International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 7 Issue: 10

Experimental Analysis of Latest Biometric Security Strategies and Its Impact on Authentication Methods

Halkar Rachappa
Asst. Prof. & Head Dept. of Computer Science
Govt. Commerce & Management College,
BALLARI(Karnataka).
email :halkarrg@gmail.com

Abstract: - Biometric technology is the latest method which is used for security purpose. The technique uses biological features for authorised access. It is unique way of security methods and reliable as compared to other traditional methods of security. The technique uses features like fingerprint, face recognition, thumb impressions, digital signature etc as a means of security methods. It is automatic way of identifying the identity of the person which is based on physical characteristics of person. It is more safe and secure method of authentication as biological or physical features is unique to individual and cannot result in security threat and cannot be accessed by unauthorised user. There are many varieties of biometric technique and the organisations can select any one of them based upon the type of business they are doing and how safe they want to keep the data and information of the individual. There are many advantages as well as challenges of biometric technique which will be explained in this paper. The components of biometric architecture will also be explained in this paper.

Keywords: - Biometric Security, Methods of biometric technique, Biometric Architecture, Advantages, Disadvantages, Steps involved in Biometric Process.

*****

Introduction: - [1]

There is a lot of information and data of individual available online which should be kept safe and secure. There are a number of security methods which are used to keep the data safe and has the capability to identify any security threats to the information. The type of security technique used depends upon the priority to keep the data safe and secure and also depends upon the type of industry. For example, the banking domain company should have the strong and efficient security mechanism as they store the most crucial information of the individual loosing which will be a great loss to the bank as well as the individual. The old traditional methods of security always have risk of getting hacked and are not as efficient as the latest technology which is Biometric Techniques of security methods. Biometric technique is the process of using physical or biological features of human beings to identify the authorised human access to any system. It is very easy and the most secure methods of security. They will use features like voice and speech recognition, fingerprint, digital signature, facial expression etc in order to identify the authentic user. There are many advantages of using biometric methods as they are easy to carry out and takes very less time and are the safest of all the methods of security. The old traditional methods will require a person to remember their passcodes, they need to carry the ID cards in order to have access. In case they forget their passwords or loose the authentication cards then it gets really difficult to get access without it. Also, the renewal process will take a lot of time and in case of emergency purpose the situation becomes worst. Where as using biometric technique the authorisation process becomes much easier than the old traditional methods. There is no need to carry separate authorisation cards as well as no need to remember the passwords for login. Simply the person can use their fingerprints, facial expressions, voice recognition in order to gain access in the system. The biometric architecture is designed in such a way that it creates a pattern in side the components and then uses the same method to determine whether it is the same person or not. It is the safest method as it will not allow hackers to get access. As the physical features and biological features differs for all the individuals, the hackers will not be able to get access in the system. That's why this technique is in demand and is trending and most of the companies and domains have already started implementing it in their companies.

Strategies/Types of Biometric Techniques: - [2]

Type of Biometric Technique is broadly divided into following three categories: -

- Biological
- Physiological
- Behavioral.

Following are the varieties of Biometric techniques used in the organisations: -

1. Shape of Ear
2. DNA matching
3. Facial expression recognition
4. Fingerprint recognition
5. Eyes Recognition (Iris recognition, Retina recognition)
6. Finger geometry recognition
7. Gait Recognition
8. Typing Recognition
9. Voice/Speech Recognition
10. Odour Recognition

1. Shape of ear recognition: -
   - In this technique the architecture of the biometric method is designed in such a way that it uses shape of ear recognition to identify the authorised user of the system.
   - The system will automatically read the pattern of the shape of the ear of person and if does not match then access will not be granted and vies-versa.

2. DNA Matching: -
   - This method uses segments from DNA of individual to identify the person.
   - This method is mostly used in the field of crime etc where the criminal can be identified by taking samples from his DNA to match it with proofs found at the crime site.

3. Facial Expression Recognition: -
   - In this method the person needs to show their face into the authentication camera and then the camera reads the pattern of the face and then provide access to the individual.
   - The facial expression authentication uses eigenfaces or local feature analysis to determine the authorised user access.

