International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 2 Ver. IV || February 2018 || PP. 16-21

A Review of Emerging Biometric Authentication Technologies

Pawan Kumar
Assistant Professor in Computer Science, DRV D.A.V. Centenary College, Phillaur (Jalandhar)
Research Scholar IKG PTU Jalandhar
Corresponding Author: Pawan Kumar

ABSTRACT: *There exists a variety of ways for the identification of any individual before providing it access to any important data, device, place or services. In the present scenario authentication methods based on the traditional methods not fulfills all the desired security requirements. This article aims to highlight the ways in which biometric based authentication systems can be helpful in the identity verification in various emerging areas like governance, e-commerce and access-control etc. Biometric based authentication techniques are more reliable and almost impossible to impersonate as compared to the other classical methods of authentication. These systems are based on the principle of unique and measurable physiological or behavioral* characteristics *like fingerprints, hand geometry, DNA, Retina, Iris, vein pattern, voice, signatures or keystroke dynamics of human beings. Biometric traits are captured, processed, stored and then matched for carrying out the authentication process.*

KEYWORDS: *authentication, biometric, identification, access control.*

Date of Submission: 09-02-2018 Date of acceptance: 24-02-2018

I. Introduction

Authentication is the core component of all the trust oriented computing services. With the increased use of sophisticated electronic-gadgets, e-commerce and online financial services, importance of sophisticated and reliable authentication techniques have increased manifolds.

This mechanism is deployed to prevent the misuse of devices or services by the unauthorized entities. It ensures the availability of services only to the legitimate users of the services after the verification of credentials provided by them. Authentication is not like a one-size-fits-all kind of domain. Different kind of services requires the varying level of authentication services, so there exists a variety of authentication techniques which are based on different types of security credentials. All these authentication methods can be broadly divided into three categories, based on something you have, something you know and something you are [6]. In the first category of authentication methods, the identity is proved/trust is established on the basis of some physical possession of something like cards, tokens etc. by the authorized entity. Second category of authentication methods is based on the knowledge of facts, which are only known to the legitimate entity, which it has already shared with the system at the time of its first interaction with the system such as password or pin. In the third category authentication of an individual is carried out based on the feature vector derived from physiological or behavioral traits of an individual by using biometric techniques.

Biometric authentication is the process of verifying the identity of an individual by using the already captured and stored unique characteristics of the body, and then on the basis of the outcome of the verification process providing access to a device, service or a place only to the legitimate users.

Biometric based authentication has been considered as the most secure or at least very difficult to forge or deceive as compared to the other classical methods of authentication. Authentication systems based on the biological characteristics have been available since more than last 25-30 years. Initially these biometric systems were slow, expensive and less accurate. These early biometric based authentication systems were mainly deployed for restricting mainframe access and controlling physical entry for only authorized persons. These systems proved workable in some high security situations. Now, computers and other electronic devices are much faster and cheaper than ever, which in turn has attracted the attention of the academia and industry in biometrics based authentication systems. In this article section 2 describes the authentication process. Section 3 is about the performance parameters of biometric based authentication systems. In section 4 important biometric selection factors are defined. Popular biometric technologies based on the physiological and behavioral traits have been described in section 5. In section 6 advantages and disadvantages of these authentication systems are given. Section 7 identifies the application areas, where the biometric authentication is very useful. Section 8 describes the issues in biometric based authentication technologies. In section 9 latest trends in biometric authentication have been discussed. Section 10 conclusions have been drawn about the biometric based authentication technology.

II. Biometric Authentication Process

A biometric based authentication system mainly consists of following subsystem**:**

- Biometric data capture subsystem
- Signal processing subsystem
- Data storage subsystem
- Matching subsystem
- Decision subsystem

The biometric authentication process consists of several stages: capturing the biometric, processing and storing the captured data, matching the captured sample against the stored samples in the biometric repository for verification, and decision making. Capturing involves sensing the biometric characteristics and is necessary both for the creation of the biometric repository and for each authentication trial. For example, when voice based verification system is implemented, then the capturing stage involves recording of one's voice sample using a microphone. Then the digital data are mathematically modeled and stored in the biometric repository. At some later stage, when a person need to be authenticated the device compares the freshly captured biometric sample with the samples already stored in the repository and then makes a decision on the basis of a pre-calculated threshold.

