A Behavioral Biometric Approach Based on Standardized Resolution in Mouse Dynamics

S.Benson Edwin Raj **A. Thomson santhosh**

Assistant Professor, Karunya University PG Scholar, Karunya University

Summary
Mouse dynamics is a form of behavioral biometrics that can be used for several security applications.Similar to keystroke dynamics, mouse dynamics does not required special hardware device for data collection. We target biometric identification problem by focusing on extracting the behavioral features related to the user and using this features for computer security. Standardized mouse dynamics biometrics involves a signature that is based on selected mouse movement characteristics under different screen resolution and mouse pointer speed settings. Several experiments are conducted under different settings to form the mouse dynamics signature of the user. Earlier approaches failed to give better results when performed under different screen resolution and mouse pointer speed. Our approach standardizes the user signature irrespective of the setting making it more useful for security application.

Key words:
Biometrics, network security, mouse dynamics.

1. Introduction

Recent years Biometrics plays a vital role in security application. There are different types of Biometric Technologies used for different security purposes. First, Biometrics is a collection of factors it describes the behavioral or physiological characteristics of human to verify identity Physiological biometrics are finger scan, iris scan, retina scan, hand scan, and facial scan use measurements from the human body.

Behavioral biometrics such as signature or keystroke dynamics use measurements based on human actions. Behavioral biometric systems have experienced less success when compared to physiological systems mainly because of their strong variability over time[6]. A common drawback of most biometric systems is the need for special hardware device[6][7][10].Keystroke verification contains two approaches static or dynamic. In this static approach, the system checks the user one time that is at authentication time. Whereas in the dynamic approach, the system checks the user continuously throughout the session. Since static verification occurs only once, they can try to attack the session later. But, dynamic verification, which is done throughout the session, prevents such an attack. We introduce a biometric system based on mouse dynamics. Similar to keystroke dynamics, mouse dynamics does not need any special hardware device for collecting the data. When compared to the existing keystroke dynamics, mouse dynamics are collected passively and verified throughout the session. This mouse dynamics biometrics may be suitable for intrusion detection, in addition to access control. In addition to keystroke dynamics, which is used in computer security, work on mouse dynamics has been limited mainly to user-interface design Improvement.

Mouse Dynamics is defined as the set of actions received from the mouse movement data for a user while interacting with a specific graphical user interface. The characteristics of mouse dynamics can be described by a set of factors generated by analyzing the recorded mouse actions. These are the factors represent which is said to be a mouse dynamics signature for a specific user, which can be used in verifying the identity of the user. To identify the user we have to collect the mouse action data such as Mouse-Move, Drag and Drop, Point and Click action.

We are collecting the data by using Standardized Mouse Dynamic Detector Architecture. It contains three units. They are Data interception Unit, Behavior analysis Unit, Behavior Standardization and Behavior comparison Unit.

Mouse dynamics is a new behavioral biometric recently introduced. The idea behind this biometric is to monitor all mouse actions generated as a result of user interaction with a graphical user interface, and then process the data obtained from these actions in order to analyze the behavior of the user. Mouse actions include general mouse movement, drag and drop, point and click, and silence (i.e. no movement). these factors are used to construct what is called a Mouse Dynamics Signature or MDS, a unique set of values characterizing the user's behavior over the monitoring period. Some of the factors consist of calculating the average speed against the traveled distance, or calculating the average speed against the movement direction. In up to seven factors that exhibit strong stability and uniqueness capability are reported

Manuscript received April 5, 2009
Manuscript revised April 20, 2009

2. Related Works

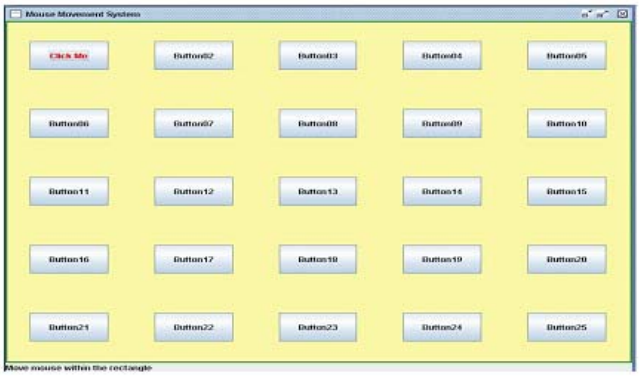
2.1 Mouse Movement Biometric Identification

