BIOMETRIC SECURITY IN MOBILE AGE

Sayali Vanjari[1] , Prof D.G.Vyawahare[2]

[1]*Student,Dept.of CSE Engineering, Anuradha College ,Maharashtra, India*
[2] *Professor, Dept. of CSE Engineering, Anuradha college, Maharashtra ,India*

---***---

Abstract - *In human ID biometrics is one of the greatest propensities. These days, in numerous genuine applications like legal, security and other ID and acknowledgment purposes biometrics is generally utilized. Here we have talked about and correlations of various biometric includes alongside their employments. In biometrics unique mark is the most generally utilized. Much further multimodal biometrics can enhance the dependability and execution of biometric confirmation. Lately, biometric verification has turned out to be standard on top of the line purchaser cell phones, most much of the time as circumspect unique mark perusers, yet in addition as iris scanners. Producers like Apple and Samsung have avoided potential risk when planning these highlights to guarantee that individual biometric information remains encoded on-gadget, failing to be sent over the web and put away on remote servers And we additionally take a gander at the eventual fate of biometrics and prospective wearable innovation. We at that point propose the possibility of two factor confirmation and a unique mark database.*

Key Words: **Biometric System, Identification, Recognition, Security, Reliability, Performance.**

1.INTRODUCTION

Biometric terms originates from the Greek words profiles (life) and metric (measure).Biometric frameworks are robotized techniques for perceiving or confirming the living individual personality based on some physiological attributes, similar to confront example, unique mark and hand, or a few parts of conduct, similar to keystroke examples, mark and voice. No framework can be secure totally. Thus, it is exceptionally hard to trade off the system.[4]

The security turns out to be more nosy, if the framework is more secure. Bertillon age is the main kind of biometrics came into shape in 1890, made by an anthropologist named Alphonse Bertillon. He construct his framework in light of the claim that estimation of grown-up bones does not change after the age of 20.[2]

Biometric technique comprising of different body estimations of a man like stature, a safe distance, expansiveness and circuit of the head, the length of lower arms, the length of various finger, length of feet and so forth.

The cell phone has turned into an indistinguishable partner for some, clients, serving for considerably more than just correspondence. It is a multi-reason gadget which satisfies critical capacities in the client's close to home and expert life. In parallel, the capacity abilities of cell phones increment quickly, and telephones would today be able to create and store a lot of various substance composes (archives, sends, visual and sound media, databases, etc.)[4].

All and every, cell phone look like in their capacities PCs or netbooks with implanted communication abilities. Be that as it may, one of the perspectives in which cell phones fall behind is security and information assurance . Customary security gives just a one-time confirmation framework upon switch on: unless bolted, the gadget is constantly open; and programmed bolting of the gadget is normally not the default setup on the telephones of the main 5 sellers [6].

Numerous clients keep their gadgets unsecured as they see the utilization of a telephone PIN(not the SIM PIN) as badly arranged . To call the innovation of the cell phone a mechanical upheaval would be putting it mildly. The cell phone has quickly changed how people connect with data, and in addition how they associate with each other. The cell phone has likewise quickly changed what it implies for a human to utilize a "computer".[6]

As PC innovation has progressively turned out to be more scaled down and intense, so have strategies for individual verification. It's currently normal to discover a cell phone that sweeps a unique mark in a small amount of a moment as a method for confirming its proprietor; truth be told, it's presently evaluated that more than 600 million telephones with biometric scanners are being used all inclusive. [14]

This biometric achievement has the capacity to include another measurement of security to the versatile universe, and in a few regards, it has prevailing with regards to doing as such. In any case, however present day biometric verification advances keep individual biometric information safe and scrambled, and however they have prompted an expansion in the general level of portable of security, a more intensive look uncovers these frameworks to be helpful yet inadequate security arrangements that, when traded off, are rendered to a great extent useless.[6]

1.1 Literature Review

The first biometrics in practice was a form of finger printing being used in China in the 14th century, as reported by explorer Joao de Barros. He wrote that the Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the young children from one another. Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. An early cataloging of fingerprints dates back to 1891 when Juan Vucetich started a collection of fingerprints of criminals in Argentina. The History of Fingerprints. Josh Ellenbogen and Nitzan Lebovic argued that Biometrics is originated in the identificatory systems of criminal activity developed by Alphonse Bertillon (1853–1914) and developed by Francis Galton's theory of fingerprints and physiognomy. According to Lebovic, Galton's work "led to the application of mathematical models to fingerprints, phrenology, and facial characteristics", as part of "absolute identification" and "a key to both inclusion and exclusion" of populations. Accordingly, "the biometric system is the absolute political weapon of our era" and a form of "soft control"[7].

