An Enhanced Information Authentication by Multimodal Biometrics Security

Ms. C. Girija[1] Ms. R. Revathi[2] Ms. S. Saranya[3] Mr. S. Sivachandiran[4]
[1,2,3]P.G Student [4]Assistant Professor
[1,2,3,4]Department of Computer Applications
[1,2]IFET College of Engineering

Abstract— In the present world, we all know that Biometric security is concerned with the assurance of confidentiality, integrity, and availability of information in all forms, in this work we are focusing on biometric authentication along with all security assurance. Authentication of a person is an important task in many areas of day-to-day life including electronic commerce, system security and access control. There is possibility of getting biometric template information by imposter and can change the information which leads to the leakage of information. If the authentication is not being done then there is compromise in security. The biometric authentication provides the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. The problem here is to authenticate using the information of the user without compromise in the security as well as the leakage of information of the individual. So, in this paper, we have proposed a multi-biometric model (integrating voice, fingerprint and facial scanning) that can be embedded in an information this making transactions more secure.

Key words: Biometrics, Keystroke, Mouse Dynamics, Authentication

I. INTRODUCTION

Biometric authentication systems are gaining wide-spread popularity in recent years due to the advances in sensor technologies as well as improvements in the matching algorithms that make the systems both secure and cost effective. They are ideally suited for both high security and remote authentication applications due to the non-repudiate in nature and user convenience. Most biometric systems are assumed to be secure but there are chances of getting hacked. There are two places to be attacked: (i) one is on communication link and another (ii) on server's database. In order to protect from this type of attacks we propose this system. However a variety of applications of authentication need to work over partially secured or in-secured networks such as ATM networks or the Internet. Authentication over insecure public networks or with untrusted servers raises more concern in privacy and security. The primary concern is related to the security of the plain biometric templates, which cannot be replaced, once they are compromised. The privacy concerns arise from the fact that the biometric samples reveal more information about its owner in addition to the identity. The biometric authentication is being used for authenticating in most of the security required scenarios. If the biometrics used in plain, there are more chances for spoofing attacks by the imposters to gain illegal access to the server to get information about the client or to gain illegal access to the client to gain information about the server, which is not desirable. The network is not secure for the server as well as for the client. Hence this is a factor of motivation for any researcher to take up a research work on the enhancement of the security to address the problem.

Authentication is the most important aspect in human life from the security point of view. Most of the existing mechanisms use the reference template for the final authentication. These templates are stored in the raw format or some encrypted format. There is possibility of getting this information by imposter and can change the information which leads to the leakage of information. If the authentication is not being done then there is compromise in security. The problem here is to authenticate using the information of the user without compromise in the security as well as the leakage of information of the individual. Widespread use of biometric authentication also raises concern of tracking a person, as every activity that requires authentication can be uniquely assigned to an individual. The primary concern is related to the security of the plain biometric templates, which cannot be replaced, once they are compromised.

II. EXISTING SYSTEM

1) The plain biometric can be easily accessed by the imposter.
2) The plain biometric is sent to the server for both enrolment and for authentication, there is a much chance for the leakage of information.
3) If the user-specific key is compromised, the template is no longer secure imposter can recover the original biometric template using specific key.
4) The network is insecure in the sense that the intruder is in the network then he can gain access to the server as well as to the client.

III. BIOMETRICS

Biometrics makes the use of biological terms that deals with data statistically. It verifies a person's uniqueness by analyzing his physical features or behaviors (e.g. face, fingerprint, voice, signature, keystroke rhythms). The systems record data from the user and compare it each time the user is claimed. A biometric system is a computer system that implements biometric recognition algorithms. A typical biometric system consists of sensing, feature extraction, and matching modules. We can classify the biometric techniques into two classes: Physiological based techniques include facial analysis, fingerprint, hand geometry, retinal analysis, DNA and measure the physiological characteristics of a person. Behavior based techniques include signature, key stroke, voice, smell, sweat pores analysis and measure behavioral characteristics. Biometric recognition systems based on the above methods can work in two modes: identification mode, where the system identifies a person searching a large data base of enrolled for a match; and authentication mode where the

All rights reserved by www.ijsrd.com

system verifies a person's claimed identity from his earlier enrolled pattern.

