Biometrics – The Need of Security

Chaitrali Tambe[1] Aasoo Yadav[2] Komal Bane[3] Nikita Vagmare[4] Sapna Vishwakarma[5]
[1,2,3,4,5]Student
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]Thakur Polytechnic, Mumbai, Maharashtra, India

Abstract— In today's world we are able to see the expansion of technology which can be useful for people in day-to-day life. This growth of technology has its advantages but these also come with its disadvantages. A number of the people take advantage of the disadvantages and hence give birth to the cybercrimes. As now-a-days all the data is stored and exchanged over through virtually there also are chances of this information are misused by someone. To stop this information there's always a requirement of reliable and accurate authentication which will decrease the mis-use of the data. The word Biometrics comes from the Greek words "bios" (life) and "metrikos" (measure). By using biometrics, it's possible to acknowledge someone supported who you're, instead of by what you possess (e.g., an ID card) or what you remember (e.g., a password).

Keywords: Biometrics, Authentication, Security, Sensor, Passwords, Pins

I. Introduction

Biometric authentication or just biometrics refers to establishing identity supported the physiological characteristics of a personal like face, fingerprints, hand geometry, iris and behavioral like keystroke, signature, voice, etc. a pleasant property of biometric traits is that it's supported something you're or something you're doing, so you are doing not should remember anything neither to hold any token. Authentication methods by means of biometrics are a specific portion of security systems, with a good number of benefits over classical methods. However, there are drawbacks.

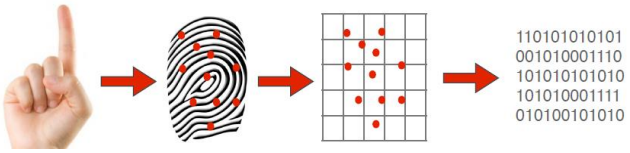

Fig. 1: Example - Fingerprint biometric

Authentication method	Pros	Cons
Handheld Tokens (Card, ID, passport, etc.)	– A new one can be issued. – It is quite standard, although moving to a different country, facility, etc	– It can be stolen. – A fake one can be issued. – It can be shared. – One person can be registered with different identities.
Knowledge based (password, PIN, etc.)	– It is a simple and economical method. – If there are problems, it can be replaced by a new one quite easily	– It can be guessed or cracked. Good passwords are difficult to remember. – It can be shared. – One person can be registered with different identities.
Biometrics (face, fingerprints, hand geometry, iris, voice, Etc.)	– It cannot be lost, forgotten, guessed, stolen, shared, etc. It is quite easy to check if one person has several identities. – It can provide a greater degree of security than the other ones.	– In some cases a fake one can be issued. – It is neither replaceable nor secret. If a person's biometric data is stolen, it is not possible to replace it.

Table. 1: Analysis of various Authentication methods

II. How Biometrics Works

A typical biometrics system incorporates four major module generally, namely sensor module that detects the characteristic being employed for identification, feature extraction module, template database, and matching module.

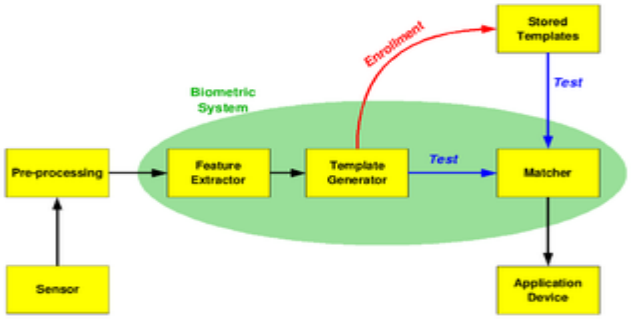

Fig. 2: Working of Biometrics with various stages

Here are 2 basic modes of a biometric system.

First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a particular template stored during a biometric database so on verify the individual is that the person they claim to be. Three steps are involved within the verification of someone. Within the beginning, reference models for all the users are generated and stored within the model database. In the second step, some samples are matched with reference models to induce the $64000 and impostor scores and calculate the sting. The third step is that the testing step. This process may use a wise card, username or ID number (e.g. PIN) to point which template should be

All rights reserved by www.ijsrd.com

used for comparison. 'Positive recognition' is also a typical use of the verification mode, "where the aim is to forestall multiple people from using the identical identity".

Second, in identification mode the system performs a one-to-many comparison against a biometric database in a trial to figure out the identity of an unknown individual. The system will achieve identifying the individual if the comparison of the biometric sample to a template within the database falls within a previously set threshold. Identification mode is additionally used either for 'positive recognition' (so that the user doesn't must 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". The latter function can only be achieved through biometrics since other methods of non-public recognition like passwords, PINs or keys are ineffective. The first time a user uses a biometric system is named enrollment. During enrollment, biometric information from a user is captured and stored. In subsequent uses, biometric information is detected and compared with the knowledge stored at the time of enrollment. The second block performs all the desired pre-processing: it's to induce obviate artifacts from the sensor, to strengthen the input (e.g. removing background noise), to use some reasonably normalization, etc. In the third block, necessary features are extracted. This step is also an important step because the right features must be extracted in an optimal way. A vector of numbers or a picture with particular properties is used to create a template. A template is also a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that aren't employed within the comparison algorithm are discarded within the template to chop back the file size and to shield the identity of the enrollee. During the enrollment phase, the template is solely stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the space between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. The matching program will analyze the template with the input. This could then be output for a specified use or purpose (e.g. entrance during a restricted area), though it is a fear that the use of biometric data may face mission creep]. Selection of biometrics in any exercise depending upon the characteristic measurements and user requirements. In selecting a particular biometric, factors to contemplate include performance, social acceptability, easy circumvention and/or spoofing, robustness, population coverage, size of apparatus needed and fraud deterrence. The selection of a biometric is based on user requirements and considers sensor and device availability, computational time and reliability, cost, sensor size, and power consumption.

III. How reliable is biometric authentication?

Authentication credentials like fingerprint scans or voice recordings can leak from devices, from company servers or from the software won't to analyze them. There's also a high potential for false positives and false negatives. An identification system won't recognize a user wearing makeup or glasses, or one who is sick or tired. Voices also vary.

People sound different after they first get on my feet, or after they fight and use their phone during a crowded public setting, or when they're angry or impatient. Recognition systems could even be fooled with masks, photos and voice recordings, with copies of fingerprints, or tricked by trusted relations or housemates when the legitimate user is asleep.

Experts recommend that companies use multiple styles of authentication simultaneously and escalate quickly if they see warning signs. As an example, if the fingerprint could even be a match but the face isn't, or the account is being accessed from an unusual location at an unusual time, it would be time to modify to a backup authentication method or a second communication. This might be particularly critical for financial transactions or password changes.

IV. Characteristics of Biometrics

The reason why system supported biometrics are much secure and reliable is in its characteristics. This makes the system far more promising. The characteristics are:

(1) *Distinctiveness:* Any two persons should vary enough to differentiate each other supported this characteristic.
(2) *Permanence:* The characteristic should be stable enough (with relevance the matching criterion) along time, different environment conditions, etc.
(3) *Collectability:* The characteristic should be acquirable and quantitatively measurable.
(4) *Acceptability:* People should be willing to simply accept the biometric system, and do not feel that it's annoying, invasive, etc.
(5) *Performance:* The identification accuracy and required time for a successful recognition must be reasonably good.
(6) *Circumvention:* The skill of fraudulent people and techniques to fool the biometric system should be negligible.

V. Types of Biometrics

Depending upon the traits, there are two major styles of Biometrics identification methods:

A. Physical biometrics:

It's supported by the direct measurements of a part of the body. Fingerprint, face, iris and hand-scan recognition belong to this group.

1) Fingerprints:

Fingerprint scanners became ubiquitous in recent years because of their widespread deployment on smartphones. Any device that will be touched, sort of a phone screen, mouse or touchpad, or a door panel, has the potential to become a straightforward and convenient fingerprint scanner. In step with Spiceworks, fingerprint scanning is that the most common style of identification within the enterprise, employed by 57 percent of companies.

All rights reserved by *www.ijsrd.com*

2) Photo and video:
If a tool is furnished with a camera, it can easily be used for authentication. Automatic face recognition and retinal scans are two common approaches.
3) Physiological recognition:
Automatic face recognition is that the second most common style of authentication, in step with Spiceworks, in place at 14 percent of companies. Other image-based authentication methods include hand geometry recognition, employed by 5 percent of companies, iris or identification, palm vein recognition, and ear recognition.
4) Voice:
Voice-based digital assistants and telephone-based service portals are already using voice recognition to identify users and authenticate customers. In step with Spiceworks, 2 percent of companies use voice recognition for authentication within the enterprise.
5) Signature:
Digital signature scanners are already in widespread use at retail checkouts and in banks and are a good choice for situations where users and customers are already expecting to possess to sign their names.
6) DNA:
Today, DNA scans are used primarily in enforcement to identify suspects -- and within the films. In practice, DNA sequencing has been too slow for widespread use.

B. Behavioral biometrics:

Its supported measurements and data derived from an action performed by the user, and thus indirectly measure some characteristics of the body. Signature, gait, gesture and key stroking recognition belong to the current group.
1) Typing patterns:
Everybody incorporates a special typing style. The speed at which they type, the length of some time it takes to travel from one letter to a special, the degree of impact on the keyboard.
2) Physical movements:
The way that somebody walks is exclusive to a non-public and may be accustomed authenticate employees in an exceedingly building, or as a secondary layer of authentication for particularly sensitive locations.
3) Navigation patterns:
Mouse movements and finger movements on track pads or touch-sensitive screens are unique to individuals and relatively easy to detect with software, no additional hardware required.
4) Engagement patterns:
We all interact with technology in several ways. How we open and use apps, how low we allow our battery to induce, the locations and times of day we're presumably to use our devices, the way we navigate websites, how we tilt our phones once we hold them, or even how often we check our social media accounts are all potentially unique behavioral characteristics. These behavior patterns could also be accustomed distinguish people from bots, until the bots reclaim at imitating humans which they will be utilized together with other authentication methods, or, if the technology improves enough, as standalone security measures.

VI. ADVANTAGES OF BIOMETRICS

Biometric technology is gaining more popularity day by day, all around the world. Biometric solutions are highly accepted by many government agencies, multinational organizations, institutions, banks, and hospitals just to call some industries. It's growing in every sector including finance, banking, workforce, borders and most rapidly for national identity. Research says that folk have more faith on modern biometric technologies rather than on traditional security systems and so the explanation is these following advantages:

A. Security

We used to have passwords with numbers, alphabets, symbols, etc. which became easy to hack every day. There are zillions of hacking incidents happening annually which we are losing our money constantly. Biometric technology brings different types of solutions which are nearly impossible to hack unlike passwords. This will be an honest help for us, specifically for business owners who are fighting with security problems for an extended time.

B. Accuracy

Traditional security systems break regularly costing us an enormous amount of it slow, money and resources. The foremost common security systems are passwords, personal identification numbers (PINs) and smart cards that aren't always accurate. However, biometric works together with your physical traits like fingerprints, palm vein, retina amongst others which is able to always serve you accurately anywhere, anytime.

C. Accountability

In other verification methods, anybody can use your password or security number to hack your personal information, which is extremely risky which we are filled with this problem continuously. But, just in case of biometric security, it needs your direct interactions to login or pass the security system which allows 100% accountability for all of your activities.