Anil K. Jain (2014)

Focused on biometric template security which is an important issue because,unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued. Protecting the template is a challenging task due to intra-user variability in the acquired biometric traits.He resent an overview of various biometric template protection schemes and discuss their advantages and limitations in terms of security, revocability, and impact on matching accuracy.

Kumar D (2014)

Discussed about the problem that a person has to take many cards and has to remember their passwords or secret codes and to keep secure to take with him all time.

Here a biometric the fingerprints payment system is used for various kinds of payment system. Biometric fingerprints payment system is much safe and secure and very easy to use and even without using any password or secret codes to remember as compare with previous system like credit card payment system, wireless system and mobile system etc Biometric fingerprints payment system is reliable and expensive and it has more advantages as compare with others

Khan, M.K. (2010)

Covers the ethics, privacy and security of biometrics. Also an in-depth review of the state of the art in what is sometimes called biometric template protection, including biometric encryption, fuzzy vaults, fuzzy extractors, biometric hashing, and cancelable biometrics.

Also covers a security analysis of these technologies including the published attacks.

Brindha, V.E. (2011):-

Presented about protection of fingerprint template from creation of physical spoof and replacement by imposter's template to gain unauthorized access by transformation based approaches and biometric cryptosystems.

The security of the fuzzyvault depends on the infeasibility of the polynomial reconstruction and the number of chaff points. In the proposed system an even more secured fuzzy vault is generated with combined features of fingerprint and palm print to enhance the security of the template stored.

1.2 Architecture

Proposed System:-

Technology is ever changing. In a world like ours we are constantly seeking the next big discovery, invention, what have you. One of the biggest influences of our daily lives right now is the internet. With that comes the idea of carrying the internet in our pocket, more specifically, the use of a smartphone.

Advances in smartphones requires equal advances in security. In a perfect world, we would not need to worry about security authentication, back-ups, passwords, etc. But we do not live in that perfect world. Things we physically own or ideas we write down, including intellectual property, need protecting.[11]

In all honesty, the point of the fingerprint reader is to save time, and to force people to implement some form of security on their devices, which often store very sensitive data.

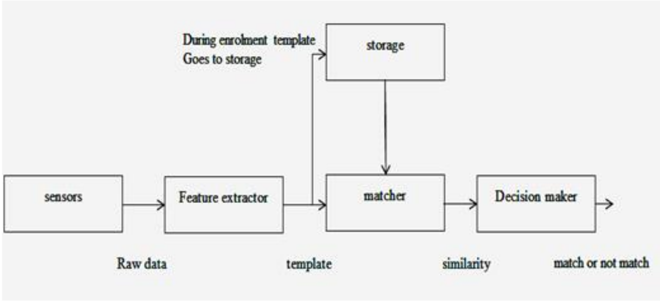


Fig-1: Architecture of biometric security in mobile

1.3 Biometrics mean

Biometrics = bios + metron. Bios means life and metron means measure Recognizing humans based on physical and behavioral traits. Also called BEHAVIOMETRICS.

1.4 Classification of Biometrics

Physiological are related to the shape of the body.
Behavioral are related to the behavior of a person.

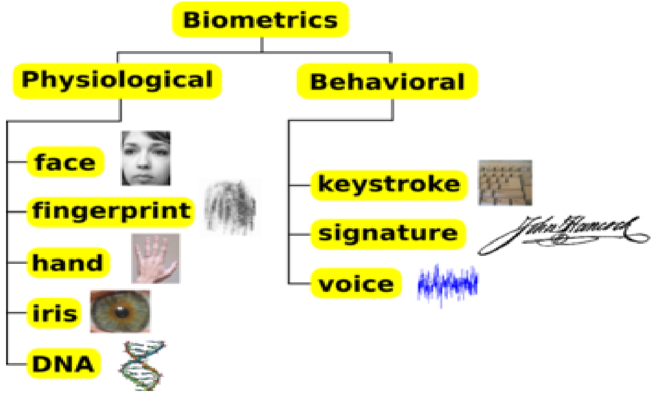


Fig-2:Classification of Biometrics

1.5 Physical biometrics

Fingerprint—Analyzing fingertip patterns
Facial recognition/face location—Measuring facial characteristics
Hand geometry—Measuring the shape of the hand
Iris scan—Analyzing features of colored ring of the eye.
Retinal scan—Analyzing blood vessels in the eye
Vascular patterns—Analyzing vein patterns
DNA—Analyzing genetic makeup.
Earprint—this method is based on geometric distances, force field transformation

1.6 Behavioral biometrics

Speaker/voice recognition—Analyzing vocal behavior
Signature/handwriting—Analyzing signature dynamics
Keystroke/patterning—Measuring the time spacing of typed words

BIOMETRIC	FINGERPRINT	FACE	HAND GEOMETRY	IRIS	VOICE
Barriers to universality	Dirt, Dryness	Hair, Glasses, Age	Hand Injury	Poor Lighting	Noise, Clouds
Distinctiveness	High	Low	Medium	High	Low
Performance	High	Medium	Medium	High	Low
Collectivity	Medium	High	High	Medium	Medium
Performance	High	Low	Medium	High	Low
Acceptability	Medium	High	Medium	Low	High
Potential for circumvention	Low	High	Medium	Low	High

Table 1:- Comparison Between Different Technique

1.7 What is "Biometric Security in Mobile Devices"

"Biometrics is the identification or verification of human identity through the measurement of repeatable physiological and behavioral characteristics "

A mobile device is a handheld tablet or other device that is made for portability, and is therefore both compact and lightweight.[13]

1.8 working of biometric system in mobile

Steps:

Capturing
Pre-processing
Feature extraction
Template matching
Matcher/Comparison
Application Device

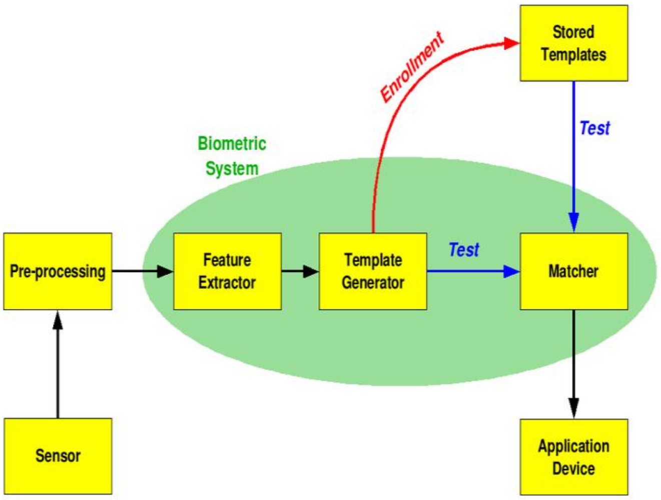


Fig-3:Working of biometric system in mobile

1.9 All biometric system works in a four- stage process that consists of the following steps

Capture: A biometric system collects the sample of biometric features like fingerprint, voice etc. of the person who wants to login to the system.

Extraction: The data extraction is done uniquely from the sample and a template is created.

Comparison: The template is then compared with a new sample.

Match/non-match: The system then decides whether the features extracted from the new sample are a match or a non-match with the template.

1.10 Need of Biometric security in mobile:-

Data

Privacy

Security

1.11 Data

Messages
Photos
Videos
Secured Card Information
Wallet Information
Apps local data

1.12 Security

In traditional methods of personal recognition such as passwords, PINs, keys, and tokens work for positive recognition, only biometrics can be used for negative recognition.

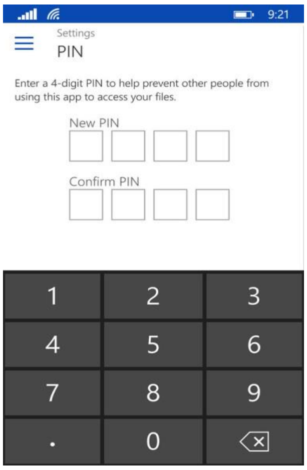
The purpose of negative recognition is to prevent a single person from using multiple identities

Biometrics cannot be lost or forgotten. They are difficult for attackers to forge and for users to repudiate.

1.13 Privacy

If the biometric data is recorded in a central database, privacy concerns may be higher than for systems where an individual's data is stored only on a card retained by the individual. However, some biometric applications require a central database for their basic functionality

The purpose of data protection legislation is to ensure that personal data is not processed without the knowledge and, except in certain cases, the consent of the data subject.[15]



9:21
Settings
PIN

Enter a 4-digit PIN to help prevent other people from using this app to access your files.