4. Fingerprint Recognition: -
   - This technique is the most commonly used technique where the patterns of the fingers are stored in the camera and next time when user keeps his fingers then it will cross check with the already existing fingerprints and allows access when it matches with each other otherwise give warning in case of not matching.
   - The system will store the pattern in the form of arches, loops, Whorls of the ridges of finger. This method can be used in banks to provide access to user to operate their lockers, by companies to provide access to the employees, as well as in crime domain to identify the criminal by matching the fingerprints identified at the site of crime with the suspected criminal.

5. Eyes Recognition: -
   - In this method two types of identification can be used one is retina and other is Iris of the eye.
   - The camera is efficient enough to store the pattern of the retina and iris itself and whenever a person places his eyes in front of the camera it will read the pattern and cross examine with the one stored in its database and then provide access accordingly.
   - This method is used in high profile banking domains.

6. Finger Geometry Recognition: -
   - In this method the application will store the pattern in the form of 3D image of the finger of the individual.
   - The designing and coding of such biometric technique is advance and requires efficient professional skills to design it.
7. Gait Recognition: -
   - This is the latest development in the field of biometric technique where the even the walking style of the individual can help to identify the authorised and unauthorised user.
   - This is high tech advance method which is used in branches like CBI, special forces etc to determine the suspects of the crime.

8. Typing recognition: -
   - This is also one of the methods used to determine the identity of the individual.
   - Each person will have their unique style of typing and the identity is determined based upon the typing speed, style and words per minute of the individual.
   - This is not very efficient technique as the person can easily copy and may
     have same typing speed as other person but still this method is used in few domains.

9. Voice Speech Recognition: -
   - This is also one of the latest methods of determining the identity of the individual.
   - The biometric application will store the voice/speech of individual in the form of rate of speech of person. This will convert the speech of human into language which is understood by computer and it will match it with the already stored pattern of speech and then provides access accordingly.
10. Odour Recognition: -
    - The biometric technology has found many ways of identification of individual and one of the methods is using the odour of the individual.
    - This technique will involve scientific engineering methods to implement the odour-based identification technique of individual.

Architecture Components of Biometric Methods: - [3]

Following are the six main components of any biometric security methods: -

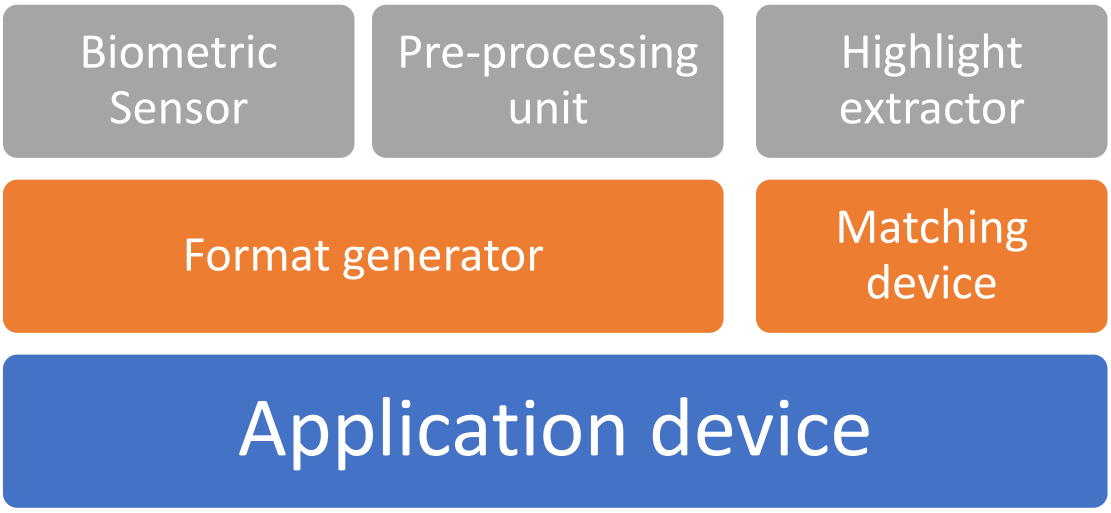

Figure 1 Components of architecture of Biometric Technique.

