ISSN: 0975-766X
CODEN: IJPTFI
Available Online through ***Research Article***
www.ijptonline.com

SURVEY ON ISSUES AND CHALLENGES IN BIOMETRIC-BASED AUTHENTICATION

Aditya Shivhare[1], Saurabh Kumar Pradhan[2] Manivannan S.S[3]
1 2 3 SITE, VIT University, Vellore, India.

Received on 25-10-2016 *Accepted on 02-11-2016*

Abstract

With the latest trend of using biometric based system for authentication leads to increase in challenges and threats in technical world. In the world of Information and data, security is our major concern to protect data. In this paper we are going to discuss all the technical challenges and issues and concerns in biometric authorization technology with the logical and physical presence to access the data. The survey includes importance on performance of the system with regard to robustness and tactics of recognizing biometric authentication. In this paper we will also add one of the way to keep the data secure. The overall discussion of the paper is going to gain deep understanding on our topic.

Key words: Biometric, data security, authorization, security breach, robustness, tactics.

Introduction

Biometric verification to authenticate someone is one of the most latest and exciting technical technique of recent time and seems to change the way lifestyle and security in today's people. In Today's world data is one of the format in which record and save our details so security of data is one of the important topic for purpose of security in modern world otherwise it will be misused or manipulated by someone for causing harm to someone or for their benefit. For authentication use of biometric system and issue occurred during it are most widely common. This paper deals with the problems which are faced during the authenticating and mismatch faced being genuine person and the method made conducted during matching and authenticating the person using its figure imprint. In the end we will recommend the idea of improving the issues faced and will give recommendation and suggestions for future implementation and research.

ComponentsIn Biometric System

System of biometric operation carries out in two phases i.e. recognition phase and enrolment phase. It involves biometric sensors such as fingerprint scanners, microphones, cameras to analyze specific person imprint and the covert the sample

input to relevant digital format. After that necessary details are fetched from that after that some preprocessing module which exist between the two modules are used to remove the interference and noise and then store in the database in appropriate These Biometric recognition software performs some modules of comparison and authenticate based on "really it is you who claimed to be". The identifier software involves user identification and database records. The main motive of identification is to get the nearest matching identity, if found. Physical and logical both access involves verification to have positive recognition of the person and avoid unwanted user to use the same identity. Identification module is used to overall authenticate and measure performance.

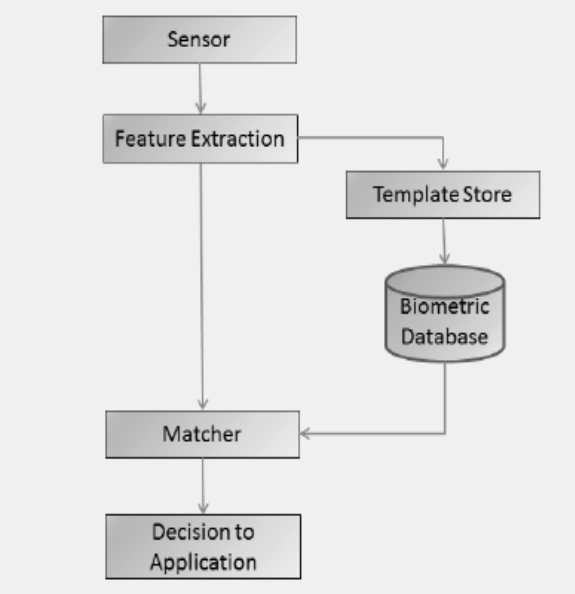

Fig-1 Traditional Biometric Procedure.

Security Involved in data of Biometric System

This biometric system involves components like database storage, communication and recording data .Once Biometric information is captured in buffer memory it can be misused for false authentication. As biometric data give details and provides information about a person. Its protection is itself a big issue various security measures are taken to protect biometric theft. There are some of types of attacks performed on it such as snooping attack by connecting USB ports and capturing data by connecting it to the system and other means is internal attack on the modules of a biometric system through jammer on media.

Attacks in biometric system

Vulnerability of Biometric system depends on the databases. Reports are been generated that various hackers have designed software with their intelligence and tactics with which they perform theft by stealing and breaking the security

of biometric system there are some the types of theft performed like spoofing attack in which they enter the network of database records by just connecting through there hacking tricks and steal the record from the database which they modify and use it for causing harm to others. Other Attack is some internal module attack in which they make some changes in the internal modules of the software of biometric and make it to work as per there desired order to capture the details of biometric when someone tries to use it for his authenticity later that copied record is used by that hacker or some third party to enter the system with false identity.