1) Types of Biometrics:

A. Facial Recognition:

The facial recognition systems differentiate between the background and the face. This is important when the system has to identify a face within a throng. The system then makes International use of a person's facial features – its peaks and valleys and landmarks – and treats these as nodes that can be measured and compared against those that are stored in the system's database. There are around 80 nodes comprising the face print that the system makes use of and this includes the jaw line length, eye socket depth, distance between the eyes, cheekbone shape, and the width of the nose.

1) Advantages:

- It is not intrusive.
- It is hands-free, and continuous.
- It can be done from a distance even without the user being aware they are being scanned.

B. Iris Recognition:

Iris recognition is an automated method of biometric identification which uses mathematical pattern recognition techniques on video images of the irises of an individual's eyes, whose complex random patterns are unique and can be seen from some distance. Iris cameras perform recognition detection of a person's identity by analysis of the random patterns that are visible within the iris of an eye from several distances. It combines computer vision, pattern recognition, statistical inference and optics. The iris is the colored ring around the pupil of every human being and like a snowflake, no two are the same. Each one is unique in its own way, exhibiting a distinctive form.

1) Advantages of Iris Recognition:

- Iris-scanning technology is not very intrusive as there is no direct contact between the subject and the camera technology.
- It is non-invasive, as it does not use any laser technology, just simple video technology.
- The accurateness of the scanning technology is a major benefit with error rates being very low, hence ensuring a highly reliable system for authentication.

C. Keystroke:

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. 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. Keystroke analysis is concerned with the frequency, accuracy, the pause between strokes and the length of time a key is depressed.

1) Advantages of Keystroke:

- Keystroke recognition system is simple to implement due to the fact that it does not require any specific hardware.
- It is relatively easy to learn.

D. Mouse Dynamics:

Mouse dynamics can be described as the characteristics of the actions received from the mouse input device for a specific user while interacting with a specific graphical user interface.

1) A Mouse Action Can Be Classified Into One Of The Following Categories:

- Mouse-Move (MM): general mouse movement,
- Drag-and-Drop (DD): the action starts with mouse button down, movement, and then mouse button up,
- Point-and-Click (PC): mouse movement followed by a click or a double click, and
- Silence: no movement. The characteristics of mouse dynamics can be described by a set of factors generated as a result of analyzing the recorded mouse actions. These factors represent the components mouse dynamics signature for a specific user, which can be used in verifying the identity of the user.

2) Advantages of Mouse Dynamics:

- Mouse dynamics does not required special hardware device for data collection.
- Low cost and low invasiveness.

IV. PROPOSED SYSTEM

A. Multibiometrics:

A multi-biometrics system is obtained by the integration of multiple individual biometrics models. A numbers of models integrating hand geometry, keystroke dynamics, face and iris recognition system have flooded the markets in recent years. Here we present a multimodal system that can be embedded in an information, which integrates fingerprint, voice and digital signature. It shuts down the problem of high False Rejection Rate of facial scanners, eliminates the fooling of fingerprint scanners and overshadows the disadvantage of voice recognition models. Multimodal biometric systems are more resistant to spoof attacks because it is difficult to simultaneously spoof multiple biometric sources. Further, a multibiometric system can easily incorporate a challenge-response mechanism during biometric acquisition by acquiring a subset of the traits in some random order.

B. Working Process:

In this system, we implement the concept of multibiometrics to provide more security for user information.

1) Step 1: If one user wants to access the secured information means they should be authenticated.
2) Step 2: During information transaction between a client and server both must have knowledge of biometrics used in their information.

All rights reserved by www.ijsrd.com

Fig. 1: Keystroke Biometrics

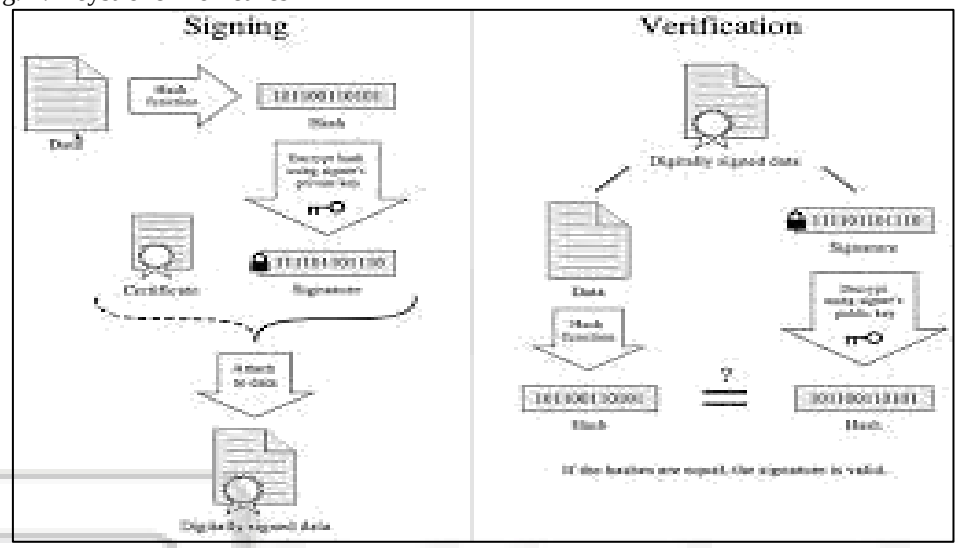

Fig. 2: Signing and Verification

V. NEED FOR BIOMETRICS IN INFORMATION TRANSACTION

Now-a-days, information sending through the internet has become very popular and familiar process throughout the world. There is also many of the hackers are present to stole the user privacy information and misused for their purpose. Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less exclusive authentication for a variety of applications. The biometric authentication provides the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements.As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users.

VI. CONCLUSION

There are several attacks that try to negotiate a computer system using a variety of methods such as unauthorized access. The most reliable identification systems are based on biometrics. Therefore, several biometrics technologies start to accompany host-based Intrusion detection systems. Until Now, behavioral biometric was the only techniques that have been used so far, since they do not need any special devices. These system will make more helpful for private organization who make business transaction through online and provide high security than security measures and will be the most important technique which dominate all other technique in current trend.

3) Step 3: Using digital signature they can verify the data by hash function.
4) Step 4: Finally the information is transferred securely.

REFERENCES

[1] ”Biometrics” by Samir Nanavathi, Dreamtech Wiley Publications.
[2] ”Biometrics made easy for you” by John walker.
[3] The Challenge of User Authentication http://www.ankari.com/whitepapers.asp
[4] The Zephyr™ Charts http://www.biometricgroup.com/e/zephyr_charts.html.
[5] A. Juels and M. Sudan. A fuzzy vault scheme. In IEEE International Symposium on Information Theory, Lausanne, Switzerland, 2002.
[6] A. K. Jain and A. Ross, (2004), Multibiometric Systems, Communications of the ACM, Special Issue on Multimodal Interfaces, 47(1), pp. 34–40.
[7] D. Gunetti and C. Picardi. Keystroke analysis of free text. ACM transactions on information and System Security, 8(3), 2005.
[8] E. Lau, X. LI, C. Xiao, and X. Yu. Enhanced user authentication through keystroke biometrics. In Computer and Network Security, Massachusetts Institute of technology, 2004.
[9] J. McHugh. Intrusion and intrusion detection. International Journal of Information Security, 1:14–135, 2001.
[10] Khalil Challita, Hikmat Farhat, Khaldoun Khaldi. Biometric Authentication for Intrusion Detection

All rights reserved by *www.ijsrd.com*

Systems. First International Conference on Integrated Intelligent Computing, 20.

[11] T. Rowley, "Silicon Fingerprint Readers: A Solid State Approach to Biometrics," Proceedings of the CardTech/SecureTech Conference, CardTech/SecureTech, Bethesda, MD (1997), pp. 152–159.

[12] WSQ Gray-Scale Fingerprint Image Compression Specification, IAFIS-IC-0110v2, Federal Bureau of Investigation, Criminal Justice Information Services Division (1993).

[13] N. Memon and P. W. Wong, "Protecting Digital Media Content," Communications of the ACM 41, No. 7, 35–43 (1998).

All rights reserved by *www.ijsrd.com*