1. Biometric Sensor: -
   - This is the first and most important component in the architecture of the biometric application as this is the one which will help to identify the patterns.
   - The type of pattern identified by the sensor depends upon the type of biometric technique used for the identification of identity of the person.
   - The sensor acts as an intermediate between the individual and the system.
2. Pre-processing unit: -
   - It is the second most important component of the biometric architecture.
   - It is used to filter the disturbances from the patterns acquired in order to read and match the pattern properly.
   - It is basically normalisation process where all the background disturbances are removed.
3. Highlight Extractor: -
   - This is the third and the main advance in the biometric framework.
   - Extraction of elements is to be done to recognize them at a later stage.
   - The objective of an element extractor is to portray an item to be perceived by estimations.
4. Format Generator: -
   - The format generator produces the layouts that are utilized for verification with the assistance of the extricated highlights.
   - A format is a vector of numbers or a picture with unmistakable parcels.

Qualities acquired from the source assembles come to frame a format.

- Layouts are being put away in the information base for examination and fill in as contribution for the match.

5. Matching Device: -
   - The matching device also plays important role in identification of the identity.
   - The obtained template is given to the matching device to match it with the stored templates.
   - The matching device uses available and implemented algorithm and then matches it with the stored template and generates the results.
6. Application Device: -
   - It is the device which uses the results generated by the biometric system.
   - Iris recognition, Facial recognition, Speech recognition are the examples of application devices.

Steps involved in Biometric Methods: - [4]

This is a two-step process which is performed in following manner: -

➢ Verification process: -

- First of all, references to be used by the users are stored in the database.
- Some samples are taken and then with the help of algorithm are matched using the matching device.
- In the final step the testing is carried out to determine which template should be used for the comparison.

➢ Identification step: -

- The framework plays out a one-to-numerous examinations against a biometric information base trying to lay out the character of an obscure person.

Advantages of Biometric Techniques: - [5]

Following are the advantages of Biometric techniques: -

1. Improved Security: - Since the biometric technique uses biological and physical features of individuals in the implementation of security methods, it makes sure that the information is safe and secure. As the physical features are unique to person the rate of security increases.
2. Reduced chances of faking: - Since the physical features of individual are unique to person there are no chances that they can be faked and used by the hackers to get access.
3. Great User experience and saves time: - The biometric security methods are fast and saves a lot of time of individual in order to get authorised access in the system. This gives great experience to users.
4. Non-adaptable: -Biometric confirmation requires its feedback is available upon approval. You can't move or share a physical biometric carefully - the best way to use most biometric confirmation frameworks is with an actual application.

Challenges of Biometric Techniques: -

1. Higher Costs: - The process of implementation of biometric technique involves great cost which is not possible for small scale organisations.
2. Hacking: - The hacking of biometric technique is possible if the hacker threatens the individual.
3. System Failure: - If the application is not designed carefully then it may give error while providing access.

Conclusion: - There is a great deal of data and information of individual accessible web-based which ought to be remain careful and secure. There are various security strategies which are utilized to keep the information safe and has the ability to distinguish any security dangers to the data. The kind of safety method utilized relies on the need to keep the information free from any and all harm and furthermore relies on the sort of industry. The old conventional strategies for security

generally have hazard of getting hacked and are not however proficient as the most recent innovation which seems to be Biometric Techniques of safety techniques. Biometric strategy is the method involved with utilizing physical or organic elements of people to recognize the approved human admittance to any framework. It is extremely simple and the most dependable techniques for security. Biometric innovation is the most recent strategy which is utilized for security reason. The method involves natural elements for approved admittance. It is interesting method of safety strategies and solid when contrasted with other customary techniques for security. The strategy utilizes highlights like unique finger impression, face acknowledgment, thumb impressions, advanced mark and so forth for the purpose of safety techniques. It is programmed approach to recognize the personality of the individual which depends on actual attributes of individual. It is free from any danger technique for validation as natural or actual elements is one of a kind to individual and can't bring about security danger and can't be gotten to by unapproved client. Still designers are looking for ways to improve the techniques in order to completely avoid data breech.

References: -

1.https://www.tutorialspoint.com/biometric-identification-techniques
2.https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/
3.https://www.geeksforgeeks.org/biometric-system-architecture/
4.https://www.google.co.in/search?q=steps+for+biometric+technique&source
5.https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics