity after some interval canvas will pop up, and it will ask to draw his signature and he has to draw the signature, so a temporary signature is created for that session. Finally the verification model compares the current sessions signature and initially created signature. In all the times both signature will not match exactly but we can give some range (matching is in between 80% to 100% etc), the user will be authenticated else the system will log out.

We are recommending Random forest Classifier to build the verification model. During the pop up of canvas all other features of computer system will be locked, the user should not be able to do anything than drawing his signature.

If the user is drawing wrong signature continuously three times then the system will identify the logged in user is a hacker, he has stolen the credentials and the entire system will lock so he will not use the entire system at all.

The login continuation of computer system or discontinuation will totally depend on percentage of matching of signatures.

Final Decision = {Yes /No}

IV. 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.

V. FUTURE SCOPE

In future, this system can be implemented for an implicit behavioral biometric system. Also some extension can be done to this system to give better security, as after logout of the system due to more than three times not matching of signature, random password can be generated and it will send to the registered user's mobile number, so hackers can't login again by using old username and password.

References

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

[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]. Zach Jorgensen and Ting Yu, On Mouse Dynamics as a Behavioral Biometric for Authentication. ACM 978-1-4503-0564-8/March 2011.

[4]. 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

[5]. 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

[6]. 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, IEEE Transactions on Signal Processing", Vol. 53, No. 2, February 2005

[7]. S. Cho, C. Han, D.H. Han, H.I. Kim, "Web-based keystroke dynamics identity verification using neural network, Journal of Organizational Computing and Electronic Commerce" 10 (4) (2000) 295–307.

[8]. L. Ballard, D. Lopresti, F. Monrose, "Evaluating the security of handwriting biometrics, in: The 10th International Workshop on Frontiers in Handwriting Recognition" (IWFHR '06), La Baule, France, 2006.

[9]. H. Gamboa, A. Fred, "An identity authentication system based on human computer interaction behavior, in: 3rd International Workshop on Pattern Recognition on Information Systems", 2003, pp. 46–55.