Biometrics as a Security System - An Overview

Mrunali Chaure Prof. Amit Sahu

Abstract- **Biometrics are an important and widely used method for identityverification and accesscontrol for providing in today’s growing computing world.A biometrics is in general term used to describe a measurable physiological and/or behavioral characteristic that can be used for automated recognition of an individual based on the individual's physical and behavioralcharacteristics. As biometric data is data inherent to one's body, and usually is unique to an individual, it can be used to recognizeindividual’sbiometric characteristics, such as fingerprint, face, retina, DNA, ECG and Voice, signature, and many others, for automatically computerized recognition systems. Biometric systems are commonly used to control access to physical assets like laboratories, buildings, and cash from ATMs, or logical information like personal computer accounts, secure electronic documents.It also determine whether a person is already in a database, important for social service or national ID applications some of which are daily concern.In this system, one neednot necessary to remember like passwordsand are not easily lost or forged likeidentifying documents. However, it is also true that, biometrics are fundamentally noisy and irreplaceable. The proliferation ofbiometric usage raises critical privacyand security concerns due to the noisy nature of biometrics. In this article, we present an overview of *Biometrics* system and along with its security measures.**

*Keywords:***Biometrics, Physical biometrics, behavioral biometrics, Spoofing, Mimicry, Security.**

I. INTRODUCTION

Biometrics refers to metrics related to human characteristics for authentication and access control is widely used in many computer science applications [1]. The distinctive, measurable characteristics of multiple sensors or biometrics identifiers are used to label and describe individuals. Access control include for token-based identification systems, such as a driver's license or passport. It also useful for knowledge-based identification systems, which includes a password or personal identification numberwhich are sometimes useful for, identifying individuals in groups that are under surveillance [2]. Foran individuals, biometrics are more reliable in verifying identity than token and knowledge-based methods; But in addition to this positive secure side, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information [5].

We can state the biometrics as, “Biometric technologies are automated methods of verifying or classifying or recognizingthe identity of a living person based on a physiological or behavioral characteristic” [4].The two keywords and two characteristics in this definitionas: “automated” and “person”, “physiological” and “behavioral”which describe the Biometric technique in detail.

The word “automated,” relates to the field of Biometric as, thisBiometrics authentication techniques aredone completely by machine, therefore differentiates it from the larger field ofhuman identification science. The techniques, such as latent fingerprint, DNA, hair andfiber analysis, etc. are not consideredas a part of this field. The biometric authentication is mainly subject to living humans; in contrast, the automatedidentification techniques can be used on animals, fruits and vegetables,manufactured goods, etc.

The second keyword is “person”. Some techniques like, fingerprint patterns, Face Recognition, Thumb Recognition, etc, have been used for differentiate or for connectgroups of people [4] or to probabilistically link persons to groups, butbiometrics is interested mainly for recognizing people as an individuals.

Biometric identifiers are often of two characteristicsthat arephysiological and behavioral [3].Physiological characteristics are mainly related to the shape of the body such asfingerprint, hand geometry,face recognition, palm veins, DNA, palm print, iris recognition, retina and odor/scent. The Behavioralcharacteristics involves that are describe by some researchers as the latter class of biometrics, whichare related to the behavior of a person, including typing rhythm, signature and voice. Both of these Physical and behavioral characteristics are not limited to these given characteristics and increasing in their field. In recent times, biometrics based on brain (electroencephalogram) and heart (electrocardiogram)[7] signals have also been emerged.

All of themeasures used for authentication mainly contains both physiological and behavioral components, both of these components can vary widely and it is in very rare situation across a population ofindividuals that it is similar [6]. So, biometrics is the use of computers to recognizepeople, instead of all the across-individual similarities and differences. It is not possible by using these Biometric techniquestodetermineexactly “true” identity of all the individuals, which seems as beyond the scope of anybiometric technology.Biometric technology can only link a personto a biometric pattern and any identity data like common name and personalattributes such as age, gender, profession, residence, nationality, etc, that are presented at thetime of enrollment in the system. As, Biometric systems inherently require noidentity data, hence allows anonymous recognition.

II. LITERATURE REVIEW

Thesecharacteristics and traits of biometrics are used to identify each human. All the details of the human body normally differs from one human to otherwill be used as unique biometric data to serve as that person's unique identification (ID) for that person,Biometric identification is used in many other places throughout the world. The scientific literature on quantitative measurement of humans for the purpose of identification dates back from 1870s and the measurement system of Alphonse

Bertillon [8].The earliest cataloging of fingerprints [12]before the date of 1891 when Juan Vucetich started a collection of fingerprints of criminals in Argentina. Thedevelopment ofdigital signal processing techniques in the 1960s led immediately to work inautomating human identification.Henry Faulds, WilliamHerschel and Sir Francis Galton proposed quantitative identification with the use ofaszwere developed in the 1990s.

In earlier time around 1960s, [14] the potential applicationof this technology to high-security access control, personal locks andfinancial transactions was recognized.In 1970s the development and deployment of hand geometry systems starts testing and increasing interest in government use of these“automated personal identification” technologies andbiometrics is defined as the unique personal, physical/logical characteristics or traits of human body [18].

The first time someone uses a biometric scanner,the scanner performs an enrollment [20]. During enrollment,the system will store the user's biometric information to bematched them on future uses. In the today’sworld, there are numerous uses for biometric identification, and all of them have their own strengthsand weaknesses in terms of security and features.In February 2011, India started theirUniversal ID program. The goal of the program is to provideeach of India's 1.2 billion people with a unique identification number[20] called ‘Aadhaar card’. In addition, the United States uses fingerprints to identify immigrants and many hospitalsuses some form of biometrics to validate that a patient iswho he or she claim to be.

III. BIOMETRIC CHARACTERISTIC

The ideal biometric characteristichas five majorqualities, which are also essential that are robustness, distinctiveness, availability, accessibilityand acceptability [16].

1. Robustness - This characteristics approves us about unchanging on anindividual over time.
2. Distinctiveness - This mean showing great variationover the population.
3. Availability- Thischaracteristics stats that the entire populationshould ideally have this measure in multiples.
4. Accessibility -This means it is easy to image using electronic sensors.
5. Acceptability -By these characteristics, we mean thatpeople do not object to having this measurement taken from them.

Some biometric characteristics are clearly moreappropriate than othersfor any particular application. However, it is also essential for any System administrators who is wishing to employ biometric authentication need to articulate clearlythe specifics of their application so that he can apply all above characteristics to his biometric applications.

IV. DIFFERENT TYPES OF BIOMETRICS

A. *Physical biometrics*

1. Fingerprint - It is based on the analysis of our fingertip patterns.
2. Facial recognition/face location - Measuring facial characteristics
3. Hand geometry - It Measures the shape and characteristics of the hand
4. Iris scan - it analyzes features of the colored ring of eye. One of the thing, which seems like unbelievable about human, which support this type of geometry [2], is that Iris patterns are started to formed in the eighth month of age of an individual and, remain stable throughout the life.
5. Retinal scan - This scans analyzes the pattern of blood vessels, which are present at the back of the eyeball.
6. Vascular patterns - It is based on analysis ofpersons vein pattern.
7. DNA - Analyzing genetic makeup of the human body.
8. Ear print - This method is based on geometric distances, force field transformation.

As people have certain distinct brain and heart patterns that are specific for each individual, the recent advancement in biometrics based on brain (electroencephalogram) and heart (electrocardiogram) signals have been emerged. Comparing to conventional biometrics like fingerprints,it is more advantages the use of such 'futuristic' technology,as it is more fraud resistant. But the downside of such technologies is, generally more cumbersome and still has issues such as lower accuracy and poor reproducibility over time.

B. *Behavioral biometrics*

1. Speaker/voice recognition - This system Analyzes vocal behavior and differences such as in pitch, and tone.
2. Signature/handwriting - It analyzesdynamics of signature.The characteristics of signature involvesacceleration,total time, speed, character direction, stroke order , pressure and contact with the writing surface are analyses by this technique.
3. Keystroke/patterning - This system measures the time spacing of typed words, i.e. typing on the keyboard.

V. ADVANTAGES AND DISADVANTAGES OF BIOMETRICS

A. Advantages

1. The first advantage of using this new technology is the uniqueness, which allows biometrics technology to become more and more important. With uniqueness, each individual's identification will be single, most effective identification for that user, as the same identification of an individual in the biometric security technology system is nearly zero.

2. It eliminates problems caused by lost IDs or forgotten passwords by using physiological attributes. It prevents unauthorized use of lost, stolen or "borrowed" ID cards and reduce password administration costs. This system replaces hard-to-remember passwords by any of the person's physical and behavioral characteristics, which cannot be shared or observed.

3. This identification i.e. (ID) of users though biometrics cannot be lost, stolen or forgotten as our normal password. This aspect of biometrics technology allows it to become more popular in its use [16]. It also, integrate a wide range of biometric solutions and technologies, applications of customer and databases into a robust and scalable control solution for facility and network access. By using this technique it becomesmakes possible, to know WHO did WHAT, WHERE and WHEN!

4. It Provides Increase security by a convenient and low-cost additional tier of security. Biometric reduce fraud by employing hard-to-forge technologies and materials. Example includes minimizing the opportunity for ID fraud, buddy punching. It is extremely hard or impossible to make duplicate or share biometrics-accessing data with other users. This provides it ever more securityto user information and data to kept highly secure from unauthorized users.

5. This system offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time & Attendance. The most biometrics security systems are easy to install and it requires small amount of funding for equipment except modern biometrics technology such as: DNA/retinal/iris recognition, etc.

B. Disadvantages:

Instead of there are many advantages of biometrics security system, it still has some flawsin its system [18].Most of each biometricsmethod has weaknesses, which can cause problems for its users.

1. If the biometrics security system is using fingerprints to identify its users and if an accident causes a user of the system to lose his/her finger then it can be a problem during the verificationprocess.
2. For voice recognition methods, illnesses such as strep throat or weakness that causeone is unable to speak in its popper voice can make it hard for authorized users to get access for his/ herinformation. Another factor that also influence voice recognition systems is the continuous aging of its users. This system also suspect to Noisy environment.
3. For iris or retinal scanning applications, users may find it very intrusive. They may also have the concern for the safety of theireyes during the iris or retinal scan, as the light at the time of scanning can be unbearable by any person with week eyesight. Furthermore, databases used to store user identification data will be very large which leads to potential threat. New and modern technology are vital required for proper retinal/iris characteristics scanning and storing large amount of database. Which results in more cost for equipment used for this.
4. Finally, many people are still concerning about biometrics technology in different aspects such as security, adaptability to rate of change in life, scalability,accuracy, privacy and others.

VI. SECURE BIOMETRICS

In today's world, advances in technology have made life easier by providing us with higher levels of knowledge through the invention of different devices. But at the same time, each technological innovation harbors the potentially hidden threats to its users. As digital data become more prevalent, its necessary for users to secure theirinformation with highly encrypted passwords and ID cards. Instead, the misuse and theft of these security measures are also increasing. This increasing battle with cyber security has led to the birth of biometric security systems which provids access control and authentication. There is a combination of biometric data systems and biometrics recognition / identification technologies, whichcreates the biometric security systems. The relationship between the between these two systems is also known as the lock and key system, As the biometrics security system is the lock and biometrics is the key to open that lock [17].

