International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 04 | April - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Does the use of Biometrics Increase Security?

Sakshi Singh[1]

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

Abstract

In recent decades there has been an explosion in the use of biometrics, in many situations where the use of biometric identification techniques is already possible. Usability is a very relevant factor. Another is privacy. There is a natural opposition to the prospect of creating a comprehensive centralized personal database. Companies need to be careful about how they implement their biometric authentication systems to prevent infringement of employee or customer privacy or improper display of confidential information. After all, it's easy to issue a new password if the old one is tampered with, but impossible to give someone a new one.

Biometric authentication uses human physical or Behavioural characteristics to digitally identify an individual to provide access to systems, devices or data. Examples of such biometric identifiers are fingerprints, facial patterns, voice or typing rhythm. Each of these identifiers is assumed to be unique to the individual and may be combined with other means of authentication to ensure greater accuracy in identifying users. Since biometrics can provide a reasonable level of confidence in the authentication of an individual, it has the potential to dramatically improve security. When computers and devices detect an authorized user's fingerprints they can be automatically unlocked. Server room doors can open when they recognize the face of a trusted system administrator. The help desk system can automatically extract all relevant information upon recognition of an employee's voice on the helpline.

Most companies classify biometric authentication as "effective" or "very effective" in protecting identity data stored provincially and claim that it is effective in protecting data stored in the public cloud. Most of the companies are already using biometric authentication and rest are planning to implement it in the upcoming years.

1. Introduction

Biometrics are growing as an advanced layer for many personal and enterprise security systems. With unique identifiers of your biology and Behaviour, this may sound silly. However, biometric identification has alerted many about its use as a standalone authentication.

Modern cyber security is focused on mitigating the risks of this powerful security solution: traditional passwords have long been a point of weakness for security systems. Biometrics aims to answer this issue by adding proof of identity to our bodies and Behaviour patterns.

Today, the Behaviour Identifier method is often used to distinguish between a human and a robot. This can help the company filter spam or detect brute force attempts towards signing in with a password.

Here are some common approaches:

i. Typing Patterns

Everyone has a different typing style. The speed at which we type, the time it takes to move from one letter to another, the level of impact on the keyboard, all of these considerations.

ii. Physical Movement

The way a person travels varies from one person to another and can be used to authorize staff in a building or as a second verification layer for the most sensitive areas.

iii. Navigation Levels

Mouse movements and finger movements on trackpads or touch screens are different for individuals and are easy to identify with the software, without the need for additional hardware.

iv. Engagement Patterns

We all work with technology in different ways. How we open and use apps, places and times of day when most likely to use our tools, how we browse websites, how we tilt our phones while holding them, or even how often we scan our social network. accounts are all aspects of Behaviour that may be unique. Today these Behaviours can be used to distinguish people from bots. They can also be used in conjunction with other verification methods or, if the technology develops sufficiently, such as independent security measures.

Origin of Biometrics

The first modern biometric device was launched on a commercial basis 25 years ago when the finger-blocking machine was scheduled to apply for a curfew at Shearson Hamill on Wall Street. In recent years, hundreds of these hand geometric devices were connected at the top safety centers operated by Western Electric, Naval Intelligence, Department of Energy, and comparable.
The word Biometrics comes from Greek arguments for "bios" (life) and “metrikos" (average). Simply put, it refers to discipline linking biological statistical tests features.

The term biometrics refers to the evolving field of technology dedicated to human data using biological characters or Behaviourrs.

2. Biometrics Overview

2.1 What is Biometrics?

Biometrics is the measurement and statistical analysis of unique physical and Behavioural characteristics of people. The technology is mainly used for identification and access control or to identify persons who are under surveillance. The basic premise of biometric authentication is that each individual can be accurately identified by intrinsic physical or Behavioural traits. The word biometrics is derived from the Greek words bio, meaning life, and metrics, meaning measuring.

2.2 Why we need biometrics?

To overcome the problems of failing to remember keywords and ID codes, Biometrics based verification helps us to verify your fingerprints, iris design and voice for your uniqueness at ATMs, airports etc. you can solve your families, withdraw money at or after the bank with just a flash of an eye, a tap of your finger or by not showing interest in presenting your expression.

