Name of Faculty: Shubha Mishra

Designation: Assistant Professor

Department: Information Technology

Subject & Subject Code: WMC & IT-602

Unit: V

Topic: Biometric authentication

LNCT GROUP OF COLLEGES "WORKING TOWARDS BEING THE BEST"

Biometric Authentication

What is biometric authentication?

Biometric authentication is simply the process of verifying your identity using your measurements or other unique characteristics of your body, then logging you in a service, an app, a device and so on. biometrics is the name for any type of body measurements and calculations. Biometric identification verifies you are **you** based on your body measurements. Biometric authentication goes one step further and uses that information to compare you against a database and enters your information in a service.

Think of it like this: biometric **identification** is like a neighbor who looks through the peeping hole at the 2 people who just rung the bell. The neighbor decides which one of them is Dave based on height, hair color, eye color and so on. Biometric **authentication** is the neighbor who looks through the peeping hole to see who is calling the door. If it's Dave, the neighbor lets him in. If it's not Dave, the door remains shut.

How biometric authentication works

Biometric authentication works by comparing two sets of data: the first one is preset by the owner of the device, while the second one belongs to a device visitor. If the two data are nearly identical, the device knows that "visitor" and "owner" are one and the same, and gives access to the person.

The important thing to note is that the match between the two data sets has to be **nearly identical** but not **exactly identical**. This is because it's close to impossible for 2 biometric data to match 100%. For instance, you might have a slightly sweaty finger or a tiny, tiny scar that changes the print pattern.

Designing the process so that it doesn't require an exact match greatly diminishes the chance of a false negative (the device doesn't recognize your fingerprint) but also increases the odds that a fake fingerprint might be considered genuine.

Popular biometric authentication methods and how they work

There are quite a few types of identifying a user by way of his own body. Below are the most popular biometric technologies that have made their way into users' hands.

Fingerprint Scanners and how they are stored

There are three types of fingerprint scanners: **optical, capacitive** and **ultrasound.**

An **optical scanner** takes a photo of the finger, identifies the print pattern, and then compiles it into an identification code.

A **capacitive scanner** works by measuring electrical signals sent from the finger to the scanner. Print ridges directly touch the scanner, sending electrical current, while the valleys between print ridges create air gaps. A capacitive scanner basically maps out these contact points and air gaps, resulting in an absolutely unique pattern. These are ones used in smartphones and laptops.

Ultrasonic scanners will make their appearance in the newest generation of smartphones. Basically, these will emit ultrasounds that will reflect back into the scanner. Similar to a capacitive one, it forms a map of the finger unique to the individual.

How are your fingerprints stored?

Both Google and Apple store your fingerprint on the device itself and do not make a copy of it on their own servers.

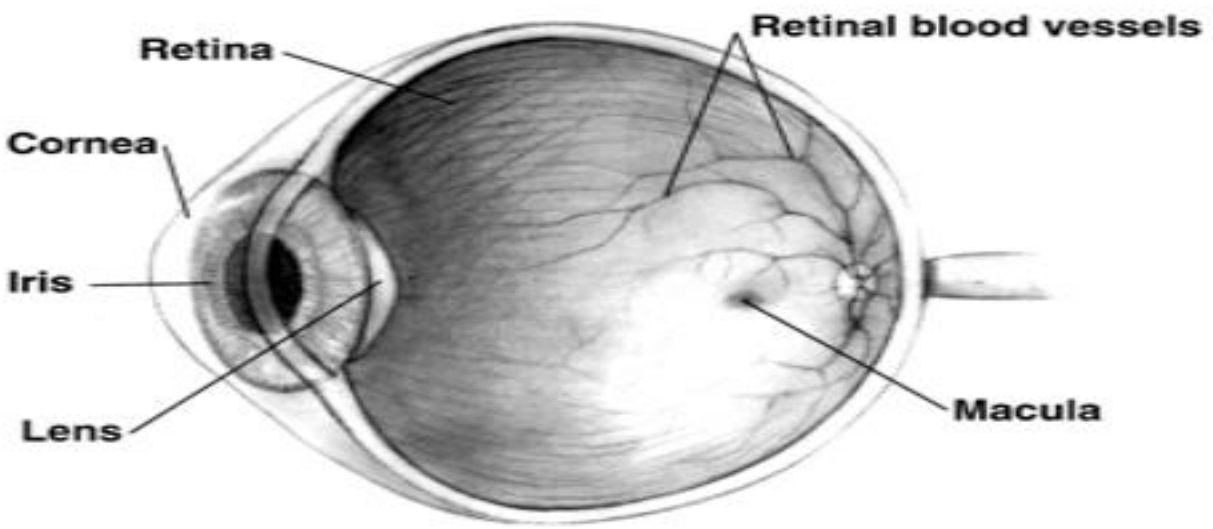
Apple's TouchID won't store the actual image of the fingerprint, but a **mathematical representation** of it. So even if a malicious hacker reaches this mathematical representation, he cannot reverse engineer it to reveal an actual image of your fingerprint. Not only that, but **the fingerprint data itself is encrypted**.

As this security researcher pointed **out**, TouchID can be hacked but it's still an extremely safe method of biometric authentication. For someone to hack an iPhone using TouchID sensors, they would need a really good copy of someone's fingerprint. This will get them access to your unlocked phone, but not to a copy of your fingerprint, so it differs from stealing a password.

Eye scanners

Security researchers consider the eye as one of the most reliable body parts for biometric authentication since it the retina and iris remains almost completely unchanged during a person's lifetime.

A **retinal scan** will illuminate the complex blood vessels in a person's eye using infrared light, making them more visible than the surrounding tissue. Just like fingerprints, no two persons will ever have the same retinal pattern.



Iris scanners rely on high-quality photos or videos of one or both irises of a person. Irises too are unique to the individual. However, iris scanners have proven to be easy to trick simply by using a high-quality photograph of the subject's eyes or face.

GROUP OF COLLEGES
"WORKING TOWARDS BEING THE BEST"

How iris scanners work

When it comes to biometrics, the iris has several major advantages compared to a fingerprint: You don't spread the information around every time you touch something. The iris stays virtually unchanged throughout a person's life. A fingerprint, on the other hand, can be dirtied, scarred or eroded. You can't use a fingerprint with dirty or sweaty hands. Irises, however, have no such problem.

The only major disadvantage of an iris scanner is that **high-quality photos of your face or eyes** can trick the scanner and unlock the device.

Speaker recognition

Speaker recognition, unlike voice recognition, wants to identify **who** is talking, and not **what** is being said.

In order to identify the speaker, the specialized software will break down their words into packets of frequencies called formants. These packets of formants also include a user's tone, and together they form his voice print.

Speaker recognition technology is either:

Text-dependent, meaning it unlocks after identifying certain words or phrases (think "Hey Alexa!" for the Amazon Echo).

Text-independent, where it tries to recognize the voice itself but ignores what is actually said.

Unlike other methods mentioned here, speaker recognition comes with a significant usability problem, since it's easy for background noises to distort the person's voice and make it unrecognizable.

When it comes to consumer devices, voice activation can come across as awkward (a.k.a. talking to Siri in the subway).

But the biggest issue with speech recognition is how easy it is to create a high-quality reproduction of a person's voice. Even low-quality smartphones can accurately record a person's voice, complete with inflections, tone, and accents.

This hasn't stopped speaker recognition and similar technologies from gaining mainstream adoption. Just look at the success of Amazon Echo, Google Home, and other voice controlled speakers integrated into a lot of smart homes. *What do you get when you combine an Amazon Alexa with an Amazon Key that unlocks your home to couriers when you're at work?*

It's an amazing biometric authentication experience for users. At the same time, it's a security risk of nightmare proportions.

We don't mean just biometric authentication exploits, but "classic" hacker methods as well. Rhino Security Labs demonstrated just how to attack Amazon Key via WiFi so the camera is blind to whoever would enter your home.

Other biometric technologies

The methods above are the most well known and most popular, but not the only ones. Here are some other technologies:

Facial recognition systems

Generally speaking, facial recognition systems approach biometric authentication from a lot of angles.

The classic way is to simply extract your face's features from an image (eyes, nose, distance between your lips and your nose etc) and compare them to other images to find a match.

Through skin texture analysis, your unique lines, beauty marks, wrinkles and so on are turned into a mathematical space, which is then compared to other images.

Hand and finger geometry

While not as unique as prints, iris scanners or tridimensional face maps, our hands are different enough from other people's. That makes them a viable authentication method in certain cases.

A hand geometry scanner will measure palm thickness, finger length and width, knuckle distance and so on.

Advantages of this kind of system are cheapness, ease of use and unobtrusiveness. It also has a few major disadvantages. A hand's size can vary over the time. Health problems might limit movements. More importantly, a hand is not that unique, so the system has low accuracy.

Vein geometry

Our vein layout is completely unique and not even twins have the same vein geometry. In fact, the overall layout is different from hand one hand to another.

Veins have an added advantage since they are incredibly difficult to copy and steal because they are visible under tightly controlled circumstances.

Advantages and disadvantages of biometric authentication

Ultimately, biometric authentication techniques are all about security. As a feature, their main competitor is the password (or PIN code, on occasion), so a comparison between the two will reveal both their flaws and weaknesses. Let's see.

Advantage: Ease of use

A fingerprint or iris scan is much easier to use than a password, especially a long one. It only takes a second (if that) for the most modern smartphones to recognize a fingerprint and allow a user to access the phone. Ultrasound scanners will soon become commonplace, since

manufacturers can place them directly behind the screen, without taking any extra real estate on a phone.

Voice recognition, on the other hand, is a bit iffier and background noises can easily scramble the process and render it inoperable.

Disadvantage: You cannot revoke the fingerprint/iris/voice print remotely

A big disadvantage of biometric security is that a user cannot remotely alter them. If you lose access to an email, you can always initiate a remote recovery to help you regain control. During the process, you will be able to change your password or add two-factor authentication to double your account's security.

Biometrics, however, don't work like that. You have to be physically near the device to change its initial, secure data set.

A thief could steal your smartphone, create a fake finger, and then use it to unlock the phone at will. Unless you quickly locked your phone remotely, a thief would quickly steal every bit of information on the device.

Advantage: The malicious hacker has to be near you

The biggest advantage of biometrics is that a malicious hacker has to be in your physical proximity in order to collect the information required to bypass the login.

Disadvantage: "Master fingerprints" can trick many phones and scanners

When you first register a fingerprint, the device will ask you for multiple presses from different angles. These samples will then be used as the original data set to compare with subsequent unlock attempts.

References :

1. https://heimdalsecurity.com/
2. Self notes