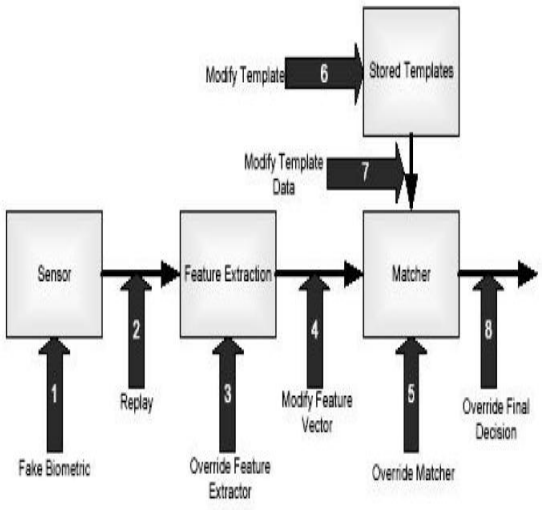

Fig2 – Points from where attack is possible.

Measurement of Biometric accuracy

1.) RFM (Rate of False Match)

Rate of false match or acceptance rate act as a interrupt in identification of the person authenticity it lowers the security and increases the rate of risk in getting the identification match of the person. The better the Security in biometric authenticity lower the Rate of False Match.

2.) Same Identity problem

Two Different identity of the individual person is by mistake to have same imprints.

3.) NMFR (Non-Match False Rejection rate)

False Rejection Rate, lowers the NFMR system easier is the system to use. It Includes making the biometric details of two person as an individual person identity by mistake. All biometric system work in the same manner but main part is that the quality of success of biometric system with suitable strengths and weakness in the methodology of biometric system.

Some Problems faced in Biometric Authentication

- Uniqueness of the figure prints should be there.
- Maintaining Database of lots of figure imprints.
- Hardware problem in judging the and taking the biometric.
- Not capturing the entire image.

Threats involved in theft of Biometric

- Dummy body parts.
- Fake accept rate.
- Inaccurate reject rate.
- Fake reproducibility using forensic techniques.
  - **Fake Accept rate** Reduction in Fake Accept rate leads to hike in reject rate. System perform good in one to one faces than what is does in database.
  - **Inaccurate Reject rate** Person changes, Scars in body parts used in authentication, any sickness like cold wounds leads to inaccurate attempt of recognition through biometric system.
  - **Dummy Body Parts** Thief takes off and steal the body parts and then use that parts for authentication. One solution of this type of theft is to use live body organs detectors which include circulation of blood in body part like fingure, body temperature etc.

Motivation for the work and future proposal

The Topic and related work explained in this paper put its light on the issues in privacy and security of Biometric Authentication, different solution and tactics are been followed to prevent the issues and authentication but we have come across with some of the tips to prevent this all i.e. to use several layer authentication so as if someone tries to breach the security then he will not be able to all the layers as pure correct presence of mind and originality of person would only lead to cross all the layers and access the data or some secured thing kept behind biometric authentication.

Below are some of the solutions that are proposed it enhance the security.

- First Use card swap-out which will be available to only authorized person.

- Use biometric fingure imprint which will be unique.
- Use iris scanner to analyze retina of an eye.
- Use OTP system to generate one time password.

These data layer security will always perform better as no one would be able to hack all the layers all at a time except for to false output.

Conclusion

In the above paper we have seen that how biometric system provides security for authentication and how it is get affected by the threats and various attacks. While using this system we must have to be careful with the failures and consequences and it must be taken cared to find the solution to prevent adverse situation that may occur. Insufficient knowledge and study about this system still exist and we should take measure to prevent those situation so that we can prevent financial and anti-fraud cases.

References

1. D.K jain and S.MAltoni, "Recognition and identificationin Fingureprints"-new York(2009).
2. A.K Asthani, "A Security and improvement in biometric system"(2007).
3. John Nixon, "Recognition of human fingerprint for Biometric Authentication"-London UK(2007).
4. J.F Kenedy, "Randomness and uniqueness of fingureprints"(2014).
5. A.S Rasto, "Legal Technology in biometric system"(2007).
6. S.M. beigi, "Key to secure password"(2011).
7. Ajay Kumar, "Hand geometry and fingure imprint for authentication (2009).
8. H. Himaga, "Fingure veins protection in biometric" (2009).