2.3 How do Biometrics work?

Authentication by the use of biometric verification has become quite common in corporate and public security systems, consumer electronics and point-of-sale applications. Besides security, convenience has been the driving force behind biometric verification, as there are no passwords or security tokens to remember. Some biometric methods, such as measuring a person's gait, may work without direct contact with the person being authenticated.

The components of biometric devices include the following:

a reader or scanning device to record the biometric factor to be authenticated;

software to convert scanned biometric data into a standardized digital format and compare match points of observed data with stored data; And

A database is required to store biometric data for comparison securely.

Biometric data can be kept in a centralized database, although modern biometric implementations often rely instead on collecting biometric data locally and then cryptographically hashing it to allow authentication or identification without direct access to the biometric data. be completed.

3. Types of Biometric Identifiers and their Services:

The two main types of biometric identifiers are either physical characteristics or Behavioural characteristics.

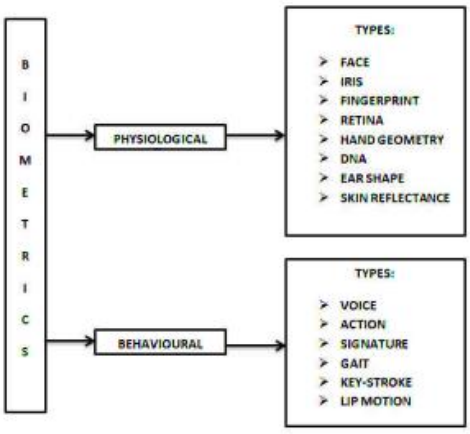

Fig 3.1 Biometric Types

When most people think of biometrics, they imagine fingerprint or facial recognition, but today there are many different types of biometrics used to identify and authenticate individuals. . Biometrics come in many forms, whether for security, access, or fraud prevention, and the software required to collect biometric data is also evolving rapidly.

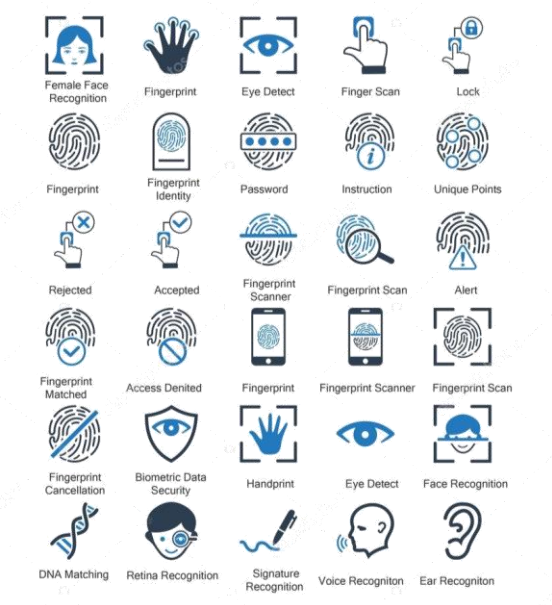

Fig 3.2 Biometric Authentication Icons

Here are 14 different types of biometrics

- **Different Types of Physiological Biometrics**

Physiological biometrics are the ones which depend on one's physical characteristics to determine identity. This type of biometrics includes, but is not limited to:

i. Fingerprints

Fingerprint recognition, which measures the unique ridges of a finger, is one of the oldest forms of biometric identification. After the print is captured, sophisticated algorithms use the image to create a unique digital biometric template. The template is then compared with new or existing scans to confirm or deny a match.

ii. Finger/hand nerves

Veins are much more difficult to hack than other biometric scans because they are deep within the skin. Infrared lights pass through the surface of the skin where they are absorbed into deoxygenated blood. A specialized camera captures the image which digitizes the data and then either stores it or uses it to confirm the identity.

iii. Hand geometry

Hand Geometry Biometrics refers to the measurement of hand characteristics such as the length and width of the fingers, their curvature and their relative position with other characteristics of the hand. Although once a predominant method of biometric measurement, modern advances in fingerprint and facial recognition software have replaced its relevance in most advanced applications.

