IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IV (Jan. 2014), PP 98-101
www.iosrjournals.org

Holistic and Procedural Features for Authenticating Users

D.Lakshmipriya, Prof.J.R.Balakrishnan
M.E (Computer Science And Engineering) Anand Institute of Higher technology
Professor and Director (Computer Science Department) Anand Institute of Higher technology

Abstract: *Security systems help to protect machines or sensitive data from unauthorized users. The need for better and cheap security systems is growing with the growth in technologies and hacking skills of the people. Various techniques are available that can provide some level of security. The problem of unintended side-effects of inconsistent experimental condition and environmental variables by restricting user's mouse operation to a tightly-controlled environment has been addressed with the solution of mouse operations as dynamics. Mouse dynamics measures and assesses a user's mouse-behavior characteristic for use as a biometric. For Each mouse operation task both holistic and procedural features are extracted. This type of authentication is very simple and efficient for the users. Then a Nearest Neighbor algorithm is employed for extracting the feature and anytime algorithm for the accuracy and speed. This approach achieves to improve the number of users with a false acceptance rate of 8.75% and a false rejection rate of 7.70%.This approach could lead to a performance boost both in authentication accuracy and authentication time.*

I. Introduction

As data are moved from traditional localized computing environments to the new cloud computing paradigm, the need for better authentication has become more pressing. These things should provide public confidence in the security of the current information infrastructure; the inadequacy of password-based authentication mechanism is becoming a major concern for the entire information society of various solutions to this problem, a particularly promising technique is mouse dynamics.

Hence it is suitable for the current internet environment. When users try to log into a computer system, mouse dynamic only requires her to provide the login name and to perform certain sequence of mouse operations. Mouse dynamic based user authentication, usually only the data from the legitimate user are readily available, since the user would choose her specific sequence of mouse operation and would not share it with others.

A mouse dynamic based user authentication performs authentication in a short time while maintaining high accuracy. The several properties are (a) it is easy to comprehend and implement, (b) it requires no specialized hardware (c) it requires only about 12 seconds o mouse behavior data to provide good, steady performance. Mouse dynamic is a behavioral biometric for analyzing behavior data from pointing devices, provides user authentication in an accessible and convenient manner. The mouse dynamic is mostly used for intrusion detection, which analyzes mouse-behavior characteristics at particular moments.

Information security (IS)

The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security.

Confidentiality

Confidentiality refers to preventing disclosure of information to unauthorized individuals or systems. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Confidentiality is necessary for maintaining the privacy of the people whose personal information is held in the system.

Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. Information security systems typically provide message integrity in addition to data confidentiality.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

Authenticity

In information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be.

Feature extraction (FE)

When the input data to an algorithm is too large to be processed and it is suspected to be notoriously redundant then the input data will be transformed into a reduced representation set of features also named features vector. Transforming the input data into the set of features is called feature extraction.

Holistic Feature (HF)

The features characterize the overall properties of mouse behaviors during interactions, such as single-click and double-click statistics.

II. Related Work

S.Hashia[5]Two authentication schemes are used one for initial login of users and another for passively monitoring a computer for suspicious usage patterns. This computed the error rate which is the point where false acceptance rate = false rejection rate. Z. Jorgensen[6]The data collected from 15 participants.The system displayed an on –screen virtual keyboard and required user to use the mouse to enter a paired user name and pin number. Here the repository of approximately 5 hours of interaction. This separation assumes that they can have access to approximately 4 minutes of user interaction while filling the sign in which were consider reasonable The system does not modify the normal login process of a conventional on-line security system. Hugo C. Shen, Z. M. Cai[8]They developed a system that captures the user interaction via a pointing device, and uses this behavioral information to verify the identity of an individual. Using statistical pattern recognition techniques, they developed a sequential classifier that processes user interaction, according to which the user identity is considered genuine if a predefined accuracy level is achieved.

Each of the above described methodologies have their own pros and cons. The following are the few essential pitfalls that will be addressed by the proposed methodology

- Password based authentication mechanism
- Many biometric authentication system
- The mouse movement are kept as static
- The log-in system takes unnecessarily long time to enter in to the account

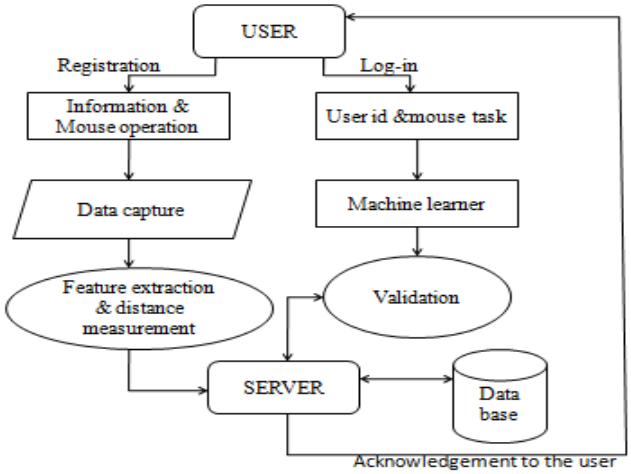
III. Proposed Work

The mouse operation task has been created and to capture and interpret mouse-behavior data which will be the dynamic. The holistic and procedural features to characterize mouse behavior and to map the raw features into distance-based features by using various distance metrics. The training phase applies nearest neighbor algorithm on the distance-based feature vectors to compute the predominant feature components. The mouse feature has been extracted using the anytime algorithm. Since the mouse movements are made as dynamic the user can give their own mouse operation and the log-in system. This is achieved because of any-time algorithm.