Another area of biometric Identification is mouse movement[3]. There is a lot of threats in system like unauthorized access, Theft of proprietary information, and Insider Net abuse are within the top five financial losses. These percentage of reporting is increased that they did not know if unauthorized access had occurred. So for the Security purpose they are trying to find the way addition to the password and have multiple forms of identification. Biometrics research has been around for a long time, but has not seen wide implementation in the security field, Work with multi-modal biometrics has shown the values of authentication using personal characteristics. There are two types of biometrics physiological and behavioral. Fingerprints are considered physiological and keystrokes are behavioral. Both have the added advantage that users cannot easily leave them behind. Keystroke biometrics work on the basis of multiple feature extraction being used to create a profile of an individual. This profile is used to identify or authenticate the user.

Mouse movement has the two advantages of low cost and low invasiveness. It was possible to re-authenticate users through their mouse movements. Normally the authentication is processed in the beginning of a session, however once that session is started; its very difficult to find who is working with the system. One method of re-authentication is by monitoring the mouse movements of the user and comparing it to a profiled. We will also be looking into obtaining profiles of users and making comparisons through the nearest neighbor method. A software system is created to gather mouse movement data; compute measurements for a set of features and use them to identify an unknown user from a known set of users. Metrics such as mouse moving speed, number of clicks, duration of clicks and variation in mouse movements are under consideration to create a profile of each user.

2.2 Refinement of a Mouse Movement Biometric System

In this Refinement of a Mouse Movement Biometric System Multiple form of application is used. i.e not only User name and password, It include user characteristic i.e addition to that it include Gender, Age, Mouse type, File name etc..The Computer and Internet usage continues to grow worldwide, so does the need to ensure that the users of computing systems are protected from unauthorized users accessing their systems. The best form of defense is a multiple layered defense. This can be done by implementing high security standards that are use different way to secure from unauthorized access that together can help protect vulnerable systems.



MM System Application

Most systems were secured with the user name and password to authenticate the user and some way to identify the user as they access various applications and systems. Once the user is authenticated, they generally are not challenged after that point and in the case of a malicious user could have free reign over the system. Security experts have pointed out that there is a necessity to provide multiple forms of authentication and identification and not based on usernames and passwords. Biometrics could provide a primary as well as a secondary way to authenticate and identify users. In security applications Biometrics refers to automated methods for identifying people based on their unique physical characteristics or behavioral traits

The need for Biometrics is brought on by the need to ensure and enhance security on systems. Users need to be assured that the system that they are using is correctly and securely authenticating them for any type of application they may use that all users are being securely authenticated and identified on the system. Data is collected into individual user profiles based on the user's mouse movements.

2.3 Detecting Computer Intrusions Using Behavioral Biometrics

In behavioral biometrics using intrusion detection[4] applications. We present a new biometrics-based technique, which can be used to detect intrusion without the need for any special hardware implementation and without forcing the user to perform any special actions. The technique is based on using "keystroke dynamics" and "mouse dynamics" biometrics.

We use a new behavioral biometrics based on computer mouse dynamics. Mouse and keystroke dynamics biometrics are two related technologies. Mouse dynamics, however, fulfills all the characteristics required for

intrusion detection since it allows passive, dynamic, and real-time monitoring of users, and it simply requires a standard computer mouse for data collection. Actually, mouse and keystroke dynamics are complementary biometrics. While a mouse is very important for graphical user interface (GUI) –based applications, a keyboard is essential for command –line based applications. So our objective is to combine these two technologies in a common detector.