iv. Iris recognition

The iris, or colored part of the eye, consists of thick, thread-like muscles. These muscles help shape the pupil to control the amount of light entering the eye. By measuring the different folding's of these muscles, biometric authentication tools can authorize identity with very high accuracy. Vibration detection (such as a scan requiring the user to blink) adds an extra layer of accuracy and security.

v. Retina scan

Retinal scans capture capillaries deep within the eye using unique near-infrared cameras. The raw image is first pre-processed to enhance the image then re-processed as a biometric template to be used during both enrollment and verification.

vi. Facial Recognition

Facial Validation is the oldest form of Biometric Authentication ever. Even babies use facial recognition to identify those closest to them. Biometric facial recognition software works in the same way, albeit with more precise measurements. Specifically, facial recognition software measures facial geometry, including the distance between the eyes and the distance from chin to the forehead (to name just a few). After collecting the data, an advanced algorithm turns it into an encrypted facial signature.

vii. Ear shape

Unlike many other biometric modalities that require unique cameras to take measurements, ear-shaped biometrics measure the acoustics of the ear using an inaudible sound wave using special headphones. A microphone inside each earphone measures sound waves as they are reflected off the ear canal, bouncing off in different directions from different curves of the ear canal. A digital copy of the shape of the ear is then converted into a biometric specimen for later use.

viii. Voice recognition

Voice recognition technology falls under both the physical and Behavioural biometric umbrellas. The shape of a person's vocal tract, including the nose, mouth, and larynx, determines the type of sound produced. In practice, the way a person says something – tempo variation, intonation, tempo, pronunciation, and so on – is also unique to each person. The combination of data from both physical and Behavioural biometrics creates an accurate vocal signature, although the mismatch may be due to disease or other factors.

ix. Thermography recognition

A thermogram is a representation of infrared energy as a temperature distribution image. Biometric facial Thermography captures patterns of heat caused by the movement of blood under the skin. Since blood vessels are highly unique, the corresponding thermograms are also unique – even in identical twins – making this method of biometric authentication more accurate than traditional facial recognition software.

x. DNA matching

DNA has long been used for identification purposes. Additionally, it is the only form of biometrics that can trace family ties. DNA matching is particularly valuable for missing persons, disaster victim identification and dealing with potential human trafficking. Furthermore, apart from fingerprints, DNA is the only biomaterial that can be "left behind" inadvertently. DNA collected from hair, saliva, etc. consists of short tandem repeat sequences (STRs). The DNA STR can confirm identity by comparing it to other STRs in the database.

- **Different Types of Behavioural Biometrics**

Behavioural biometrics are the ones which measure the Behaviour patterns as opposed to or in added with the physical characteristics. These are some examples of Behavioural biometrics.

i. Gait

Gait biometrics records the stride pattern via video imaging and then turns the mapped data into a mathematical equation. This type of biometric is unobtrusive which makes it ideal for large scale crowd monitoring as it can quickly identify people from afar.

ii. Lip movement

One of the newer forms of biometric authentication involves measuring lip movements. Like a deaf person it can track lip movement to determine, biometric lip motion authentication tracks and records precise muscle movement around the lips to determine if they follow an expected pattern or not. Biometric lip motion sensors often require users to verbalize a password and record the corresponding lip movement to grant or deny access.

iii. Signature identification

Signature Recognition is a Behavioural biometric that measures spatial coordinates, pen pressure, inclination and pen stroke in both "off-line" and "on-line" applications. A digital tablet records the measurement and then uses the information to automatically generate a biometric profile for future authentication.

iv. Keystroke

Keystroke Dynamics takes standard passwords to the next level by tracking the rhythm used to enter passwords. Measurements may include the time it takes to press each key, the delay between keys, characters typed per minute, etc. Keystroke patterns work in conjunction with passwords and PINs to improve security efforts**.**

4. Are biometrics secure?

Though very high-quality cameras and other sensors help with the use of biometrics, they can also bring in attackers. Because people do not protect their face, ears, hands, voice or gait, attacks are only possible by capturing biometric data without people's consent or knowledge.