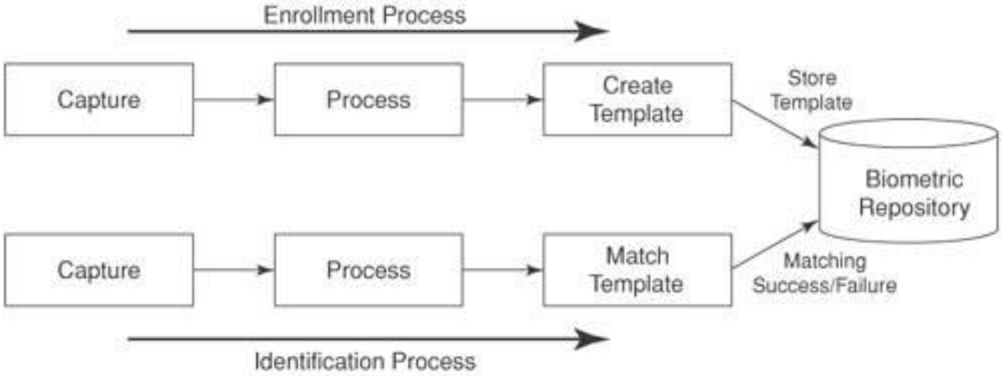

Fig. 1: Enrollment and Identification processes in a biometric authentication system.

III. Performance Parameters Of Biometric Authenticatin Systems

Biometric based authentication systems are not accurate completely. Performance of a biometric system is analyzed by various error estimation techniques. Two well known performance metrics used for evaluating these systems are '**False Rejection Rate**' and '**False Acceptance Rate**'. A False Rejection Rate (FRR) is the rejection ratio of authorized persons trying to access the system. A False Acceptance Rate (FAR) is the acceptance ratio of persons, who are in fact not the legitimate persons. These two types of errors can be controlled by adjusting the confidence threshold of the system. To increase the security of any system, threshold can be increased, which in turn will decrease FAR errors and will increases FRR errors.

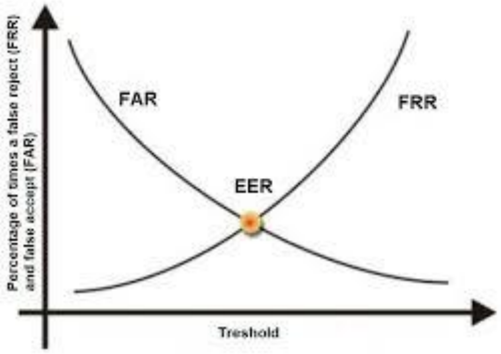

Fig2: Impact of biometric sensitivity/threshold on FAR & FRR.

Equal Error Rate is a midpoint region between False Accept and False Reject plot. It is also a measurement of accuracy of the system in rejecting an impostor. EER is also called as cross over error rate between FAR and FRR.

IV. Biometric Selection Factors

Before deciding on any specific biometric trait to be used in any biometric based authentication system, it is necessary to consider the important characteristics of that trait. However the relevance and importance of these factors vary from application to application, even then these are the main factors which affect the choice of a specific biometric trait for any application in question.

Permanence: The biometric trait must have no effect of time or any other varying condition on it i.e. it must not be affected with the passage of time or due to some illness.

Uniqueness: The biometric trait must have unique and distinguishable features over the entire population.

Universality: The biometric trait must be applicable on the entire entity set under the domain.

Easy to Capture: It must be convenient and practically possible to capture and use the selected biometric trait.

Circumvention: The biometric trait should not be reproducible by fraudulent methods for deceiving the authentication system.

Social Acceptability: The authentication system based on some specific biometric trait must have very high degree of acceptability among large groups in the society.

Measurability: Biometric trait must be measurable and comparable with simple and cost-effective technical instruments.

V. Popular Biometric Authentication Technologies

There exists a variety of authentication methods based on the different biometric traits for ensuring the secure and reliable authentication process. Biometric traits can be categorized as physiological versus behavioral traits. Physiological traits are related to the shape of the body, for example fingerprint, face recognition, hand geometry, retina scan, iris scan, DNA Profiling and vascular pattern. Behavioral traits are related to the behavior of a person, includes signature, keystroke dynamics and voice.

Each of these methods has unique set of features and properties. Some biometric systems are easy to deploy and use, some others are more reliable but are sophisticated and costly. Each system has its own set of strengths and weaknesses.

Physiological Biometric Authentication Techniques:

- **Fingerprint Based Authentication**

Finger print scanning technology is the oldest of the biometric identification methods and uses distinctive features of the finger patterns for identification and verification of the identity of individuals. This technique of authentication and identification involves comparing the pattern of ridges and furrows on the finger tips, as well as the minutiae points of a sample to be verified with repository of samples already stored in the system. Fingerprint patterns are having the property that these remain unchanged throughout the life and are also having uniqueness feature. In the history of more than 100 years of fingerprint identification technology, no two fingerprints have ever been found to be similar, not even those of identical twins. Fingerprint scanners can be fitted or attached with gadgets for user authentication, so this technology is also very easy to deploy. One major weakness of this biometric trait is that it might not work properly in the industrial environment where the users may have dirty fingers.

- **Face Recognition based Authentication**

Face recognition systems systematically scan some specific features which are common to everyone's face, like width of the nose, position of cheekbones, distance between the eyes, jaw line, chin and so on. This numerical data is then encoded in such a manner that it uniquely identifies each person.

This is the most flexible biometric based authentication methods, due to its effective and flexible operation even when the person is unaware of being scanned. It provides a means to search through masses of people who spent only seconds in front of a scanner or a digital camera.

- **Hand Geometry biometrics based Authentication**

Hand geometry readers are designed and developed to be deployed in harsh industrial environments and do not require clean conditions. This authentication method is generally preferred in industrial environments.

- **Retina Scan based Authentication**

There are two types of eye scan technologies which are used for authentication purposes: retinal scans and iris scans. In the retinal scan technology retina of an individual is used for his/her identification. Retina is the surface on the back of the eye that processes light entering through the pupil. The basis of this technology is blood vessel pattern in the retina of the eye, which forms a unique pattern. This blood vessel pattern in the retina of an individual can be used as tamper proof personal identifier. The pattern of the blood vessels is unique and stays the same for a lifetime. However, it requires about 12-15 seconds of careful concentration to take a good scan. Retina scan is often used in military and government organizations for identification.

- **Iris Scan based Authentication**

An iris scan also provides unique biometric data that is very difficult to duplicate and remains the same for the entire lifetime. Iris scanning biometrics measures the unique patterns in the colored circle of the eye to verify and authenticate the identity of an individual. After scanning the encoding of iris scan biometric data is performed in such a way that it can be carried around securely in a convenient format for further storage and future matching.

- **DNA Profiling**

Among the various known types of biometric traits, deoxyribonucleic acid (DNA) is the most reliable personal identification biometric trait. DNA is the genetic material found in most organisms, including human beings, and remains unchanged during a person's life or even after the death. DNA based identification is the most accurate biometric technology that never fails. DNA can be easily found in the blood, urine or any other liquid that comes out from a human body. The results of a DNA test are very fast and can be obtained within one to two hours.

DNA profiling is a technique that is used to identify and compare sets of DNA. It is now used for many purposes but forensic is the major area where it is mainly used.

- **Vascular Pattern Recognition**

Vascular or vein pattern recognition is another method of biometric authentication that uses pattern recognition techniques based on the images of human finger or palm's vein patterns under the skin. Layout structure of veins of a person is a biometric trait which is completely unique and can be used for the identification purpose. Even the twins don't have the same vein pattern. This biometric trait has advantage that it is very difficult to copy or steal, because they are visible under tightly controlled circumstances. Specialized scanners are used to light up the veins with the help of infrared light for capturing the vein pattern of a person for further processing and storage.

Behavioral Biometric Authentication Techniques:

- **Signature based Authentication**

Signature is another example of biometric data that is easy to gather and verify. Digitized signature verification is designed to verify the identity of individuals based on the traits of their unique signature. As a result, individuals who do not sign in a consistent manner may have difficulty enrolling and verifying in signature verification.

- **Voice Recognition System**

Like face recognition, voice biometrics also provides a way to authenticate identity even without the knowledge of an individual. Voice recognition systems are also known as **speech recognition systems**, where a computer software and hardware are used for capturing, processing, decoding, storing and matching the human voice for the authentication purpose. This authentication technology work by analyzing the captured voice sample of an individual for its unique characteristics, then matching is performed with the already stored voice samples to carry out the identification process.

- **Keystroke Dynamics**

It is the automated method of verifying the identity of an individual based on the way and rhythm of typing on a keyboard. While typing a series of characters, the time a person takes to find the right key and the time he/she holds down a key is specific to that person, and can be calculated in such a way that it is independent of overall typing speed. The rhythm with which some sequences of characters are typed can be person dependent.

VI. Advantages & Disadvantages Of Biometric Authentication

Biometric authentication methods have many advantages over the traditional techniques of authentication. Some major advantages of these systems are as under:

- Fully Automated Process
- Can't be Lost or Forgotten like other Credentials
- Provide more Reliable Service at Lesser Cost
- High Operational Availability
- Highly Difficult to Forge and Repudiate
- Full Compliance with KYC and AML Guidelines
- Remote Installation and Authentication
- Quick and Easy to Add New Users

Disadvantages of Biometric Authentication:

Although biometric based authentication systems have many advantages over the classical techniques, even then these systems are not 100% accurate, reliable and secure. These can also be spoofed, hacked or breached but more sophisticated tools and techniques are required to do so.

- Devices used in some biometric techniques like retina scan, iris scan and DNA profiling are very costly and sophisticated, so technical expertise is required to operate these systems.

- Like other traditional methods of authentication e.g. password or PIN, it is not possible to change or recover once it is compromised.
- The face recognition systems can be obstructed by wearing hat, hair, glasses or scarves etc.
- In voice recognition systems, illnesses related to throat can make it hard for a legitimate user to get access to the services.

VII. Applications of Biometric Authentication Systems

Authentication service is the core component of every system that needs some kind of security. Applications of biometric systems can be broadly divided into three main areas.

- **Commercial Applications:** It includes computer network logins, e-commerce, ATMs, electronic data security, credit cards, physical access control, personal gadget security and distance learning.
- **E-governance Applications:** such as Identity cards, driving licenses, passport control, social security, border control and disbursement in welfare schemes.
- **Forensic Applications:** It includes criminal investigation, terrorist identification, parenthood determination and missing children identity proving.

VIII. Issues In Biometric Authentication Systems

As the biometric data is extremely personal and unique so, there can be severe consequences of stolen biometric data than that of stolen passwords or tokens. Uniqueness of biometric traits is their major strength as well as the same property is their major weakness also. Once biometric trait of a person is scanned it generates a unique pattern of highly personalized data. If this data is stolen or compromised, it is not like something which we can change very easily. Once the biometric data is compromised, the identity of that individual at stake forever. One more issue is that the current biometric scanners still can't differentiate between the whether the fingerprint is on the real finger or is on the emulated one. Similarly voice and facial recognition systems sometimes fail to recognize legitimate user and allow the illicit person due their technical flaws.

Attacking techniques are also getting advanced in parallel with the advancements in security technologies so, major issues with the biometric authentication systems are related to the security of biometric data, which is the mainly related to the data and information security.

IX. Trends In Biometric Authentication

In the unimodal authentication systems, where the identification process is carried out by capturing and comparing only one biometric trait, there are many issues like noise or trait variation. So to enhance the accuracy of biometric authentication systems, a new trend called multimodal biometric authentication is preferred over the unimodal one. Multimodal biometric authentication system takes input from two or more biometric devices by capturing the different biometric traits to increase authentication accuracy.

A single device can also be used for capturing more than one biometric traits in one go. Multimodal solution with both fingerprint and finger vein modality is used for capturing the fingerprint and vein pattern simultaneously in a single scan. Similarly fingerprint and hand geometry multimodal systems are combined together for better accuracy and more reliability.

These multimodal systems are more accurate and robust. For example in a harsh industrial environment where workers are expected to have cut on their fingers, only having fingerprint based solution may not be an ideal biometric system.

X. Conclusion

With the advancement in technology things are getting more accurate, fast, reliable and secure. As the authentication is one of the most important security service, which is necessary for ensuring the proper access control on data and services. Biometric based authentication methods have changed the landscape of entire identification and authentication technology arena. It has made authentication process difficult to spoof, forge or repudiate. On the other hand it has made the authentication process more reliable.

References

[1]. [1]Prabhakar, Salil, Sharath Pankanti, and Anil K. Jain. "Biometric recognition: Security and privacy concerns." *IEEE security & privacy* 99.2 (2003): 33-42.

[2]. [2]Jain, Anil K., Arun Ross, and Sharath Pankanti. "Biometrics: a tool for information security." *IEEE transactions on information forensics and security* 1.2 (2006): 125-143.

[3]. [3]Le, Chien, and R. Jain. "A survey of biometrics security systems." *EEUU. Washington University in St. Louis* (2009).

[4]. [4]Lai, Lifeng, Siu-Wai Ho, and H. Vincent Poor. "Privacy–security trade-offs in biometric security systems—Part II: Multiple use case." *IEEE Transactions on Information Forensics and Security* 6.1 (2011): 140-151

[5]. [5] Dharavath, Krishna, F. A. Talukdar, and R. H. Laskar. "Study on biometric authentication systems, challenges and future trends: A review." *Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on*. IEEE, 2013.

[6]. [6] Adámek, Milan, Miroslav Matýsek, and Petr Neumann. "Security of biometric systems." *Procedia Engineering* 100 (2015): 169-176

[7]. [7] "Biometric news portal" UK 2017http://www.biometricnewsportal.com

[8]. [8]PBworks, “Authentication technologies”,

[9]. http://biometrics.pbworks.com/w/page/14811351/Authentication%20technologies

International Journal of Engineering Science Invention (IJESI) is UGC approved Journal with Sl. No. 3822, Journal no. 43302.

Pawan Kumar.“ A Review of Emerging Biometric Authentication Technologies” International Journal of Engineering Science Invention (IJESI), vol. 07, no. 02, 2018, pp. 16–21.