International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Mouse and Keystroke Based Behavioural Biometrics: Techniques, Problems and Solutions.

Raina K. Jain[1], Sancheti Shital D.[2] ,Pansare Jyoti T.[3] ,Kawale Shubhangi K.[4] , Aishwarya Gopalkrishnan[5]
[1]*Department of Information Technology , SNJB's KBJ COE, jain.rainkcoe@gmail.com*
[2]*Department of Information Technology , SNJB's KBJ COE, shital4695@gmail.com*
[3]*Department of Information Technology , SNJB's KBJ COE, jyotipansare93@gmail.com*
[4]*Department of Information Technology , SNJB's KBJ COE, srchechare@gmail.com*
[5]*Department of Information Technology , SNJB's KBJ COE, [5]aishwaryanair819@gmail.com*

Abstract—Identity theft has become a widespread crime all over the soft world. Various techniques from login-password up to complex biometric systems have been devised to cope up with this crime. But the problem persists. This paper lists various behavioral biometric systems while focuses only on two of them viz. keyboard dynamics and mouse dynamics. This paper also lists the problems that persists in these two techniques and suggests a solution that could increase the accuracy of existing system.

Keywords-Behavioral biometrics, mouse dynamics, keyboard dynamics.

I. INTRODUCTION

With the growing discoveries in the world of computers, internet, e-commerce etc. world is facing new problems of data and identity theft, malwares, hacking etc. Out of which identity theft has become a widespread problem. Many security systems have been devised till date trying to cope up with this problem. But the issue still remains. The basic security system began with login and password and till date we have complex biometric systems.

After the text based security, there came a method which used PINs and smart cards. These security measures were followed by biometrics that used the biological features of human body to identify a user. These features are unique to every being. Hence a user can be identified using these features.

Biometric authentication system has long since been a field of vast research and has provided a trusted solution for user identification and authentication system. A biometric system has been categorized as :

1. System that recognizes a user based on the physical appearance.
2. System that recognizes a user based on the behaviour.

The former is termed as physiological biometrics and its common examples include face recognition system, fingerprint scanning system, retina scanning system and so on. The latter is termed as behavioural biometric system. Examples include speech or voice recognition system, signature recognition system, stride recognition, gaming strategy recognition etc. Even though, physiological biometric systems are used widely, still many of its applications cannot escape spoofing. An equivalent facial model or a fingerprint punch card can be easily produced and the system can be spoofed. Moreover, the security of the database of physiological biometric system is also an issue. Physiological biometric system requires expensive hardware devices like scanners, cameras and sensors for implementation.

All these issues are handled in behavioural biometric systems. It avoids spoofing, provides database security and no requirement of any expensive hardware devices. One can reproduce physiological characteristics of an individual to spoof but cannot reproduce behavioural model of an individual.

Even if the database of features of behavioural biometric system is hacked, it will make no sense to the attacker.

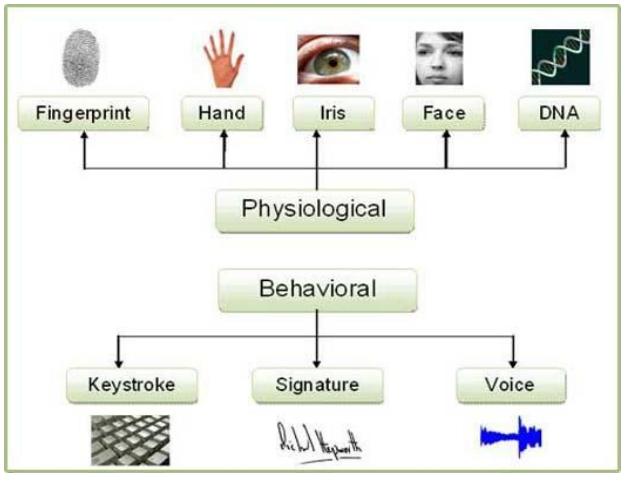


Figure.1. Classification of Biometric System

II. BEHAVIOURAL BIOMETRICS

We can say that a biometric system is a pattern matching system with the basic modules such as the one to capture events, one to extract events, a pattern matcher/recognizer, a database that stores all the actions to be performed during certain events, and a database that stores user pattern. All these (and sometimes more) may constitute a biometric system.

Behavioral biometric system can thus be defined as a system which continuously "verifies" a user identity by capturing the specific behavior of the user.

The general architecture of behavioral biometric system is as shown in figure 2. Yampolskiy et. al.[1] has classified the behavioural biometric techniques further, as follows:

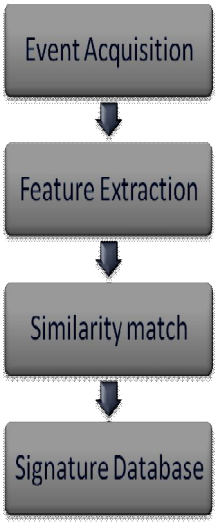


Figure 2. General Architecture of Behavioral Biometric System

2.1 Authorship based biometric: It is based on examining a piece of text or a drawing produced by a person. Verification is accomplished by observing style peculiarities typical to the author of the work being examined, such as the used vocabulary, punctuation or brush strokes.

2.2 Human computer interaction (HCI)-based biometrics: It is based on the unique ability of each individual to apply skills or knowledge

2.3 The indirect HCI-based biometrics: These are the events that can be obtained by monitoring user's HCI behavior indirectly via observable low-level actions of computer software (Yampolskiy). Ex. Audit logs[1], gait or stride[1], car driving style[1], credit card use[1],etc.

2.4 Motor-skill based behavioral biometrics (kinetics): Motor-skill is an ability of a human being to utilize muscles [1]. Motor skills indirectly reflect the quality of functioning of brain.

2.5 Purely behavioral biometrics: Purely behavioral biometrics measures human behaviour such as an individual's stride, or drives a car etc.

Table 1: Comparison of mouse based behavioural biometric techniques

	Data Collection				**Feature Source**		**Result (%)**	
	Environment	Apparatus	Users	Task	Move	Click	FAR	FRR
Pusara et al. [10]	uncontrolled	different	18	free		✓	27.5	3.06
Gamboa et al.[12]	uncontrolled	different	50	free		✓	6.2	6.2
Ahmed et. al.[11]	uncontrolled	different	22	free	✓	✓	2.46	2.46
Revett et al.[9]	uncontrolled	NA	6	fixed	✓	✓	3.5	4
Bours et al.[13]	uncontrolled	different	28	free		✓	26.8	26.8
Shena et al.[14]	Controlled	Same	37	fixed	✓	✓	8.74	7.69

III. PROBLEMS WITH IMPLEMENTATION

The basic limitations of the existing systems are:

1. Large size of database: The feature dataset in the existing system tends to be very large because minute mouse movements and keystroke movements of the users are recorded. There may be many hundreds of record in the feature set of a single user. Also, many existing systems take multiple samples of one user to provide greater accuracy in identification of user. This makes the size of feature set very large.
2. Large authentication time: The authentication period of the system depends upon the similarity match function used and the size of the dataset. The authentication time is directly proportional to the size of the dataset. Hence the authentication time is also more.
3. Large enrollment or training period: The existing systems need to take multiple samples for each user. that means user needs training for enrollment. This training may consist of multiple attempts for enrollment to achieve higher accuracy.

IV. PROPOSED SOLUTION

Through the discoveries and inventions of years in this field, we come to understand that every technique has its own pros and cons. But to acquire high range of accuracy one can combine two or more techniques, for example:

1. Combination of username password system alongwith mouse/keyboard
2. Use of dynamically changing data [5].
3. Combination of physiological and behavioral biometric data. These solutions may provide better accuracy for user identity verification.

So, the proposed system uses multimodal behavioural biometrics. The multimodality is a promising technique to provide higher accuracy. In the proposed system, input or the user behaviour is acquired from two sources namely mouse and keyboard (hence the name multimodality). The architecture of the proposed system is shown in figure 2.

5.1. Event Acquisition:

The event acquisition module takes the input from two different sources namely mouse and keyboard. A user has to provide a user defined pass key for the system to capture the keystrokes. An interaction window is provided for user to perform certain mouse activities and basic mouse events are captured from this interaction window.

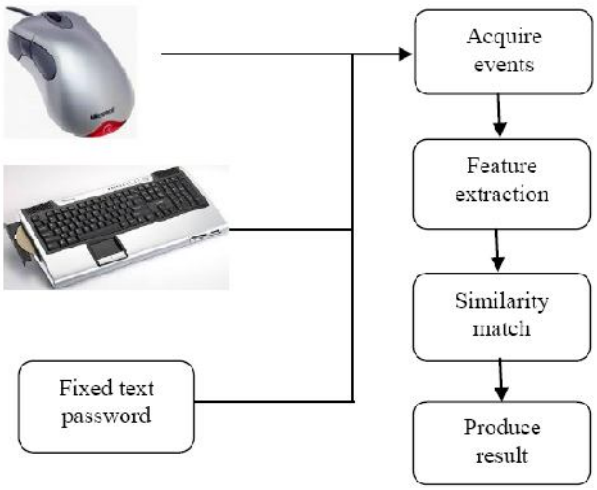
5.2 Feature Extraction:

The features like distance, speed, time etc related to both the input devices are calculated in the feature extractor and stored as a feature profile in a database. This feature profile is unique to each user. User identification is based on this feature profile. A unique pass key is also attached with each feature profile to make the system completely invulnerable.

5.3 Similarity Match:

A similarity match function is applied during user identification time to identify the user. The feature profile is constructed for the second time during identification and matched with the one previously stored in the database. Based on a certain pre-defined threshold value, the matching function will generate result whether user is granted access or not.

The proposed system considers limited number of samples for each user (in this case, just 3 samples). Also a feature set of 40 features is used in the proposed system to characterize a user. Therefore, as compared to the existing methodologies the feature dataset is considerably smaller in size. That will remove the overhead in searching. The triple security of mouse- movement identification, keystrokes identification and password matching promises a greater accuracy thus reducing the false acceptance and rejection ratio.



Fiureg 3: System architecture

REFERENCES

[1] Roman Roman V. Yampolskiy, VenuGovindaraju "Behavioral biometrics: a survey and classification", Int. J. Biometrics, Vol. 1, No. 1, 2008.

[2] Clint Feher, Yuval Elovici, Robert Moskovitch, LiorRokach, AlonSchclar, "User identity verification via mouse dynamics", Information Sciences 201 (2012) 19–36.

[3] M. Karnana, M. Akilab, N. Krishnarajc, "Biometric personal authentication using keystroke dynamics: A review",Applied Soft Computing 11 (2011) 1565–1573, 17 august 2010.

[4] Benjamin Purgasona, David Hiblerb," Security Through Behavioral Biometrics and Artificial Intelligence", Procedia Computer Science 12 (2012) 398 – 403, Conference Organized by Missouri University of Science and Technology 2012- Washington D.C.

[5] Nobuyuki Nishiuchi, "Combining dynamic data with physical biometric verification to counteract spoofing",Journal of medical informatics & technologies, Vol. 15/2010, ISSN 1642-6037.

[6] Enzhe Yu, Sungzoon Cho, "Keystroke dynamics identity verification: problems and practical solutions", Computers & Security (2004) 23, 428e440.

[7] Scholkopf B, Platt J, Shawe-Taylor J, Smola AJ, Williamson RC, "Estimating the support of a high-dimensional distribution",Technical Report MSR-TR-99-87,Microsoft Research, Redmond,WA; 1999.

[8] http://www.engineersgarage.com/articles/biometrics

[9] Revett, K., Jahankhani, H., de Magalhaes, S., and Santos, H., "A Survey of User Authentication Based On Mouse Dynamics", *In Proc. of the 4th Intl. Conference on Global E-Security (ICGeS 2008),* London, UK, June 23-25, pp. 210-219, 2008.

[10] M. Pusara, C.E. Brodley, "User re-authentication via mouse-movements", in: Proceedings of the ACM Workshop Visualization and Data Mining forComputer Security, (VizSEC/DMSEC 2004), ACM, Washington, DC, USA, 2004, pp. 1–8.

[11] Ahmed, A. A and Traore, I., "A New Biometric Technology Based On Mouse Dynamics", IEEE Transactions on Dependable and SecureComputing4, 3 (July), pp. 165-179, 2007.

[12] Hugo Gamboa and Ana Fredb,. "A Behavioural Biometric System Based on Human Computer Interaction" , The Pennsylvania State University CiteSeerX Archives, PRIS, 2003.

[13] Bours, P., Fullu, C.J., "A Login System Using Mouse Dynamics", *In Proc. of the 5thIntl. Conference onIntelligent Information Hiding andMultimedia Signal Processing (IIH-MSP 2009),* Kyoto, Japan, Sept. 12-14, 2009.

[14] Chao Shena, ZhongminCaia, XiaohongGuana,b, HuilanShaa, JingziDua, "Feature Analysis of Mouse Dynamics in Identity Authentication and Monitoring", 978-1-4244-3435-0/09/$25.00 ©2009 IEEE.

[15] AnandMotwani, Raina Jain and Jyoti Sondhi. Article: A Multimodal Behavioral Biometric Technique for User Identification using Mouse and Keystroke Dynamics. *International Journal of Computer Applications* 111(8):15-20, February 2015.