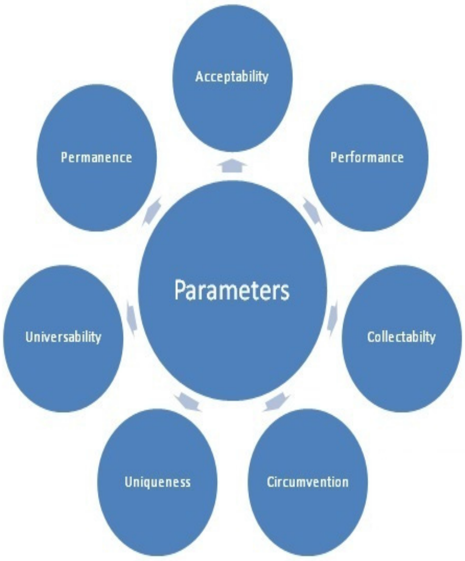

Fig.1 - Basic Criteria for Biometrics Security System

There are seven basic criteria for biometric security system that are: uniqueness, universality, permanence, collectability, performance,acceptability and circumvention which is also shown in fig.1above followed by its descriptions [18].

1) Uniqueness – It is considered that priority requirementfor biometric data,which will be able to recognize single user

amonggroups of users, this can beindicated differently and uniquely by the biometric system. For e.g., the DNA of each person is unique.

2) Universality – This is the secondarycriteria for the biometric security. The parameter indicates requirements for unique characteristics of each person in the world thatcannot be replicated. For e.g., retinal and iris are characteristics will satisfy this requirements.

3) Permanence – This third parameter is required for every single characteristic or trait. This is recorded in the database for that system and needs to beconstant for a certain period of time. This parameter will mostly affected by the age of the user.

4) Collectability - The collectability parameter requires the collection of each characteristic and trait bythe system in order to verify their identification.

5) Performance –This is the next parameter for the system, whichdenotes how the security system workswell. For the biometric security system,the accuracy and robustness are main factors.Performance of the biometric security systemis decided by this factor.

6) Acceptability – This parameter will choose fields in which biometrictechnologies are acceptable.

7) Circumvention – This final parameter will decide how easily each characteristic provided by the user can becomefailure during the verification process. DNA is believed to be the most difficult characteristic leading to the failure of theverification process.

Individual-unique biometric information based on their different characteristics like fingerprints, retinal or iris patterns; facial patterns voice prints, biometrics used with card technologies. Biometric information stored on the ID card and verified with actual biometric at point of interaction which provide additional level of security compared to traditional levels as shown in following fig.2 [19]:

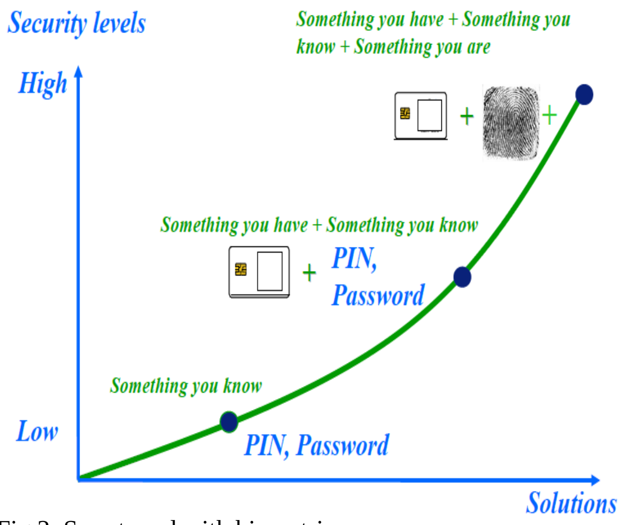

Fig.2. Smart card with biometrics

VII. Types of adversary attacks and their possible solution:

There are many types of adversary attacks, the most basic of which involves spoofing, Mimicry, directly manipulating the biometric scanner, etc. However, these attacks can be attacks on the software as well.

A. Spoofing

Spoofing with artefacts is generally a concern for physiological biometrictechnologies such as fingerprint, hand, iris etc. Spoof attacks consist in submitting fake biometric characteristics to biometric systems, and are a major threat that can provide threats to their security [21]. Multi-modal biometric systems used for multiple scanare commonly believed to be intrinsically more robust to spoof attacks.

On technical solution to detect or reject, the functionality is usually termed *liveness detection*, which refers to the ability of the system to distinguish between a sample feature provided by a live human being and a copy of a feature provided by an artefact. One is the specific detection of known spoofs e.g.silicon and gelatin fingerprint spoofs, forgery photograph of face etc. The other is necessary to look forexplicit signs of liveness in the presented biometric feature.

B. Mimicry

Through mimicry, one can attempts to "copy" the relevant biometric features of anenrolled user so that he can make the manipulation in the biometric authentication process. Becausebehavioral biometrics are applicable to the recognition of acquired, rather thaninherited features, the features can also be acquired by an impostor. Impostors are unlikely attempt to mimicry attacks against biometric systems that completely or predominately utilize physiological features such as fingerprint, iris, etc. Because mimicry may be perceived to bea low technology form of attack requiring a lower level of expertise, biometric systemsemploying behavioral biometrics may be subject to a higher incidence of attacks froma wider range of attackers.

As mimicry does not involve the use of an artefact like spoofing attack, *liveness detection* is not generally applicable as possible solution for mimicry. Counter-measures should focus on the ability to distinguish between a genuine person and a mimicker. This attack include improved technical performance, supervised operation and challenge/response features present.

C. Insider Attacks

This form of attack is provided to biometric system by those who directly Operate that system [22]. Such attacks may be accidental, for instance,the owner of the system neglecting to validate credentialsa potential user provides and failing to authenticate thatusers are actually is this. However, insiderattacks can also be caused by the owner or operator of thesystem intentionally allowing an unauthenticated person toauthenticate, or allowingan unauthorized person access to the system.Such attacks are outside the scope to handle, as theydeal with personnel management instead of software or hardware solutions.

One method of protecting a scanner is to increase the physical security present. This can include adding a person orcamera watching the scanner, or requiring a password to access the scanner. This however would defeat the purpose of biometric identification, and which is not recommended. Because these methods do not involve the biometric system itself. However, it is oftentimes trivial to get around these methods, so while the use of them can help, a determined attacker should not have any difficulty bypassing them

D. Non-secure Infrastructure

This kind of attack includes any attack, which involves manipulating the data being passed at any point in the authentication process after the scan has been made. These attacks usually involve finding security breaches in either the database where the users' authentication data is stored or security breaches in the data itself, such as poor data encryption.

One of the simplest methods of preventing a physical attack is to add complexity to your scanner. In order to protect against false fingerprints or retinal scans, a heat sensor could be used to ensure that a real finger or eyeball is being used [23]. A signature scanner could include a pressure pad to ensure that a user is not trying to trace a copy of someone's signature.

E. Biometric Overtness

This method of attacking involves tricking the biometricscanner itself into incorrectly identifying the user as an authorized person. Examples of these include using lifted finger prints, making a gummy eyeball, or attempting to mimicsomeone's gait.While this is the most basic security issue in biometric passwords.This can be reduce by providing security by adding physical security, by adding cameras or possibly by using sensors.

F. Middleware / software of biometrics security

Middleware and software for biometrics security system provides the link between services and instructions by making use of multiple processes. The middleware is a useful component as it helps the biometrics devices and the database to run effectively across the network. Biometrics devices and the computers together are connected together by. Middleware and software also connects, while working compatibly with each other on the network. Further, integral part can be form by the software and middleware used by the biometrics systems to the efficiency and effectiveness of the whole biometrics security system. This system is flexibile to bind all the applications which are located at the database/server to any biometrics devices at the verification location [23].

VII. Conclusion

In summary, biometrics technology is a new technology for most of us because it has only been implemented in public for shortperiod of time in advance sectors. There are many characteristics mainly based on physical and behavioral are most effective for its development. Along with this, there are many applications and solutions of biometrics technology used in security systems. This paper presents manyadvantages, which can improve our lives with improved security and effectiveness, reducing fraud and also costs of password administrator, ease of use and makes live consisting of some daily concern more comfortable along with some disadvantages needs to be overcome. Even though the biometrics security system still has many concerns such asinformation privacy, physical privacy so it is our need to provide solution for security concern so that we will make our living standard more better in today’s computing and advanced world.

References

[1] "Biometrics: Overview". Biometrics.cse.msu.edu. 6 September 2007. Retrieved 2012-06-10.

[2] Jain, A., Hong, L., &Pankanti, S. (2000). "Biometric Identification". Communications of the ACM, 43(2), p. 91-98. DOI 10.1145/328236.328110

[3] Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2.

[4] James Wayman, Anil Jain, DavideMaltoni and Dario Maio, “An Introduction to Biometric Authentication Systems” Springer Journal , (Eds) 2005.

[5]Weaver, A.C. (2006). "Biometric Authentication". Computer, 39 (2), p. 96-97. DOI 10.1109/MC.2006.47

[6] Ashraf El-Sisi, “Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filtere”, The International Arab Journal of Information Technology, Vol. 8, No. 4, October 2011.

[7] R. Palaniappan, and S. M. Krishnan, “Identifying individuals using ECG signals,” Proceedings of International Conference on Signal Processing and Communications, Bangalore, India, pp.569–572

[8] C. Beavan, Fingerprints: The Origins of Crime Detection and the Murder Case that Launched Forensic Science. Hyperion, New York, 2001.

[9] H.Faulds,On the skin furrows of the hand. Nature, 22, 605,October 28, 1880.

[10] A. Rosenberg, Automatic speaker recognition: a review. Proc. IEEE, 64(4),475–487, 1976.

[11] M. Trauring, Automatic comparison of finger-ridge patterns. Nature, 197,938–940, 1963.

[12] A. Fejfar and J.Myers, The testing of 3 automatic ID verification techniques for entry control.2nd Int.Conf. on Crime Countermeasures,Oxford,25–29 July, 1977.

[13] R. Chellappa, C. L.Wilson and S. Sirohey,Human and machine recognition offaces: a survey. Proc. IEEE, 83(5), 705–740, 1995.

[14] J.D.Daugman,High confidence visual recognition of persons by a test of statisticalindependence, IEEE Trans. Pattern Analysis andMachine Intelligence, 15(11), 1148–1161, 1993.

[15] J. Wayman, Fundamentals of biometric authentication technologies. Int. J.Imaging and Graphics, 1(1), 2001.

[16] Advantages of Biometrics: Why opt for biometric technology? [Online] available: http://www.questbiometrics.com/advantages-of-biometrics.html

[17] [Jain, 2006] Jain, A.K.; Ross, A.; Pankanti, S., "Biometrics: a tool for information security" Volume: 1 Issue: 2, Issue Date:June 2006, page(s): 125 – 143

[18] A Survey of Biometrics Security Systems [Online] available:http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/index.html.

[19] [Schuckers, 2001] Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001.

[20] Wikipedia. Biometrics | wikipedia, the free encyclopedia.[Online]available:http://en.wikipedia.org/w/index.php?title=Biometrics&oldid=419298116, 2011.

[21]Anthony Delehanty, "Security Issues in Biometric Identification",University of Minnesota, Morris

[22] Kim, W., and Lee, H. Multimodal biometric image watermarking using two-stage integrity verification.Signal Processing 89, 2 (2009), 2385 - 2399.

[23] Peter O'Neill; Anne O'Neill; Shaun Winters; Lucy Kwiaton "Biometrics security system", 2011 http://www.findbiometrics.com