2.4 Biometrics Technologies

Our detection framework is based on mouse and keystroke dynamics biometrics, which represent two separate but related biometrics. Data collection is performed using a common detection module.
Keystroke dynamics is considered a strong behavioral biometric .The functionality of this biometric is to measure the dwell time (the length of time a key is held down) and flight time (the time to move from one key to another) for keyboard actions. After these measurements have been collected, then the collected actions are translated into a number of digraphs or trigraphs to be analyzed in order to produce a pattern that identifies the user who generated these keyboard actions. Our Keystroke Dynamics Signature or KDS, which is used as a reference user profile and matched against active user Profiles to dynamically detect masqueraders.
To construct the KeyStrokeDynamics we propose a key oriented neural network based approach, where a neural network is trained for each keyboard key to best simulate its usage dynamics with reference to other keys. We also propose a technique which can be used to approximate a digraph/ tri-graph value based on other detected graphs and the locations of the keys with reference to each other, aiming to speed up the user enrollment process.
Mouse and keystroke data was collected transparently and sent to a central server. At the end of the data collection phase, we used the collected data to conduct an offline evaluation of our detection system. The confidence ratio calculated for evaluate the false positives, for each legal user we compared their own remaining sessions (not involved in the computation of the reference signature) against their reference signature.

2.5 Username and Password Verification through Keystroke Dynamics

Biometrics when used with a password is the use of unique human physical characteristics to identify and authenticate authorized personnel [5]. You can use these devices to control doors, gates, etc. Biometric access control solutions can be applied to a wide variety of challenges, including network or device identification and authentication. Human traits used for biometrics are divided into physical and behavioral. There are several human physical characteristics that can be used to uniquely identify a person. They include:

1. The retina, specifically the blood vessel pattern inside the eye 2. Voice patterns 3. Finger or hand geometry, including fingerprints, finger or hand height and width, etc. 4. The features of the iris, the colored area of the eye surrounding the pupil. Keystroke dynamics (KD) is a behavioral biometric. KD solutions usually measure both of the following:

Dwell time – how long a key is pressed
Flight time – how long it takes to move from one key to another.

Keystroke dynamics may be a way to combine the usability of username and password schemes with the benefits of biometric systems at minimal cost to system administrators and users.
For example, the way you walk or the way you sign your name; it can be said that the current state of either behavior is the culmination of many years of practice / experience. On the other hand, it has been said that behavioral biometrics offer a degree of replaceability that physiological biometrics do not. For instance, in terms of a person to person comparison, the way an individual says one word may be fundamentally different from the way he says a different word. Furthermore, although a time intensive process, it is said that individuals may be able to change such behavioral characteristics given the appropriate desire / commitment. For example, one could reinvent the way she signs her signature, it would take a lot of practice, but it is clearly a possible

2.6 A Statistical Model for Biometric Verification

Traditional biometrics technologies such as fingerprints or iris recognition systems require special hardware devices for biometrics data collection. This makes them unsuitable for online computer user monitoring, which to be effective should be non-intrusive, and carried out passively. Behavioral biometrics based on human computer interaction devices such as mouse and keyboards do not carry such limitation, and as such are good candidates for online computer user monitoring. The artificial intelligence based techniques that can be used to analyze and process keystroke and mouse dynamics to achieve passive user monitoring
Most biometrics systems require special hardware device for biometrics data collection, restricting their use to only networks segments where such devices are available. Behavioral biometrics such as mouse dynamics and keystroke dynamics are appropriate for such context

because they only require traditional human-computer interaction devices.

2.7 Biometrics Modes and Metrics

Biometric systems operate in two modes, the enrollment mode and the verification identification mode. In the first mode, biometric data is acquired using a user interface or a capturing device, such as a fingerprints scanner. Raw biometric data is then processed to extract the biometric features representing the characteristics, which can be used to distinguish between different users. This conversion process produces a processed biometric identification sample, which is stored in a database for future identification/verification needs. Enrolled data should be free of noise and any other defects that can affect its comparison with other samples. In the second mode, biometric data is captured, processed and compared against the stored enrolled sample. According to the type of application, a verification or identification process will be conducted on the processed

Verification process: conducts one-to-one matching by comparing the processed sample against the enrolled sample of the same user. For example, user authentication at login: the user declares his identity by entering his login name. He then confirms his identity by providing a password and biometric information, such as his signature, voice password, or fingerprint. To verify the identity, the system will compare the user's biometric data against his record in the database, resulting with a match or non-match. Identification process: matches the processed sample against a large number of enrolled samples by conducting a 1 to N matching to identify the user; resulting in an identified user or a non-match order to evaluate the accuracy of a biometric system.

3. Our Contribution

Mouse dynamics is a new behavioral biometric recently introduced. The idea behind this biometric is to monitor all mouse actions generated as a result of user interaction with a graphical user interface, and then process the data obtained from these actions in order to analyze the behavior of the user. Mouse actions include general mouse movement, drag and drop, point and click, and silence (i.e. no movement). these factors are used to construct what is called a Mouse Dynamics Signature or MDS, a unique set of values characterizing the user’s behavior over the monitoring period. Some of the factors consist of calculating the average speed against the traveled distance, or calculating the average speed against the movement direction.

In our approach users are allowed to play two different games in a period of time. The game is designed in such a way that all the type of actions are involved. we monitor the users mouse behavior and model the behavior through seven different factors.

We introduced behavior standardization process which will distinguish user behavior in a better way even under different screen resolutions.

Graphs is used to compare the two users data`s Standardized Mouse Dynamic Detector Architecture [Fig .3.] contains four units

3.1) Data Interception Unit
3.2) Behavior analysis Unit
3.3) Behavior Standardization stage
3.4) Behavior comparison Unit

3.1 Data Interception Unit

The data collected by the detector is a list of actions such as an MM event, left-button-down event, left-button-up event, and so on. Such events do not provide meaningful information for analyzing the behavior. For example, a set of actions that is considered to be a good input to the behavior analysis unit could be represented by the following series of events, measured in milliseconds:

3.2 Behavior Analysis Unit

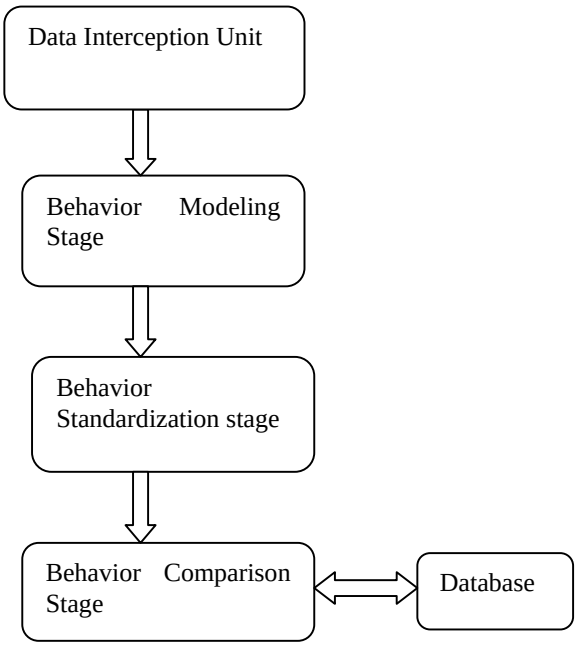


Fig 3.Standardized Mouse dynamic Architecture

The interception software continuously collects the behavior analysis unit every time mouse actions are detected on the monitored workstation. The screen

resolution used for this session was less than or equal to 1,200 pixels.

3.3 Behavior Modeling Unit

Factors Involved in Mouse Signature

1. Movement speed compared to traveled distance (MSD)
2. Direction of movement (DOM)
3. Direction of movement Occurrence(DOM Occur)
4. Types of actions (TOA)
5. Types of actions Occurrence (TOA Occur)
6. Movement elapsed time (MET)
7. Movement elapsed time (MET Occur)

3.3.1 Movement Speed Compared to Traveled Distance (MSD)

In this factor we have to collect the data to identify user behavior contains 12 data points over the MSD curve.i.e we splitted into 12 different ranges from 0-1200.
In this factor comparing the MSD curve over different sections. i.e. comparing movement Speed with travel distance

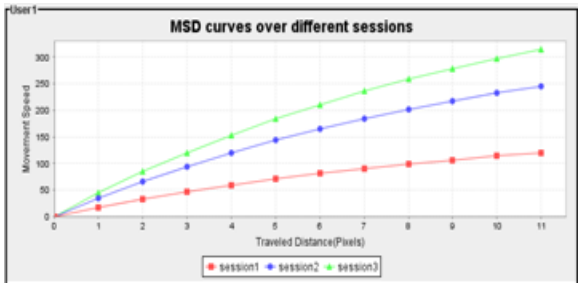


Fig 3.3.1 (a)

Fig 3.3.1(a) shows the Movement Speed compared to traveled Distance (MSD) Curve over Same User.