D. Convenient

There may be situations once you forgot your passwords. This can be often quite nerve-wracking because it's tough to memorize or inscribe each and every password which we are over likely to forget it in some sticky situations. There are some handy tools to undertake to the work for you, but none of these can beat the convenience of biometric solutions which stands to be the foremost convenient solution ever. Your credentials are with you forever, so it doesn't require you to memorize or inscribe anything.

E. Scalability

Unlike other solutions, biometrics is highly scalable solutions for all forms of projects. Biometric technologies are utilized in many government projects, banking security systems, workforce management, etc. It's possible because of the scalability of its solutions.

F. ROI

Unlike other solutions, biometrics is highly scalable solutions for each reasonably projects. Biometric

All rights reserved by *www.ijsrd.com*

technologies are utilized in many government projects, banking security systems, workforce management, etc. it's possible thanks to the scalability of its solutions.

G. Flexibility

Definitely biometric systems are the foremost flexible security solution. You've got your own security credentials with you so you don't must bother memorizing awkward alphabets, numbers and symbols required for creating a flowery password.

H. Trustable

Reports claim that the young generations trust biometric solutions over other solutions. Banks have already started using biometric security systems to spice up the protection and reliability for his or her customers.

I. Save Time

Biometric solutions are highly time conserving. In most cases, you simply have to put your finger on a tool or observe a retina device to pass the system. On the opposite hand, traditional methods have layers of hassles and interrogations which become annoying and unbearable.

J. Save Money

Governments are putting their money to form a national biometric database in order that government services may be provided to the people with more accuracy and less cost. Corporations are adopting biometric system to urge accurate information which saves both time and money. With bit money, any company can track their employees and reduce the additional costs they're paying for years.

VII. Disadvantages of Biometrics

Technology is constructed to enhance the standard of our life. It brings betterments within the way of our life in every aspect. Biometric technology is additionally an excellent invention that brings significant changes in our lifestyle. As said, with state comes even greater responsibility, biometric technology may be an ideal of this quote. With all the Goosebumps surrounding the positive news about biometrics, it also incorporates a dark side of its own. We all know little or no about the disadvantages of biometrics, compared to its well-known advantages.

While the introduction of biometrics brings many benefits, unfortunately, it also came with its own set of problems. You'll want to understand the disadvantages of biometrics technology. Here are some key points to contemplate regarding the disadvantages of biometrics:

A. Physical Traits don't seem to be Changeable:

Most of the biometric modalities work with physical traits like fingerprint, iris, palm vein, etc. We all have only a pair of eyes; a specific number of fingerprints, and other body parts that are unchangeable. We will reset a password, but we never can change our fingerprints or retina, these are fixed. Our biometric data is stored in respective government's databases or companies who enable such services.

Can they guarantee that these data will never be hacked or stolen from the server? Unfortunately, it's already happening around us. There is news about data breach of billions of Indians' private data from the Aadhaar database. A large-scale breach materialized at the centralized Office of non-public Management in US where 5.6 million workers' fingerprints were stolen in 2015. You'll change your password if it's stolen, but you've got no choice to change your fingerprint in anyway.

B. Error Rate:

Biometric machines are but perfect and mistakes can happen. Usually, biometric devices make two sorts of errors, False Acceptance Rate (FAR) and False Rejection Rate (FRR). When the device accepts an unauthorized person, it's called FAR and when it rejects a licensed person, it's called FRR.

The error rate in some cases is so high that it creates great chaos for the whole security system. It could happen thanks to weather, strength, age and other issues. Turmoil could happen with a slip-up rate of as low as 1% during a large-scale authentication process.

C. Cost:

The costs of biometric devices are comparatively beyond other traditional security devices. The prices of biometric software, devices, programmers, server and other relative equipment combined may be a great deal of cash.

D. Delay:

Some biometric devices take quite the accepted time and a protracted queue of workers form waiting to be enrolled in large companies. In these cases, people get hard time while scanning the biometric device a day. It's hard for an individual when he/she needs to undergo a biometric verification system before going in school, office or other places a day.

E. Complexity:

One of the most important disadvantages of biometrics is that the highly technical and complicated system that creates up the entire process. A non-techy person is going to be flopping like fish out of water when trying to know the system. Companies hire highly experienced and skilled programmers to develop the system, so it requires programmers for managing the system similarly.

F. Unhygienic:

There are various sorts of biometric modalities. A number of them are contact based like fingerprint and palm vein scanner; some are contactless like iris and face recognition, etc. In contact-based modalities, a biometric device is employed zillion times by enormous amount of individuals. Everyone is actually sharing their germs with one another via the device. You never know what you're taking with you after placing your finger on the device. You wouldn't have any choice to change the system.

G. Scanning Difficulty:

Some biometric modalities like iris scan can undergo scanning difficulties. It happens thanks to several reasons including eyelashes, eyelids, lens and reflections from the cornea. For these reasons, identity verification might not be as reliable to be used.

All rights reserved by www.ijsrd.com

H. Physical Disability:

Some people aren't fortunate enough to be ready to participate within the enrollment process. They may have lost or damaged body parts like fingers or eyes. During this kind of case, a fingerprint/ Iris recognition device to acknowledge would be embarrassing and easily offensive. These sorts of people will surely pass a tough time to cope up with others within the system.

I. Environment and Usage Matters:

Environment and usage can affect the measurements taken. Especially in highly cold areas, the error rate is higher which creates unnecessary chaos and disappointments over the entire system.

J. Additional Hardware Integration:

Some biometric modalities need additional hardware integration which is dear, inconvenient and complicated. It's hard to manage these sorts of modalities.

REFERENCES

[1] Biometrics: authentication & identification (definition, trends, use cases, laws and latest news) - 2020 review www.gemalto.com
[2] What is biometrics? 10 physical and Behavioral identifiers that can be used for authentication www.csoonline.com
[3] Marcos Faundez-Zanuy Biometric security technology www.researchgate.net
[4] Advantages and Disadvantages of Biometrics www.ukdiss.com
[5] Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A (eds.). Handbook of Biometrics.
[6] Biometric-authentication www.ilantus.com
[7] biometrictoday.com
[8] https://findbiometrics.com/exclusive/articles/
[9] https://findbiometrics.com/exclusive/articles/
[10] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1490310/
[11] http://www.scholarpedia.org/article/Biometric_authentication
[12] https://www.sestek.com/2016/11/advantages-disadvantages-biometric-authentication/
[13] Prints charming: how fingerprints are trailblazing mainstream biometrics – Paul Lee
[14] Facing the future: the impact of Apple Face ID - Andrew Bud
[15] Biometrics becoming must-have for fraud prevention - Charlotte Hill
[16] R. Ang, R. Safavi-Naini, and L. McAven, "Cancellable key-based fingerprint templates," in Proceedings of the 10th Australasian Conference on Information Security and Privacy, ACISP 2005, pp. 242–252, July 2005.View at: Google Scholar
[17] A. Kümmel and C. Vielhauer, "Reverse-engineer methods on a biometric hash algorithm for dynamic handwriting," in Proceedings of the 12th ACM Multimedia Security Workshop, MM and Sec'10, pp. 67–72, September 2010.
[18] K. Dewangan and M. A. Siddhiqui, "Human identification and verification using iris recognition by calculating hamming distance," International Journal of Soft Computing and Engineering (IJSCE), vol. 2, 2012.
[19] Biometric Surveillance and the Right to Privacy - By Angus Willoughby on October 5th, 2017 in Commentary, Ethics, Magazine Articles, Privacy & Security
[20] How Biometrics May Be Key In Reducing The Hassles Of Travel - By Jimmy Samartzis and Helena Bononi
[21] Security Vulnerabilities Against Fingerprint Biometric System(Article)

All rights reserved by *www.ijsrd.com*