3.1 OVERALL PROCESS DESIGN

The overall design explains that the user need to perform operation as registering and log-in, while registering they have to give the user information and mouse movement as password and after that the system will extract the feature and measure the distance and store the data in DB

Then the user want to Log-in means they have to give the user name and mouse operation as password then they have the machine leaner to validate the mouse task with speed and accuracy and the server will produce the result.



3.2ALGORITHM DESIGN

3.2.1 Nearest neighbor algorithm

Step 1: The user will register with the information and mouse operation
Step 2: The system will extract the feature with the arbitrary vertex as current vertex
Step 3: Distance measured through shortest edge connecting the current vertex and an unvisited vertex V
Step 4: Set current vertex to V mark as visited, the following operations take place
for $r = 1, \ldots, R$ do
$Y0$: a point drawn randomly from a uniform distribution
over D.
for $t = 1, \ldots, T$ do
$Yt = \text{argmin}Y \in N(Yt-1,E,G)\ P(Y,Q)$.
$S = S$
$N(Yt-1,E, G)$.
$U = U$
$\{P(Y,Q) : Y \in N(Yt-1,E, G)\}$.
end for
end for
Sort U, pick the first K elements, and return the corresponding
elements in S.
Step 5: If all the vertices are visited then terminate
Step 6: Store the information in server database

3.2.2 Any-Time algorithm

Step 1: Log-in id and the password as mouse operation will be given
Step 2: The similarity measure will be taken for the mouse operation.
Step 3: The each similarity measure D(O),as a function D(O,P)
O-Parameters
P-Pixeles
The parameters and the pixels will be compared for the similarity with the information stored in the database.
Step 4:The speed of the operation will be increased with the measure of the dynamic performance profile
Step 5:The dynamic performance profile is done with the
$\varepsilon = \|\nabla \text{true}D - \nabla \text{measured}D\|$
$\|\nabla \text{true}D\|$
Step 6: The validation is done with the performance and speed which evaluated as above
Step 7:If the user is valid means the access permission will be given otherwise not.

IV. Implementation

4.1 USER REGISTRATION

In this module the implementation of the user interface by which the user can interact with the Application. To access the Application, the user want to the register their details with Application provided by the Server. They have to provide their information like Name, Password, Date Of birth, Mobile Number and etc.

This information will store in the database of the Application Server. The User is allowed to the access the application only by their provided Interface.

The Server will monitor the entire User's information in their database and verify if required. Also the Server will store the entire User's information in their database. Also the Server has to establish the connection to communicate with the Users. The Server will update the each User's activities in its database. The Server will authenticate each user before they access the Application. So that the Server will prevent the Unauthorized User from accessing the Application.

4.2 LEARNING PHASE

The second module has been designed with the the major things they are

- Mouse-behavior capture
- Feature construction
- Distance measurement

The mouse-behavior is nothing but it wills serves to create a mouse-operation task and to capture and interpret mouse-behavior data. Then next is the feature extraction the nearest neighbor algorithm has been designed to be implement here only the to extract the features correctly and accurately the working of the algorithm will be start in this stage only then distance measurement of the operation is done with the feature-distance vectors and to mitigate the effects of these issues.

In the calculation of the distance measurement Dynamic Time Warping (DTW) distance to compute the distance vector of the procedural feature. The procedural feature of two data samples are not likely to consist of the exactly two same numbers of points. The DTW can be applied to measure the distance between the procedural features of the two samples without deforming either or both of the two sequence in order to get an equal number of points.

4.3 VERIFICATION PHASE

The third module has been designed for the user validation; the Server will verify the User when they are login into their account. The Server will verify the signature provided by the User while login with the Signature provided by the User when they provided during the Training Phase. If the signature is not matched, then the Server will not allow the User to access their account

V. Conclusion

This method will bring the high level of security and the account is created for the user with the personal details and mouse operation as a password and the feature is extracted and the distance is measured and the log-in system will be in high speed and it will produce the secured authentication in the real world.

References

[1]. A.A.E.Ahmed and I.TraroeCompur (2007), 'A new biometric technology based on mouse dynamics,' IEEE Trans. Depend. Secure.

[2]. P.Bours and C.J.Fullu (2009),'A login system using mouse dynamics,' Proc.5th Int. Conf. Intelligent Information Hiding and Mulimedia Signal Processing.

[3]. R. Brooks, T. Arbel, and D. Precup(2008), 'Anytime similarity measures forfaster alignment,' J. Comput. Vis. Image Understand.

[4]. R. Everitt and P. W. McOwa(2003),'Java-based internet biometric authentication system,'IEEE Trans. Pattern Anal. Mach. Intell.

[5]. S. Hashia, C. Pollett, and M. Stamp(2005), 'On using mouse movements as a biometric,' Proc. Int. Conf. Computer Science and Its Applications, Singapore.

[6]. Z. Jorgensen and T. Yu(2011), 'On mouse dynamics as a behavioral biometric for authentication,' Proc. 6th ACM Symp. Information, Computer and Communication Security, Hong Kong.

[7]. M. Pusara and C. E. Brodley(2004), 'User re-authentication via mouse movements,' Proc. 2004 ACM Workshop on Visualization and Data Mining for Computer Security, Washington.

[8]. C. Shen, Z. M. Cai, X. H. Guan, H. L. Sha, and J. Z. Du(2009), 'Feature analysis of mouse dynamics in identity authentication and monitoring,' Proc. IEEE Int. Conf. Communication (ICC), Dresden, Germany.

[9]. K. Ueno, X. Xi, E. Keogh, and D.-J. Lee(2006),'Anytime classification using the nearest neighbor algorithm with applications to stream mining,' Proc. IEEE 6th Int. Conf. Data Mining (ICDM), Hong Kong.

[10]. N. Zheng, A. Paloski, and H. M. Wang(2011),'An efficient user verification system via mouse movements,' Proc. ACM Conf. Computer and Communications Security, Chicago, IL.