Biometric Authentication Towards Security And Privacy

Harini M[1], Dr Thara L[2]
[1]Dept of MCA
[2]Associate Professor, Dept of MCA
[1, 2] PSG college of Arts & Science, Coimbatore,India

Abstract- *Biometric authentication has been intensively explored and has piqued the interest of both academics and industry in order to overcome the password management difficulty and enhance the usability of authentication systems. Yet, contemporary biometric authentication technologies have flaws. Some biological abilities have not been properly researched in a long time. There is presently no comprehensive review of the most recent improvements in biometric authentication for the goal of quick identification while maintaining privacy. In this work, we categorise and systematically analyse current biometric authentication systems by focusing on security and privacy solutions. We examine the hazards of biometric authentication and advocate for a range of standards for secure and private authentication*

Keywords- Biometric, Authentication, Security, Privacy, Pattern, Technologies

I. INTRODUCTION

Throughout ancient times, people have recognised one another based on a variety of traits. We can identify someone by their voice when we speak to them and by their face when we first encounter them. In the past, identity verification (authentication) in computer systems has relied on a key, magnetic or chip card, or on knowledge (PIN, password). Yet, items like cards or keys frequently become lost or stolen, and passwords are frequently forgotten or shared, we should utilise anything that accurately defines the provided person in order to obtain more trustworthy verification or identification. [1]

A voice sample or a fingerprint are examples of quantifiable physiological or behavioural features that may be used in biometrics to automatically verify oridentify a person. The traits are quantifiable and distinct. These traits should not be replicable, but sadly, it is frequently feasible to use biometrics to produce a clone that the biometric systemaccepts as a genuine sample. This is a common scenario where the degree of security offered is indicated by the sum of money an imposter requires to get access without authorization. Nowadays, there are several biometric approaches accessible. A handful of them are still in the phase of research (for instance, stench analysis), but a large number of them are just developed and widely available (at least ten various sorts of biometric security are available today nowadays: fingerprint, finger geometry, hand geometry, palm print, iris pattern, retina pattern, facial recognition, voice comparison, signature dynamics, and typing rhythm).

II. BIOMETRIC TECHNIQUES

Nowadays, there are several biometric approaches accessible. A handful of them are still in the phase of research (for instance, stench analysis), but a large number of them are just developed and widely available (at least ten various sorts of biometric security are available in these days: fingerprint, finger geometry, hand geometry, palm print, iris pattern, retina pattern, facial recognition, voice comparison, signature dynamics, and typing rhythm). [2]

2.1 IRIS

The vivid ring of textured tissue that covers the aperture of the eye is known as the iris. Even identical twins have various iris patterns, so everyone's left and right iris is unique. A unique gray-scale camera is used to capture the biometric traits at a distance of 10-40 cm from the camera. The camera is hidden behind a mirror; the viewer looked further into reflective surface to see his or her very own eye; the camera could then "see" the eye. The snapshot of the eyeball is taken after the eye is fixed and the camera has appropriately centered. The iris scanner does not require any unique lighting conditions or types of light. An iris scan generates a large amount of data, implying a high percentage of discrimination (identification). Iris systems are really suited for identification. An iris scan generates a large amount of data, implying a significant increase of discrimination (identification). If the background is too dark, any conventional lighting can be employed. Some iris scanners additionally feature a light beam that turns on immediately when needed. [3][4]

2.2 RETINA

Retina scan is based on the blood vessel pattern in the retina of the eye. Retina scan technology is older than the iris scan technology that also uses a part of the eye. The first retinal scanning systems were launched by EyeDentify in 1985. The method of obtaining a retina scan is personally invasive. A laser light must be directed through the cornea of the eye. Also the operation of the retina scanner is not easy. A skilled operator is required and the person being scanned has to follow his/her directions The retinal scanning systems are said to be very accurate. For example,theEyeDentify's retinal scanning system has reputedly never falsely verified an unauthorized user so far. The false rejection rate, on the other side, is relatively high as it is not always easy to capture a perfect image of the retina. The false response rate, while on the other hand, is rather high since capturing a flawless picture of the retina can sometimes not be practicable.

2.3 HAND GEOMETRY

Hand geometry is built around the notion that practically every human's hand is distinctive and that a human's hand structure doesn't really alter after a certain age. Hand geometry systems estimate specific hand dimensions, especially the length and breadth of fingers. The hand is measured using a range of methods. Optical hand geometry scanners obtain a snapshot of the hand and estimate its parameters by using image edges detection methods. Optical scanners are divided into two groups. The first kind of devices generates a black-and-white visual picture of the hand's form. This is simple to accomplish using an illumination and a black-andwhite camera. Scanners and software applications then analyze the bitmap picture. Under this circumstance, only 2D hand attributes may be employed. The other category's hand geometry systems are more advanced. Hand geometry sensors are simple to operate. The hand template is generally as short as 9 bytes in size. The verification process takes around one millisecond. Because hand geometry methods are used solely for verification, speed is not a barrier. [5][6]

2.4 SIGNATURE DYNAMICS

Signature dynamics recognition concentrates on the mechanics of signing instead of the subsequent matching of the signature itself. The most apparent and significant benefit associated with this is that a fraudulent cannot learn how to make a signature by merely glancing at one that has already been written. To capture the signatural characteristics, many technologies are utilised. They are either conventional tablets or specialised gadgets. Tablets record 2D dimensions as well as pressure. An individual frequently fails to sign in an identical way, thus the data retrieved from an user's signature must account for some fluctuation. Majority of signature mechanisms technologies validate the dynamic behaviour simply, they don't really give any consideration to the resulting signature. The data collected during the signing phase is around 20 kB in size. The efficiency of signature mechanisms biometric sensors is not significant; the manufacturers' reported crossover rate is roughly 2%, but our personal experience indicates that the accuracy is substantially lower. [7]

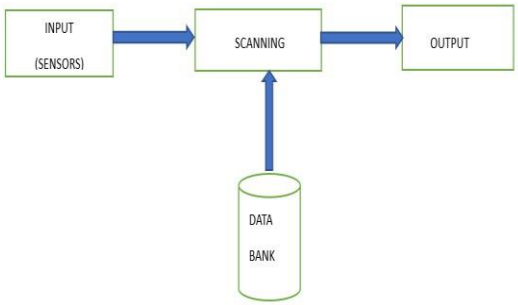

Fig 1 Biometric system

2.5 FACIAL RECOGNITION

One of most intuitive method of biometric authentication is facial recognition. Almost every human being has the knack for distinguishing one person from another. Any webcam can be put to use to capture a facial image. Any scanned image can also be utilised. In general, the better the given images, the more accurate the outcomes. The lighting conditions necessary are mostly decided by the camera's quality. Different characteristics may be hard to recognize under low-light conditions. Most face recognition systems need the user to stand a certain angle away from the sensor and stare directly at it. This guarantees that the acquired image of the face falls within a particular size constraint and that the features (for example, the eyes) are in the same location every time. The processing system's initial responsibility is to pinpoint the face (or faces) inside the picture. The face traits are then taken. The methodology of facial metrics is based on the measurement of certain face traits . The existing programme frequently fails to locate the face or identifies "a face" in the wrong area. This drastically worsens the outcomes. Greater outcomes may be accomplished if the person can inform the machine where the eyes are located. If privacy is the primary issue, even verification thoroughness may be insufficient. [8]

III. ADVANTAGES

a) Facial biometrics provide a quick and easy user experience.

b) They are connected to a specific individual, as contrast to a password, which may be used without authorization.
c) They are extremely convenient since there is no need to memorise or maintain anything.
d) They are particularly resistant to fraud in terms of security.Exploiting a biometric authentication system is more challenging than exploiting a password or access-card authentication system.
e) With biometrics, one may instantly unlock an application. Using a fingerprint or facial scan to authenticate a person becomes extremely fast.
f) The primary advantage of biometrics is the fact that people perpetually have a means to authenticate yourself. As an instance, anyone could lose your login information or misplace your access device. Users fingerprint, walk, and signature are tough to forget.

IV. DISADVANTAGES

a) Long or varied eyelashes may cause problems with the scanner recognising retina lock on the smartphone.
b) A fault in the system might cause the biometric software to fail. The biometric system may fail due to a power outage.
c) Employee fingerprint data can be misused by the company. As a result, an employee's or a person's privacy may be damaged.
d) Some biometric identification techniques, which include DNA as well as retinal detection, may not be extremely intuitive. It may also be unhygienic. It is attainable that people will refuse to take advantage of such a system.
e) The issue of privacy is also raised by biometric authentication. It is concerning if your fingerprints are requested on every occasion you go, or if people may recognise you simply by analysing your voice every time you communicate.
f) Furthermore, numerous biometric authentication technologies are still under progress and might be costly to deploy.

V. CONCLUSION

A person's identity cannot be isolated from their biometrics. As a result, biometric solution suppliers must invest extensively in safety measures to address the issue of privacy and data leak. Introduction of improved safety methods and technological innovations can assist the sector in remaining in advance of fraud advances. Although the accuracy of biometric approaches remains far from perfect, several mature biometric systems are already accessible. Proper planning and execution of a biometric system can definitely boost overall security; smartcard-based technologies, in particular, appear to be particularly promising. The wording is a little different, but it's still a good place to start. The term biometrics is frequently used as a synonym for flawless security. This is a deceptive viewpoint. While creating a safe biometric system, a variety of factors must be considered. To commence, it is important to understand that biometrics are not mysteries. This means that biometric measures cannot serve as competency tokens and can not be utilized to establish cryptographic keys. Second, the input device must be acknowledged, and the channel of communication must be trustworthy. Finally, the input device has to validate the proper functioning of the individual being examined and the instrument ought to be certified for instance through a challenge-response protocol.

REFERENCES

[1] Mr.Vinayakpujari-“Research paper on Biometric Security”-2021
[2] Kavita Gupta-“Review paper on Biometric Authentication”-2017
[3] Zdenel Riha- “Biometric Authentication Systems-2020
[4] URL-https://en.m.wikipedia.org/wiki/Biometrics
[5] URL-https://medium.datadriveninvestor.com/biometricsfor-authentication-security-and-privacyimplications-5d59317ff18e
[6] Sushma Jaiswal-“BIOMETRIC-Case study”2011
[7] Mandeep Singh Walia-“Modern Biometric Technologies: Technical issues and Research oppurtunities.