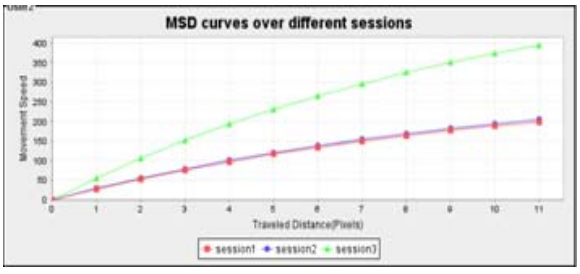


Fig 3.3.1(b)

Fig 3.3.1(b) shows the Movement Speed compared to traveled Distance (MSD) Curve over different User.

3.3.2 Direction of Movement (DOM)

This factor referred to as the Average Speed per Direction of Movement (DOM).i.e. to calculate the movement speed in each of eight directions. The Screen is divided into eight direction of 0 to 45 degree as direction 1and direction 2 represent 45 to 90 degree and so on.

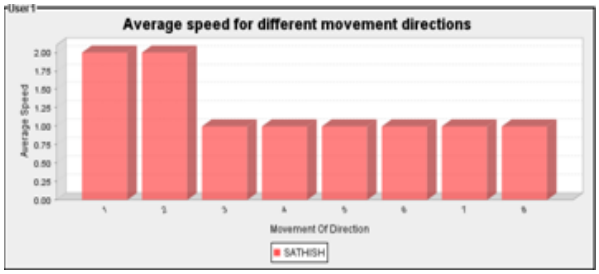


Fig 3.3.2 (a)

Fig 3.3.2(a) shows the Average speed per direction of Movements of user 1

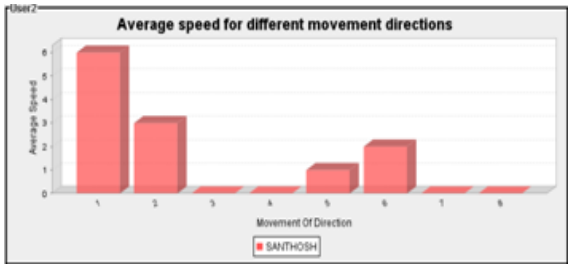


Fig 3.3.2(b)

Fig 3.3.2 (b) shows the Average speed per direction of Movement of user 2.

3.3.3 Direction Of Movement Occurrence (DOM Occur) of two different Users

This factor used to find the histogram of the Mouse Movement Direction. i.e. for each direction we have to calculate the occurrence of the Mouse movements. It contains the value of Average speed for different Movement Direction.

Fig 3.3.3(a)

Fig 3.3.3(a) shows the Occurrence of the Direction of Movement of user 1.

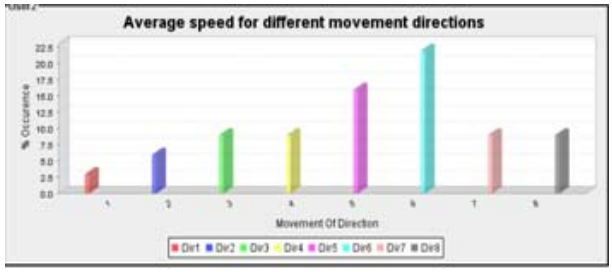


Fig 3.3.3(b)

Fig 3.3.3(b) shows the Occurrence of the Direction of Movement of user 2.

3.3.4 Average Movement Speed per Types of Actions (TOA) for two different users

There are three types of actions.PC (Point Click), DD (Drag and Drop) and MM (Mouse Move).TOA shows the relation between the movement speed and the type of performed action for the three recognized types of actions.

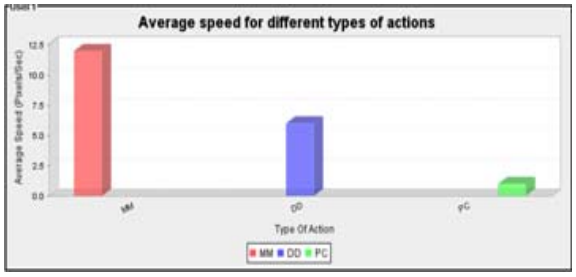


Fig 3.3.4 (a)

Fig 3.3.4(a) shows the Average Movement speed per Types of Actions of user 1.

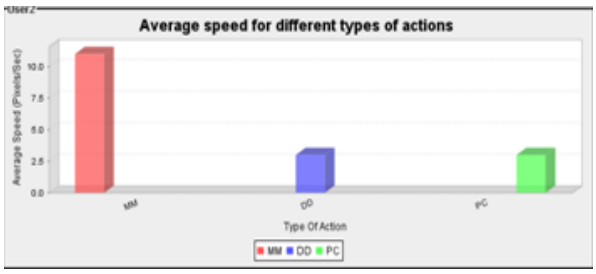


Fig 3.3.4 (b)

Fig 3.3.4(b) shows the Average Movement speed per Types of Actions of user 2.

3.3.5 Type of Action occurrence (TOA Occur) of two different Users

In this Action Type Histogram We compared the Histogram of the different Action. i.e. PC, DD, MM between the two different user.

Fig 3.3.5 (a)

Fig 3.3.5 (a) shows the Occurrence of the Type of Action of user 1.

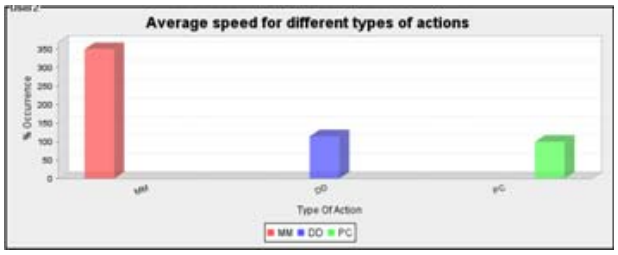


Fig 3.3.5(b)

Fig 3.3.5 (b) shows the Occurrence of the Type of Action of user 2.

3.3.6 Movement Elapsed Time (MET)

The Movement Elapsed Time (MET)) illustrate the distribution of the number of actions performed by the User within different distance ranges. The distribution differs from one user to another.

3.3.7 Movement Elapsed Time (MET) for two different Users

The elapsed time is the time spent by the user to perform an action.i.e it is between the traveled distance and the type of the performed action. Movement Elapsed Time (MET) defines the number of actions performed by the user within the different time ranges during the user's session. Collect all types of Actions over one user session with a specific range.

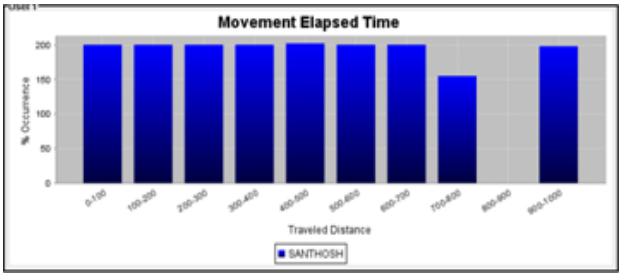


Fig 3.3.6 (a)

Fig 3.3.6 (a) shows the Movement Elapsed Time of user 1.

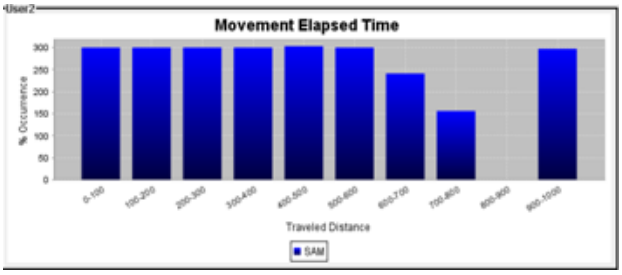


Fig 3.3.6 (b)

Fig 3.3.6 (b) shows the Movement Elapsed Time of user 2.

3.4 Behavior Standardization Stage

We have introduced the behavioral standardization stage to standardize the user signature irrespective of the setting of the screen resolution. In the earlier approaches the mouse signature for different users varies under different screen resolution making it difficult to introduce for different application. If the reference signature has been calculated on a specific resolution and the detection process has been done on a different resolution, this will affect the range of the data collected and will be reflected in the results. Similarly the operating system mouse pointer speed and acceleration settings; any changes to these settings can affect the calculated figures and, consequently, the user behavior itself.

To improve the accuracy of the detector we have introduced the Behavioral Standardization stage. Experimentation is done with the users under different settings and a standardized signature is obtained. relation between the user signatures under different settings is derived. This relation helps us in the standardization process.

Standardized Approach is used to find the user behavior in different screen resolution.

Initial Resolution: x * y
Target Resolution: l * m

Initial resolution distance d = d1+d2+d3
Where d1 = X mouse move
d2 = Y mouse move
d3 = diagonal movement

Target Resolution:

$$A = d1 * l / x + d2 * m/y + d3 * (l * m) /x * y$$

Futher we are trying to apply for different Mouse pointer speed also.

3.5 Behavior Comparison

In this Behavior comparison unit we compare the difference between the current users with already existing user data which is stored in database. The status of the trained network is stored in the database. In order to find the detection process, find the threshold limit to ensure the identity of the user. The sample data consists of five session from which to find the accuracy. Other user data is compared with the data that is stored in database.

4. Conclusion

We have introduced new Biometric technology based on standardized mouse dynamics which provides better result even under different screen resolution making it suitable for application like Intrusion detection. The mouse dynamics can be further standardized based on the mouse pointer speed. The combining standardized screen resolution and standardized mouse pointer speed will guarantee even better result.

References

[1] A. Awad E. A. and I. Traore, "A New Biometric Technology Based on Mouse Dynamics", IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 3, Sep 2007

[2] N. Ajufor, A. Amalraj, R. Diaz, Mohammed Islam, M. Lampe, "Refinement of a Mouse Movement Biometric System", Pace University

[3] A. Weiss, A. Ramapanicker, P. Shah, S. Noble,L. Immure, " Mouse Movements Biometric Identification: A Feasibility Study", Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 2007.

[4] A. Awad E. A. and I. Traore, "Detecting Computer Intrusion Using Behavioral Biometrics" University of Victoria.

[5] V.Matyas Jr and, z.Riha "Username and Password Verification through Keystroke Dynamics" IEEE Security and Privacy Magazine, Vol 1,no .3,pp45-49,may/june 2003.

[6] F.Bergadano, D.Gunetiad and c.picardi,"User Authentication through Key stroke Dynamics"ACM trans.Information and System security, Vol.5,no.4,pp.367-397,Nov 2002.

[7] M.Brown and S.J Rogers, "User Identification via Keystroke Characteristics of Typed Names Using Neural Networks" Int'l Man-Machine Studies,Vol 39,pp 999-1014,1993

[8] A.Chan,R.W.H.Lau,and A.Si," A Motion Prediction Method for Mouse-Based Navigation,"proc,.IEEE Computer Graphics Int'l conf.(CGI'01),pp139-146.

[9] R.Joyce and G.Gupta "Identify Authentication Based on Keystroke Latencies" commn..ACM Vol 33,No 2,pp 168-176,Feb 1990.

[10] J.McHugh "Intrusion and Intrusion Detection ,"int"Information Security,Vol,pp14--35,2001.

[11] F.Monrose and A.Rubin,"Authentication via Keystroke Dynamics" proc .Fourth ACM conf.Computer and Commn Security(CCS.'97),pp 48-56,April 1997.

[12] P.Oel, p.schmidt and A.Shmit," Time prediction of Mouse Based Cursor Movements"proc.Joint AFIHM-BCS conf. Human Computer Interaction (IHM-HCI'01)V0l2 pp37-40,sept 2007…

[13] A.Martin and M.Przybocki,"The NIST 1999 Speaker Recognition Evaluation –An Overview,"Digital Signal Processing ,vol. 10 ,no 1-3,pp 1-18,2000.

[14] Denning "An Intrusion Detection Model," IEEE Trans.software Eng Vol 13 no 2,pp222-232, Feb 1987.

Mr.S. Benson Edwin Raj is young and dynamic computer professional with over 9 years of teaching and technical experience in Karunya University. He is a man behind the IT infrastructure development of Karunya University. He is heading the Network Security Research group and has been instrumental in moulding the students.

A. Thomson Santhosh doing Post Graduate in Computer Science and Engineering at Karunya University. He is doing his research work in Network Security. Area of Interest is networking and Network Security.