An old attack on a fingerprint biometric authentication system was referred to as the gummy bear hack, and it dates back to 2002 when Japanese researchers using a gelatin-based confection showed that an attacker could pick up a secret fingerprint from a shiny surface. Gelatin's capacitance is similar to that of a human finger, so fingerprint scanners designed to detect capacitance would be fooled by gelatin transfer.
Determined attackers can beat other biometric factors as well. In 2015, Jane Chrysler, also known as Starbug, a Chaos Computer Club biometric researcher, demonstrated a method to extract enough data from a high-resolution photograph to defeat iris scanning authentication. In 2017, Chrysler reported defeating the iris scanner authentication scheme used by the Samsung Galaxy S8 smartphone. Chrysler had previously redacted a user's thumbprint from a high-resolution image to demonstrate that Apple's Touch ID fingerprinting authentication scheme was also vulnerable.
After Apple released the iPhone X, it took researchers only two weeks to bypass Apple's Face ID Facial recognition using a 3D-printed mask; Face ID can also be defeated by persons related to the authenticated user, including children or siblings.

5.1 Advantages

- It provides all services in a convenient way. It makes the password stronger and more complex.
- They are stable and permanent. It can detect a person despite the slightest variation.
- Strong assurance and unquestionable accountability.
- It requires very little memory and little storage.
- Provides security and is non-transferable.

- It takes very little time to scan fingerprints.
- It also sees different features.
- It is really easy to operate and most people are aware of this technology.
- Iris scanners are well protected.
- The iris is usually stable for decades.
- each iris has a specific pattern.
- Voice recognition is very reliable.
- It is quite safe and simple to use.
- It is very difficult for someone to fake it as it is well protected and ensures that it does not get spam.
- Keystroke is one of the most suitable technologies available.
- It is very fast working.
- It is impossible for anyone else to copy by looking at the person typing.
- There is no user interface.

5.2 Disadvantages

- The biggest challenge for the biometric process is that it is taken and mapped for visualization.
- There is a lack of accuracy that can lead to biometric system failure.
- Privacy is a major biometric solution.
- Once information is hacked, it can lead to many negative consequences.
- Sometimes errors in biometric machines appear as false denials and acceptance.
- It is caused by the inability to read different aspects of each person.
- There are cases when the device rejects an authorized user.
- It is expensive and involves the cost of implementing and operating the system and maintenance.
- Integration is another complex issue that makes technology aggressive.
- Acceptance from an authorized person should be taken onto account when one feels uncomfortable.
- In some cases, it causes damage to the fingerprints during the verification process.
- Technology can also be used to duplicate and steal personal identity.
- Implementation, establishment and maintenance are really expensive.
- A short distance should be kept by the person in order to read directly.
- Individual voice can be copied.
- A large amount of storage is covered when various patterns are considered.
- The authorized person must know how to use the keyboard to get accurate pattern analysis.
- False identity issue may come into picture if the algorithm used is not correct.

6. Conclusion

Improvements in accuracy and efficiency and cost reduction have made biometric technology a safer, more realistic and cost-effective way to identify individuals. Biometric structures such as reading fingerprints, retina scanning, iris scanning, signature verification, hand geometry, voice verification and more are all well-recognized for their precise features. Limitations of band speed and bandwidth are now a thing of the past and their actual performance may be better in most cases than predicted.

7. Acknowledgement

It gives me great pleasure to present my research paper on “Does the use of biometrics increase security?”. I would like to express the sincerest gratitude to all my teachers who have helped me throughout the research and provided me with proper guidance and support.

I am also grateful towards, ‘Head of Department'. This acknowledgement will remain incomplete if I do not mention a sense of gratitude towards our esteemed principal who provided me with the necessary guidance, encouragement and all the facilities available to work on this project.

8. References

https://www.techtarget.com/searchsecurity/definition/biometrics

https://www.ibeta.com/different-types-of-biometrics/

https://www.kaspersky.com/resource-center/definitions/biometrics

https://www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks