International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 5, July-August 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Security Issues Related to Biometrics

Sushmita Raulo, Saurabh Gawade

Department of MCA, ASM Institute of Management & Computer Studies, Thane, Maharashtra, India

ABSTRACT

With the growth of technology their grows threat to our data which is just secured by passwords so to make it more secure biometrics came into existence. As biometric systems are adopted and accepted for security purpose for various information and security systems. Hence it is immune to attacks.

This paper deals with the security of biometric details of individuals. In this paper we will be discussing about biometrics and its types and the threats and security issues which is not talked about usually. The different technologies evolved and had contributed to biometrics in long run and their effects.

KEYWORDS: *security, biometrics, technology, data, cryptography*

How to cite this paper: Sushmita Raulo | Saurabh Gawade "Security Issues Related to Biometrics" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-5, August 2021, pp.1352-1356, URL: www.ijtsrd.com/papers/ijtsrd44951.pdf

IJTSRD44951

INTRODUCTION

Protection of individuals, their belongings, environment, etc., are all given utmost importance but in the era technology has added one more priority – protection of individual's data. Data collected through biometrics is collected, stored and utilized when it is needed. But as we all know there is a threat to anything out there in the world so do our data too. We as an individual working with technology have a responsibility to protect our fellow citizen's data.

Biometrics has opened a way through which we can identify a person's identity using his/her fingerprints, iris scan, face recognition and many more. Biometrics serves as a way for identification or verification of a person. But biometrics has also paved way for the hackers or the illegal tech practitioners to access data easily. As we are moving towards a digital era, we will be experiencing more of this security threats which we may be unaware of. [1]

Biometrics

The biometrics word has a large meaning in the study of identification's persons from a number of characteristics. A complex human inheritance, very rich in combinations, and perfectly adapted to such systems of user identification, and/or authentication. It's a Mathematical analysis of biological characteristics of a person to determine his identity decisively. Biometrics based on the principle of some characteristics recognition's. Fingerprints, face, iris, retina, hand, keystroke and voice, provide irrefutable proof of the identity of a person they are unique biological characteristics distinguishing one person from another.

Both identification and authentication differentiate the definition of the biometrics:

- Identification: The confirmation of the identity of the individual which is identity papers or automatic teller machines.
- Authentication: Identification of an individual from a quantity of biometric recorded people. This type of biometric recognition is especially used in the high fields with low number of users or ends of police investigation.

Types of Biometrics

1. Fingerprint Recognition:-

The use of the ridges and valleys (minutiae) found on the surface tips of a human finger to identify an individual.

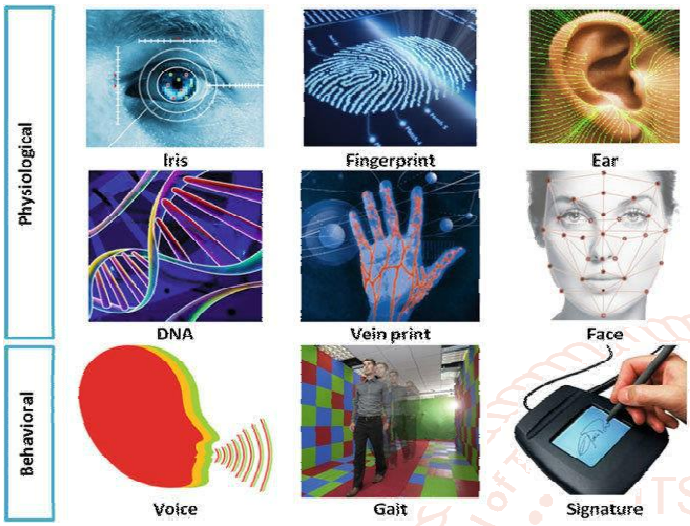
2. Face Recognition:-

The analysis of facial features or patterns for the authentication or recognition of an individual's identity. Most face recognition systems either use Eigen faces or local feature analysis.

3. Eyes:-

A. Iris Recognition- The use of the features found in the iris to identify an individual.

B. Retina Recognition- The use of patterns of veins in the back of the eye to accomplish recognition.



4. Ear:-

The identification of an individual using the shape of the ear.

5. Hand Geometry Recognition:-

The use of the geometric features of the hand such as the lengths of fingers and the width of the hand to identify an individual.

6. Typing Recognition:-

The use of the unique characteristics of a person's typing for establishing identity.

7. Voice - Speaker Identification:-

Identification is the task of determining an unknown speaker's identity.

Speaker identification is a 1: N (many) match where the voice is compared against N templates. Speaker identification systems can also be implemented covertly without the user's knowledge to identify talkers in a discussion, alert automated systems of speaker changes, check if a user is already enrolled in a system, etc.

8. Signature Recognition:-

The authentication of an individual by the analysis of handwriting style, in particular the signature. There are two key types of digital handwritten signature authentication, Static and Dynamic.

A. Static is most often a visual comparison between one scanned signature and another scanned signature, or a scanned signature against an ink signature. Technology is available to check two scanned signatures using advances algorithms.

B. Dynamic is becoming more popular as ceremony data is captured along with the X,Y,T and P Coordinates of the signor from the signing device. This data can be utilized in a court of law using digital forensic examination tools, and to create a biometric template from which dynamic signatures can be authenticated either at time of signing or post signing, and as triggers in workflow processes.

Biometric Features

1. Physiological biometrics.

Features notably identified through the five senses and processed by finite calculable differences: sight (how a person looks including things like hair and eye color, teeth, or facial features), sound (the pitch of a person's voice), smell (a person's odor or scent), taste (the composition of a person's saliva or DNA), and touch (such as fingerprints or handprints).

2. Behavioral biometrics.

Based on the manner in which people conduct themselves, such as writing style, walking rhythm, typing speed, and so forth.

For any of these characteristics to be used for sustained identification encryption purposes, they must be reliable, unique, collectable, convenient, long term, universal, and acceptable.

Principles of Biometrics

Although the various biometric technologies vary in what and how they scan, the principle of operation is very similar. Biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, and wherever the data is to be analyzed, a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data scanned when a user tries to gain access.

Verification vs. identification

Depending on the application context, a biometric system can operate either in verification or identification mode.

In verification mode, the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. 'Positive recognition' is a common use of

verification mode, where the aim is to prevent multiple people from using same identity.

In identification mode, the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person where the system establishes whether the person **is** who she (implicitly or explicitly) denies to be.

Performance of biometric systems

There are many characteristics which make it possible to compare the biometric systems. The following are the most used as performance metrics for biometric systems:

1. False Rejection Rate (FRR):

The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

2. False Acceptance Rate (FAR):

The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

3. Equal Error Rate (EER):

The rates at which both accept and reject errors are equal. The value indicates that the proportion of false acceptances is equal to the proportion of false rejections. The lower the equal error rate value, the higher the accuracy of the biometric system.

Identification and verification methods

To confirm the personal identity are used by different physiological characteristics and behavioral features. In practice there are constantly discovering new ways to measure the attributes and the uniqueness.

1. Hand

Measuring the physical characteristics of hand and fingers from a three-dimensional perspective
False Rejection Rate (FRR): 0, 1%
False Acceptance Rate (FAR): 0, 1%
Verification time: 1 as 2 second

2. Fingerprint

Optical, capacitive or thermal fingerprinting ("minutážne" body alebo tvar papilár)
False Rejection Rate (FRR): <1%
False Acceptance Rate (FAR): from 0, 0001% to 0, 00001% depending on type
Verification time: 0, 2 - 1 sec.

3. Face

Facial recognition
False Rejection Rate (FRR): <1%
False Acceptance Rate (FAR): 0, 1%
Verification time: 3 sec.

4. Eye

Iris scanning
False Rejection Rate (FRR): 0, 00066%
False Acceptance Rate (FAR): 0, 00078%
Verification time: 2 second
Other methods:

There are currently explored other methods of biometric identification and verification:

- Retina: the analysis of the capillary vessels located at the back of the eye
- Signature: the analysis of the way a person signs his name
- Ear: the analysis of ear shell shape
- Vein: the analysis of pattern of veins
- Voice: the analysis of the tone, pitch, cadence and frequency of a person's voice

Vulnerabilities of biometrics

Biometric systems as an authentication measure is attractive because they are unique and measurable and they cannot be easily stolen and shared with others. As we know biometrics are unique but their representation may vary during measurements. The variations may be natural or man-made i.e., a technical error or human intervention. The variations may lead to a vulnerable situation. A vulnerable situation is occurred when an unauthorized user gets access to the data. A biometric system while acquires, processes, stores and helps matching the data in the meanwhile it causes the system to be vulnerable with lack of accuracy, reliability, robustness against fraudulent attacks, secrecy of biometric data and privacy protection.

Some methods to alter the data are like synthetic reproduction of anatomical identities(acquisition of facial images or lifting of latent fingerprints) and the imitation of behavioral identities(reproduction of handwritten signature or producing similar voices), replaying stored information or producing false information in the processing chain or spoofing the system with new or raw data are some of them.

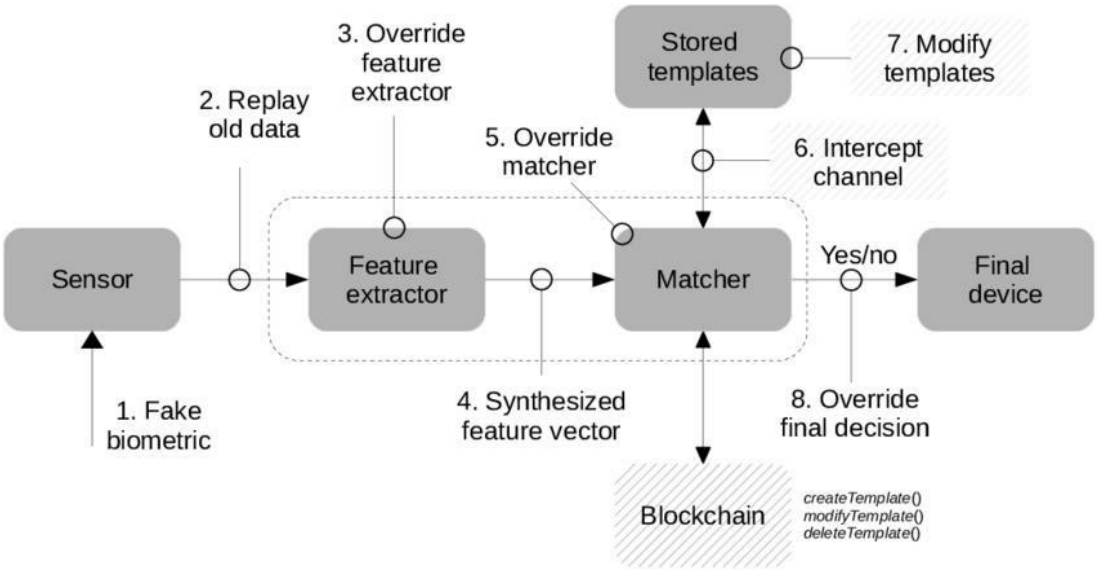


Fig 1 Vulnerabilities of biometric system

Vulnerabilities often call for threats in a biometric system which can be classified as faults, failures and security attacks.

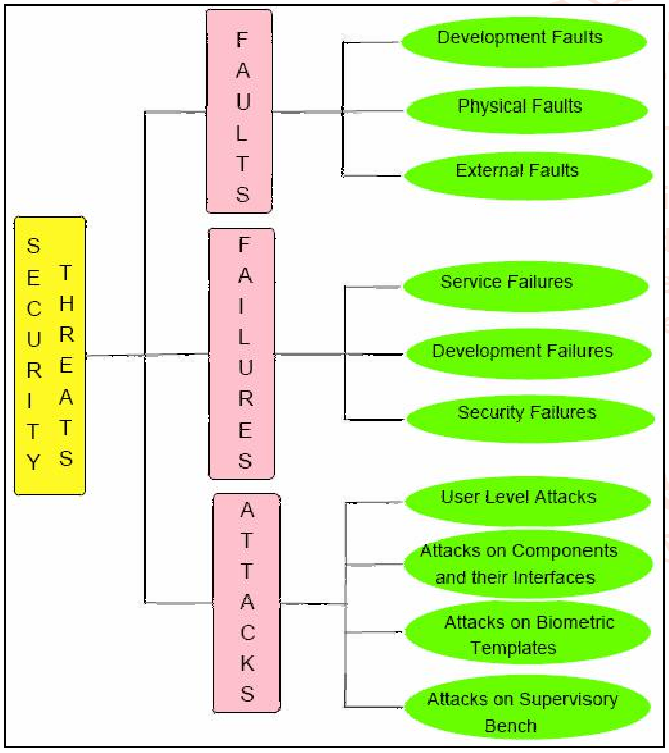


Fig 2 Vulnerability threats

Security of biometric system

A biometric system can directly be attacked on machine or the man who is supervising the machine. Biometric system attacks can be classified as direct and indirect attacks according to Martinez-Diaz et al. (2011). Indirect attacks require the information of the development phase e.g., data representation which is in order to done to impersonate a real user. Indirect attacks include attacks on template database or on the communication channel as reported by Ratha et al. (2001). [2]

According to Cappelli et al. (2007) the most common attack is stealing biometric templates and that is spoofing and manipulating the data for use. In generic encryption methods like AES, RSA, etc. the templates can be vulnerable in each of the recognition transaction during decryption because the templates maybe unprotected during encryption. (Nagar et al., 2008). [3]

Biometric when combined with cryptography adds the strength to both fields. [4] Symmetric cryptosystem are very strong for attacks but the weakness lies in our symmetric cryptosystems is regular attempt of cracking the system through different passwords i.e., brute forcing the secret key. [5]

Conclusion

Safety of our biometric systems is the need of the hour. A company or organization should have a solid, effective and accurate biometric system to ensure that their data is safe. As discussed above one should be aware of the threats related to biometric data he/she submits as there are many fraudulent activities are carried out on the of well recognized institutions or offices.

References

[1] Drahansky, M.: Fingerabdruckerkennung mittels neuronaler Netze, Diploma thesis, 2001

[2] Smolik, L., Drahansky, M.: Exploitation of smart cards and human biometric attributes, CATE, 2001

[3] Yogendra narain Singh, Sanjay Kumar Singh, "A taxonomy of biometric system vulnerabilities and defences, Int. J. Biometrics, Vol. 5, No. 2, 2013.

[4] Edwin T. L. Rampine, Cynthia H. Ngejane, "A brief overview of hybrid schemes for biometric fingerprint template security", ICISSP 2016 – 2nd International Conference on Information Systems Security and Privacy

[5] Alisher kholmatov, Berrin Yanikoglu, "Biometric cryptosystem using online signatures", Computer and Information Sciences – ISCIS 2006.

[6] Mohammad Shahnawaz Nasir, Prakash Kuppuswamy Perumal, "Implementation of biometric security using hybrid combination of RSA and simple symmetric key algorithm", International Journal of Innovative Research in Computer and Communication Engineering, Vol.1, Issue 8, October 2013.