New PIN

Confirm PIN

2. Biometric Security Methods in mobile

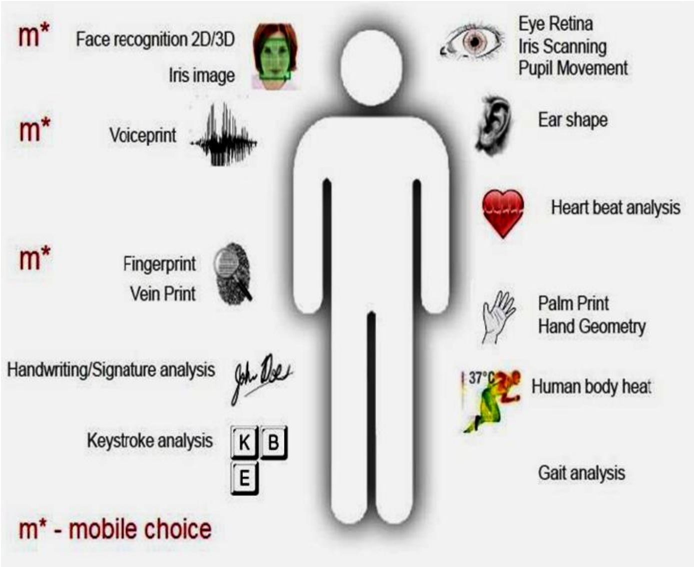


Fig-4: Biometric security Methods in mobile

2.1 Apple iPhone

Apple controls both the equipment and programming of the iPhone, giving it broad control over its whole security biological system. This control enables Apple to make some sweeping security choices, for example, the incorporation of verification contributes Lightning links.

These chips permit iOS gadgets to check and check whether the link is from an approved maker, decreasing the possibility of incognito malware injection.8 As a stage, the iPhone sparkles for instance of what should be possible whenever equipment and programming both collaborate for security.

The Apple iPhone initially started utilizing biometrics with the arrival of the iPhone 5S of every 2013.9 Its usage incorporates both the Touch ID unique mark sensor itself, and also the "safe 8 T enclave" in Apple's processor.

The enclave inside each telephone contains a one of a kind computerized identifier not known to Apple, implying that Apple has no indirect access into the system.10 The enclave boots independently from whatever is left of the telephone, and any associations amongst it and other telephone parts happen in scrambled memory.11 Furthermore, Apple's custom processor is planned so that at the point when Touch ID unique mark information is perused by the sensor, it is sent to the protected enclave, yet Apple's processor itself can't read it.12 The greater part of this meets up to make Touch ID on iPhone a very secure framework.

Despite the fact that fingerprints are not hashed, their scrambled computerized portrayals are segregated with the end goal that they can never leave the safe enclave, guaranteeing that entrance to the encoded portrayals is close difficult to accomplish. Unique mark information never leaves the gadget and is never put away decoded, so clients ought to have no down to earth worry about the information regularly being secretively stolen by vindictive applications or government associations. The equipment just does not take into account it.

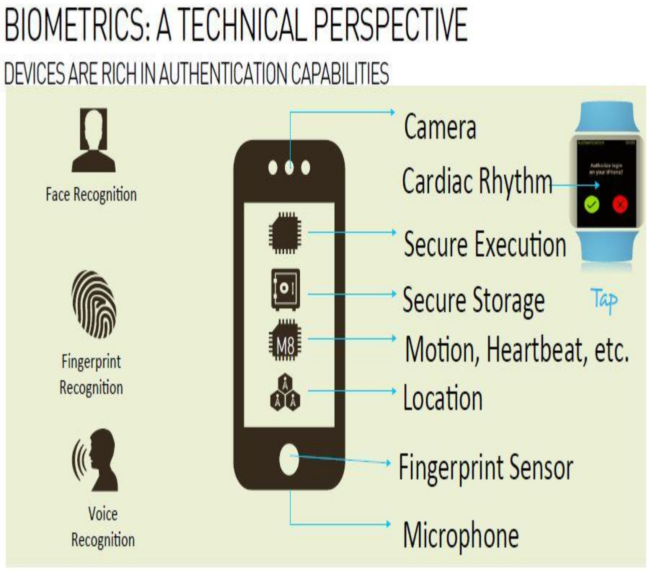


Fig -5:Biometrics techniques in mobiles

2.2 Samsung Galaxy

Samsung outlines and fabricates cell phones that run Google's Android working framework, implying that Samsung does not have a similar aggregate best down control of the security biological community that Apple does. Be that as it may, as Android is open source, Samsung can alter the stage to better suit its telephones and their highlights. This paper will center around Samsung's Galaxy Note 7 – which, before a universal review because of battery issues, spoke to Samsung's most security-centered telephone to date.

The Galaxy Note 7 incorporates Samsung's Knox security stage, which is based over the Android working framework. Like Apple's iPhone, Knox on the Galaxy Note 7 assembles a lot of its security and encryption from the telephone's extraordinary advanced identifier.13 It offers confined workspaces for work and individual use, and in addition a custom envelope where individual applications and records can be put away scrambled.

This encoded information can't be unscrambled by the gadget without client mediation. The telephone has an iris scanner at the highest point of the gadget that has a comparable client interface to Touch ID; it just requires an output of the client's eye to verify. Samsung takes note of that iris checks are put away as "encoded code", however no parallel to Apple's safe enclave exists in the processor.14 This implies, in the impossible occasion that the encryption calculation utilized was broken, the biometric information could be carefully accessible to an assailant, instead of being secured by physical disengagement.

At last, however Apple may have Samsung beat with its level of equipment bolster, both makers have completed a to a great degree intensive occupation of building a protected versatile biological system. Tragically, neither one of the systems is immaculate, due to some extent to biometrics being effortlessly imitable, and to some degree because of execution.

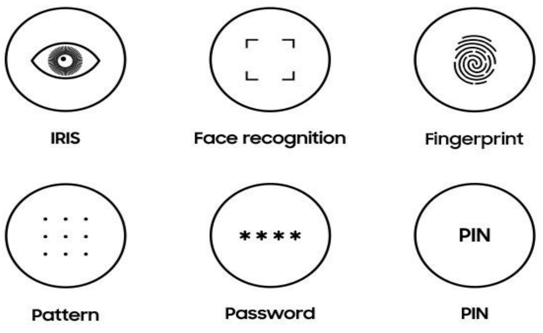


Fig-6 biometric technica in mobile

2.3 Shortcomings and Defenses

In 2013, Apple's Touch ID was demonstrated uncertain by an analyst, offering conversation starters about exactly how beneficial and private fingerprints are for confirmation. Marc Rogers, a security analyst, point by point his procedure of lifting a unique mark and remaking it with a notable strategy that produces counterfeit prints made of dried paste.

Rogers was effectively ready to trick the Touch ID sensor on the iPhone 5S, implying that full telephone access could be accomplished if an enlisted unique finger impression of the telephone's client could be lifted – an included assignment, however effortlessly possible by an aggressor persuaded to get into an iPhone.

Attacks like this are not new, with comparative vulnerabilities being reported in the mid 2000s.16 Unfortunately, the present weakness exhibits that in one case, buyer review unique mark acknowledgment innovation doesn't do what's necessary to keep this kind of assault. Iris filtering has additionally been refered to as potentially unreliable, with examine exhibiting that high-determination iris symbolism can effectively go as a genuine eye.

Jan Krissler, a security scientist in the biometric space, has possessed the capacity to break iris acknowledgment frameworks utilizing high determination symbolism of eyes found on the web, for example, those of Vladimir Putin.17 Though the false iris print must be printed with a high number of specks per inch, the iris picture itself doesn't need to be a restrictively high determination: "We have figured out how to trick a business framework with a print out down to an iris distance across of 75 pixels," claims Krissler.

This implies there are a lot of typical photographs on the web that could be effectively utilized – photographs of world pioneers, big names, and more. Despite the fact that Krissler won't talk freely about the defenselessness until 2017, it could genuinely raise doubt about the authenticity of innocent iris filtering for biometric security. This underscores the need of utilizing more intelligent programming components to enlarge biometric filtering.

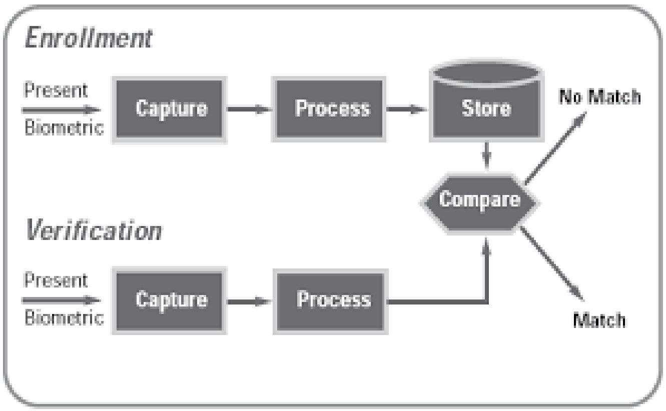


Fig- 7: Working of biometric security in mobile

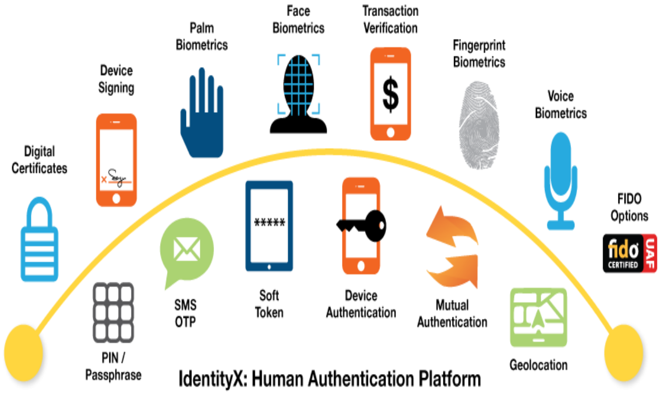


Fig-8: Human authentication platform

2.4 Authentication Process

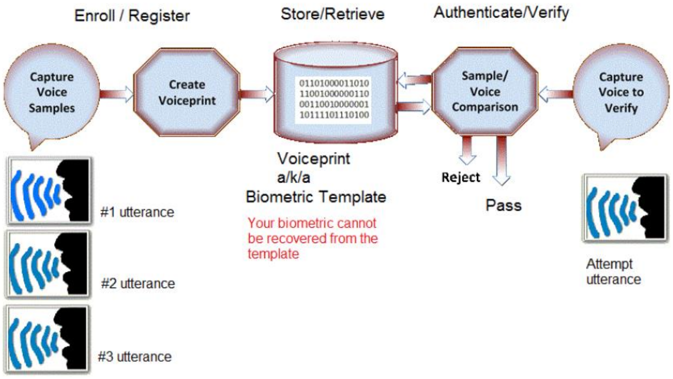


Fig-9: Authentication Process

2.5 Two Factor Authentication

You can have enabled Two factor authentication on your accounts via the Google Authenticator app, which provides users with a randomly generated token that expires after 30 seconds. However where exactly is that app located, on the phone of course. [12]

Another question that might be asked is how can this happen my fingerprint biometrics cannot be hacked. On the contrary as human beings we leave our finger prints everywhere, anything we touch, the fingerprint can be lifted and copied to create a fingerprint a sensor would not know was real or not.[10]

In addition "As Deloitte & Touché researchers noted way back in 2006, spoofing a person's biometrics, particularly fingerprints (using lifted prints on gummy bears), and is a legitimate threat. However, it's the second problem with biometrics that is the really big one: once a person's biometrics have been compromised, they will always be compromised." [2]

So the question that remains is how can we use this unique trait, and is it even worth our time and investment? Although like anything having to do with technology, it will continue to get better, and now that it has been integrated with one, if not the most popular brandings other manufactures will follow suit and implement those in their phones. So essentially it comes down to us computer scientists.[12]

We need to create solutions to resolve this issue, and others to come in the future. The main advantage that comes to mind is since it is not secure enough to be used alone, it will enhance security since it can be used as a layered defense strategy, which is also used in Network Security. Like with anything, two things are better than one, and the same is true here. I suggest a fix to this problem is to implement a two-factor option which can be enabled by the user via it settings. Not only should a user be able to authenticate themselves via the fingerprint readers, but they should also have to enter a pin passcode. These two together will greatly increase its security.[9]

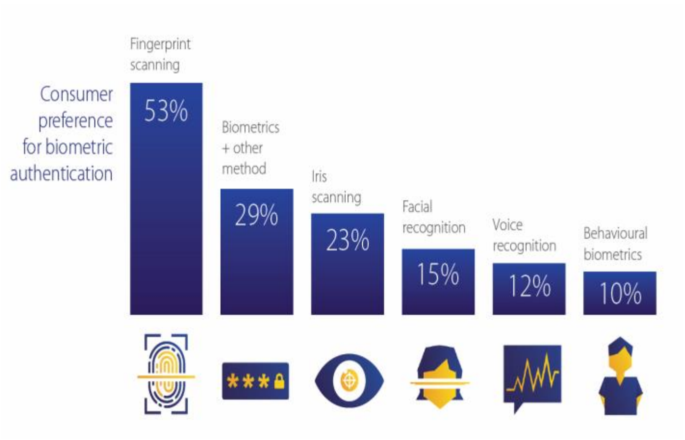


Fig-10: Consumer preference for biometric authentication

2.6 Apple's Fingerprint Hardware

1. Mobile Phone:-

Just about 3 years ago, Apple came up with fingerprint biometrics for the first time on its device iPhone 5s. It was the first successful attempt at integrating a fingerprint sensor onto a mobile device. 2016 witnessed a major increase in devices equipped with fingerprint sensors. Biometric softwares leverage the built-in applications for authentication. Camera for fingerprint and facial recognition. Microphone for voice and touch screen for behavioral capabilities. By the end of 2017, about a billion functional mobile phones would be in circulation throughout the world. Also, there were a few unsuccessful attempts at iris identification as well. Coupled with fingerprint recognition, iris identification would substantially augment the security level.[1].

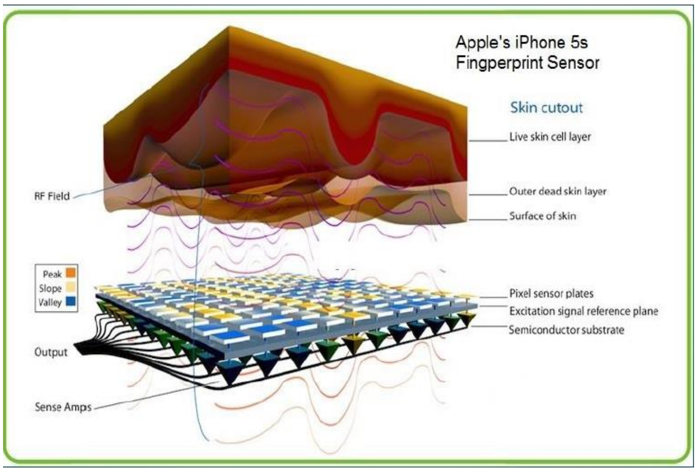


Fig-11: Apple's Fingerprint Hardware

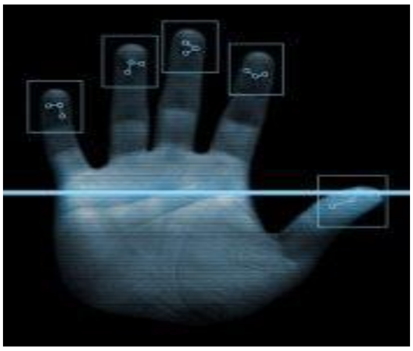
2.7 Uniqueness

Since biometrics are unique to the individual that they are describing, they tend to be more secure than previous methods of identification and access control. Previous methods for these include photo identification and written passwords. It is much more difficult to fake a retina scanner or palm print than to guess a password or create fake photo identification

Typing a password or constantly carrying photo identification is also much more of a hassle than placing your palm or eye up to a scanner. Granted the first two methods are not an enormous inconvenience or incredibly difficult, the latter two methods are much easier. Also, a password or photo identification card can be lost or forgotten, whereas a hand or eye cannot be.

This contributes to the security of biometrics because not only is it more difficult to fake a palm scanner or retina scanner, but also the authorized individual cannot give or loose these to an unauthorized user When biometric data is taken, it verifies certain parts of the scan as match points. These match points are then converted to numeric data via an algorithm.

Then, this numeric data is compared to verified match points of how the scan is supposed to be. If the new numeric data is compared and accepted, the new scan is approved. If the data is rejected, then the new scan is denied. Also, all of this information is immediately encrypted to help decrease the chances of identity theft. [3]



1.8 Principles of Biometrics

Biometric technology needs to contain a few principles in order for it to be used. The first is that every person needs to contain whatever biological part is being analyzed (ex. If implementing a palm scanner in a business, every employee needs to have a hand). Next, the biological trait needs to be unique and permanent to every individual (ex. All humans have different palm and fingerprints and these prints do not become unrecognizable over time).[8]

Measurability and performance are the next principles; they also overlap a little. Measurability means that this trait needs to be able to measured (ex. Fingerprints) and performance means that this measurement needs to happen fast and it needs to be accurate and reliable.

The final two principles are acceptability and circumvention. This technology needs to be so secure so that the individual providing the scan needs to feel secure and not worried, and also the one protecting the information (ex. The employer) needs to feel safe that their private information is guarded by this biometric security.

Biometric devices consist of a reader or scanning device software that converts the gathered information into digital form, and a database that stores the biometric data with comparison with existing records.[8]

2.9 Advantages and Limitation

Advantages

- Fingerprints are unique to individuals.
- Human biometric features are unique.
- Very Economical.
- Highest factor of security.
- Hidden characteristics are used as biometric features.
- One time registry and usage throughout life.
- It is not affected by dryness or roughness of skin or by physical injury on surface of the hand.

Limitation

- Face recognition system can't tell the difference between identical twins.
- The finger print of those people working in Chemical industries are often affected. Therefore these companies should not use the finger print mode of authentication.
- It is found that with age, the voice of a person differs. Also when the person has flu or throat infection the voice changes or if there are too much noise in the environment this method may not authenticate correctly. Therefore this method of verification is not workable all the time.
- For people affected with diabetes, the eyes get affected resulting in differences. Biometrics is an expensive security solution.

2.10 Applications

There are few applications base on the proposed system are as follows:

Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks.

It can be used during transactions conducted by telephone and Internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with keyless entry devices.

Criminal identification.
Prevents unauthorized access to private data.
Financial transaction management.

3. CONCLUSIONS

In this paper we have explained the Biometric Security in mobile age . It also explain about Biometric authentication Biometrics are a powerful mechanism for authentication, but their current implementation on mobile devices is incomplete and insecure. Biometrics can succeed because they are an immediate and natural way for people to carry around a personal and physically-identifying token.

Future Scope

As the future progresses, biometrics will become more entwined with it. Currently, the largest biometrics database system is in India, it's called the "Aadhaar." It's India's National ID program. It is a biometric identity which will follow an individual their entire lifetime. Also, it's accessible and verifiable instantly, anytime, and anyplace.

Some hospitals use biometric systems to make sure mothers take home the right newborns.

New methods that use DNA, nail bed structure, teeth, ear shapes, body odor, skin patterns and blood pulses
More accurate home-use systems

Opt-in club memberships, frequent buyer programs and rapid checkout systems with biometric security

REFERENCES

[1] Aitel,.Dave. USAToday. "Why fingerprints, other biometrics don't work".

[2] Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp.

[3] Sutherland, Lennard-Peter. "biometrics." Search Security. .

[4] Khan ,m.k. Biometrics Security." RSS 20. N.p., n.d. 1st Edition

[5] R. Palaniappan, "Biometric data safe and encrypted" published in E. Corchado et al. (eds): Intelligent Data Engineering and Automated Learning – IDEAL 2006, Lecture Notes in Computer Science, vol. 4224, pp. 604–611, Springer-Verlag, Berlin Heidelberg,

[6] Zahid Akhtar, "Security of Multimodal Biometric Systems against Spoof Attacks", Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy,

[7] Nitzan Lebovic, "Biometrics or the Power of the Radical Center", in Critical Inquiry 41:4 (Summer, 2015)

[8] Anil k.jain "Biometrics Security Considerations." Systems and Network Analysis Center Information Assurance Directorate. NSA, n.d. . 2nd Edition.

[9] Sutherland, Lennard-Peter. "biometrics." Search Security. N.p., n.d. 3rd Edition.

[10] Weaver, A. C. (2006). "Biometric Authentication". Computer.

[11] Damaševičius, R.Maskeliūnas, R.; Venčkauskas, A.; Woźniak, M. Smartphone User Identity Verification Using Gait Characteristics,

[12] Kumar D and Brindha V.E."Biometric Authentication".

[13] Jain, A.; Hong, L. and Pankanti, S. (2000). "Biometric Identification". Communications

[14] Jain, A. K.; Bolle,., eds.(1999). Biometrics:Personal Identification/authentication.in Networked Society. Kluwer Academic Publications.

[15] Debnath Bhattacharyya,Rahul Ranjan ,Poulami Das,Tai Hoon Kim,Samir Kumar Bandyopadhyay,7 Need of Biometric security in mobile and Its Future probabilities. IEEE Trans Int. conf. On Computer

BIOGRAPHIES:-

Miss. Sayali Vanjari pursuing Bachelor of Engineering in Computer Science & Engineering Department from Anuradha Engineering College of SGBAU Amaravati