BIOMETRICS - AUTHENTICATION AND ACCESS CONTROL SYSTEMS

Final Project Report

CIS-481-50

Spring 2022 - Group 10

Table of Contents

I. Executive Summary

We have all seen that futuristic technology featured in action movies and television shows, where the hero or the bad guy can break into a top-secret area using a high-profile individual's stolen fingerprint to access a scanner that opens steel doors and disarms laser sensors. That technology is biometrics, and it is not futuristic at all. We are already living in a time where this technology is real, and its use is quickly spreading to the everyday consumer applications and tools.

Biometrics implies the use of biological or behavioral attributes for the identification of an individual. The use of biometrics for top security and identification purposes is a very powerful tool, but it can also become very dangerous if not handled properly. There are some initial direct costs that should be considered when using this technology, like purchasing the proper hardware and software to facilitate full function, but technology advances so quickly that those costs will soon become negligible. The downside to that is stealing identities will take a new turn, and the consequences could be devastating.

Future developments and adoption of this technology and how aggressively it should be done depending on which entity will be supporting it. For example, the government would be more worried about accusations of violation of privacy than those using the technology in the medical field or consumer products like our smartphones.

In this report, we first discuss the different options of access control systems in the market today and then why biometrics is quickly becoming the option of choice with all its advantages and disadvantages. In the end, we discuss the options within the biometrics technology we could use for access control and make our recommendations.

II. Access control solutions

A. Brief description

The term “access control” refers to mechanisms or tools we use for the management of an access point, such as a door, keypad, or card reader, to only allow entry to authorized users.

Access control systems can be used today with almost any access point that uses an electronic lock mechanism. However, doors are the most common applications for access control.

B. Available options in the market today

There are many options available and many vendors in the market today, but all of them can be divided into three main categories, based on:

1. What the user ***has*** (object-based):

The user must *possess* a specific object to be granted entry. These can be considered legacy options. The most common are:

- Keys
- Fobs
- ID Cards

2. What the user ***knows*** (information-based):

The user must *know* a specific code to be granted entry. These are traditionally used for software/web portal access or in ATMs. The most common options are:

- Password
- Passphrase
- PIN number

3. Who the user ***is*** (biometric-based):

The user identification is made using his/her own body traits using biometrics. The most common biometric modalities include:

- Palm vein
- Fingerprint
- Iris scan
- Face recognition

This last category is the object of our report, which we describe in the following sections.

III. Why use biometrics for access control?

There are plenty of reasons to use biometrics for access control. The most important reasons to utilize biometrics for access control are the possibility of using more robust security levels and using human characteristics that cannot be lost or need replacement.

Organizations use biometric identification by relying on recognition. Like the way we as people use recognition to differentiate between friends, families, and other individuals, biometrics identification does this, but at an enormous scale. Just identifying through biometric identification allows the system to collect and document records as permitted.

Biometrics is recognized as a widely used authentication mechanism/ factor to identify an entity. This authentication mechanism is known as "something you are'', identifying someone through something that is unique and in their possession. This convenience allows one to be identified through fingerprint comparison, palm print comparison, hand geometry comparison, facial comparison (photographic ID card or digital camera), retinal print comparison, iris pattern comparison, signature comparison, and voice comparison. A biometric device is then used to compare the requested input and evaluate it to find verifiable matches. The more unique these characteristics are while limiting intrusion, the more advanced the authentication will be.

The Department of Homeland Security regularly uses biometrics for fingerprints and facial recognition. These aids prevent identity fraud and reject criminals and immigration violators from crossing the borders. The Department of Defense and the Department of Justice also use biometrics for similar purposes.

Similar entities in other countries also use biometrics for border protection. For example, thanks to this technology, Panamanian authorities identified 38 people linked to terrorist organizations trying to cross the border with Colombia in 2021 (La Estrella de Panama, 2022).

There are many other use cases for biometric access controls in segments like financial services, healthcare and medicine, and customer service.

The use of biometrics for personal access control was introduced for mass consumption with the release of newer smartphones like Apple's 2013 iPhone 5S with *TouchID* (fingerprint) and

2017 iPhone X *FaceID* recognition features. This allows phone users to check their phones without repeatedly entering their pins regularly. About half of smartphone users today use biometric technology without realizing it. Android phones like Google Pixel 6 series, Samsung Galaxy S21 series, OnePlus 9, and 9 Pro, also use this functionality.

Biometrics allows for stronger security levels in access control. There are two ways that it allows for this, one being through multi-factor verification. This requires multiple authentication mechanisms to be used, one being biometric and the other being either "something you know" or "something you have."

- The "something you know" consists of personal information or a PIN/ password. This is your Social Security number or ID information that you have memorized or hidden somewhere.
- The “something you have” consists of a smart card or ID that allows verification through encryption or showing a photo of the intended person.

Multi-factor verification presents more obstacles to unintended users and a greater security conviction.

Another way that biometric security allows for strengthened security is that it limits more unintentional threats. It is common for someone to lose their ID or smart card allowing for an unauthorized person to obtain possession of it to exploit or someone voluntarily sending passwords to an unauthorized person through psychological tricks. Biometric access controls reduce the probability of such risks.

Biometrics also provides unique characteristics by being irreplaceable. There is no need to memorize a password or change it every so often. No more hassles are due to losing or theft of an ID card or forgetting it at home and not being able to be at your desk on time. Biometric access controls eliminate these problems that are real with other mechanisms.

A. Advantages & disadvantages.

Like any other technology solution, biometrics has its advantages and disadvantages.

The main advantages are:

- Unlike traditional username/password authentication methods, biometric traits are harder to fake or replicate because human characteristics are universal (can be found in all individuals) and unique (differentiate one individual from another).
    - "The probability of two individuals sharing the same fingerprints is 1 in 64 billion. "To this day, no two fingerprints have been found to be identical" (Baker, 2021).
- It provides an easier authentication method for users (no need to memorize passwords, just scan your finger or face, and access is granted).
- Depending on the method used, authentication can be done without a centralized database, simply storing the data on a device such as an ID card or smart credit card.
- Reduced costs for companies by reducing the need to have security staff at access points or replacement of lost fobs or access cards

However, there are some disadvantages:

- Accurate and reliable biometric systems are expensive. A system with lower-cost sensors, for example, would be more prone to "false positive" or "false negative" errors.
- It is not exempt from attacks by cybercriminals on the authentication systems or breaches of the databases storing biometric data.
- Since known methods to protect sensitive data like the hashing process doesn't work with biometric data, organizations must use more complex methods to make sure such data is adequately encrypted.

IV. Comparison with object-based solutions and information-based solutions

Object-based authentication solutions require possession of a specific token like an ID card or key fob to be granted access to an asset.

Information-based authentication solutions require the user to know a specific code like a password or pin number to be granted access to an asset.

The following table provides a comparison of factors like reliability, convenience, and cost of each option against biometric access controls:

Access Control Alternatives Comparison			
Features	Biometric	Object-based	Information-based
Authentication data	Based on unique user characteristics.	Based on a token or object like an ID card or key fob.	Based on specific code like a password or pin number.
Market Acceptance	Low. Relatively new technology.	High. Favored by corporations for remote access.	High. Favored by financial services like banks.
Reliability	Robust. Some traits like fingerprints can be obtained by criminals in public places. Some systems still suffer from false detection errors.	Robust. User credentials are secured with only one key, which can be compromised.	Strong, but depends on security awareness by the user creating a strong password or safely storing the pin number. The traditional target of attacks like social engineering
Convenience	High It cannot be lost or forgotten. It cannot be changed.	Medium Easy to use, but the card or fob can be lost or stolen.	Medium Users must memorize a code and change it periodically. It can be changed in case of a security breach.
Cost	Reliable systems are still expensive. No need for security staff at the gates. Zero replacement costs.	Card or fob replacement cost (avg. $22 per card).	Storage servers and encryption software for passwords or pin numbers.

V. Types of biometrics for access control

There are four biometrics that are most used for access control: palm vein, fingerprint, iris scan, and facial recognition.

A. Palm vein.

Palm vein scanners use infrared light to map the unique vein structure of your palm. By doing so, it captures over 5 million data points that the palm vein scanner then converts to a unique encrypted code that becomes your biometric ID.

When the image is stored, the veins in the hand show a black-like pattern that maps out the unique vein pattern of the hand and encrypts the image to make storage easy and secure.

The best uses for palm vein scanners would be for identification purposes or to allow access to secure content such as banking information, or to identify a person before entering a secure facility.

The benefits of using a palm vein scanner include the security of the said product, making it harder for a person to forge the unique pattern hidden inside the body. They also provide privacy in the sense that, unlike your face, which is clearly visible to the public, your veins are hidden away and stored inside the body. The palm veins also provide greater accuracy than a fingerprint or iris scan by providing a larger surface area to scan and identify.

The reliability of palm vein scanners is much higher than other types of biometrics due to the unlikely change in a person's vein structure in the palms. Additionally, a palm reader does not require physical touch to complete the scan, so it provides a higher level of hygiene by removing human contact from the equation.

Advantages:

- The process is fast and easy
- Provides a high level of privacy and security
- The equipment itself is relatively small and easy to transport.
- The results are not affected by surface conditions such as grim or cuts on the hand.
- Data that is gathered from the palm is reliable and can be used throughout a person's lifetime.

Disadvantages:

- The price of the technology is currently higher than other types of biometrics.
- The database is relatively small since this is a newer technology.
- Health factors that include fever could affect the quality of the image-based distortion of the veins.

B. Fingerprint.

In the 1800s, the first use of fingerprint identification was used in criminal identification. Sir William Herschel was the first credited with this by taking finger and hand images for verification. He would record the prints on the workers' contracts so he could tell who was there on the workdays.

Sir Francis Galton was the first to suggest the records of all ten fingerprints be used to identify people, and this is still being used today for such purposes. In 1896, Sir Edward Henry paired up with Sir Francis Galton to devise a method of classifying and storing fingerprint information so it could be easily used.

Fingerprint scanners work by taking the pattern of the ridges and valleys on a finger and then processing the image on a device's pattern-matching software to compare it to the list of registered fingerprints on file. The Optical scanner shines a bright light over the fingerprint and takes digital images and, by using the ridges in it, converts the depth to 1s and 0s to create the user's own personal code. The problem with this is that a physical image could be used to fool the scanner into unlocking it. The Capacitive scanner uses human conductivity, creating an electrostatic field, to create a digital image based on the electrostatic field.

This type of fingerprint scanner is used on your everyday smartphone.

Advantages:

- Fingerprint recognition remains the most specific when it comes to verifying the user's identity by applying high accuracy.
- Compared to other biometric technologies, the fingerprint scanner is more affordable and easier to install.

- Fingerprint patterns are diverse, leaving the user with a secure way to access their personal information.

Disadvantages:

- Hygiene is an issue when it comes to scans due to the nature of having to physically touch the scanner.
- Hardware issues arise whenever the scanner is influenced by outside forces, like water and dirt, and will cause misreads to happen.
- Fingerprints can be affected by scaring and could cause previously stored data to not match the user's information in the database.

C. Iris scan.

Iris scanners are a type of biometric technology that uses images of the retina to verify the identity of a person based on a scan of the iris. The technology was first proposed by ophthalmologist Frank Burch in 1936. He said that each person's iris was unique enough with the probability of 1078, which in comparison to fingerprinting technologies was much higher.

It was John Duffman of Iridian Technologies that patented the algorithm that detects the iris of the eye.

There are two unique stages that are required during the scanning of the iris. The first is taking a snapshot of the eye. Infrared light is used to help enhance image clarity by recognizing the unique pattern of darker eyes more accurately. Regular lighting is also used in combination with infrared light to capture all aspects of the iris. Both pictures are then put through a computer analysis which removes unwanted details, such as eyelashes, and then highlights around 240 features in the iris pattern. They are then converted to a digital code consisting of 512 digits called the iris code.

The second stage is the confirmation of the authenticity of the eye. This does a quick rescan of the eye using the earlier technology to cross-reference the database and match the iris code signature.

The NIST (National Institute of Standards & Technology) has shown that iris scans are between 90 and 99% accurate.

Advantages:

- The unique iris pattern is formed when you reach the age of 10 months and remains unchanged throughout life, making the stability high.
- The uniqueness of the iris shows that the probability of two people having the same pattern is practically zero.
- The flexibility of technologies allows it to be used in conjunction with other technologies.
- The reliability of the scan is high due to the fact the iris cannot be lost, stolen, or counterfeited.
- The iris scan is non-contact and can measure from about 30cm away.

Disadvantages:

- The initial cost of the scanner is higher than other biometrics like fingerprint scanners.
- Government entities can use the technology to track the masses.
- The scanners themselves are susceptible to hacking by outside entities.

D. Facial recognition.

Facial recognition was first developed in 1964 by Woody Bledsoe, Charles Bisson, and Helen Chan and was funded by an anonymous intelligence agency. In the 1970s, this was further advanced by the software being able to differentiate lip thickness, hair color, and a magnitude of other facial features.

Through the 80s and 90s, recognition technology was able to apply linear algebra to the equation to help in the detection process. A decade later, a facial image database was created by the combined efforts of the National Institute of Standards and Technology and the Defense Research Projects Agency.

Facial recognition is the software used to identify facial features using the software's algorithm by processing a video or digital image to compare facile features. It takes video or a still image, and through the 2D image, the program distinguishes different physical points referenced as nodal points that can distinguish facial length and different aspect ratios.

From those nodal points, the image is converted into numerical data that is stored in the database. The code produced is referred to as a faceprint. The face then can be matched through various databases to see if the faceprint is identical to the numerical data. The FBI has access to 21 state databases with over 641 million photos to access from.

There are a few different algorithms that are used in the coding. One example is an application that takes a photo and emphasizes the details to better recognize the character. Another method is to take the 2D image and wrap it around a 3D cylinder to display features that would be hidden in a 2D image. Different forms of this are used for mundane tasks such as a lock screen for a cellular device or something more advanced like the identification through law enforcement during a routine stop.

Advantages:

- The security is high as only your face will be able to unlock the devices.
- It's simple to use and allows anyone to easily access their devices without having to go through a multitude of steps.
- The features are easily applied to other programs that take photographs and allow people to be tagged with ease for marketing research and sharing of photos.

Disadvantages:

- It allows access to sensitive data by having the scans be easily recognized from surveillance video, making it easier for government entities to track you.
- Privacy is lost when this is uploaded to the database, allowing others to get the likeness of your image.
- The technology can be affected based on lighting and makeup and can cause issues with the scan itself.

VI. Risks associated with the use of biometric technology

The use of this type of access control brings up two important risks: privacy and cyber security threats.

A. Privacy risks.

These types of systems are based on the ability to collect biometric data for future authentication purposes. Once the data is in the hands of a third party, there is a risk it could be used by unethical service providers or advertisers for other purposes than those agreed by the user (known as function creep).

It may sound like something out of a movie, but biometric information could be abused by repressive government regimes to influence public opinion in case of elections. Information is power, and biometric information can be a very powerful tool in the wrong hands. For example, if DNA scans become the preferred choice for biometric controls, they could lead to a widespread concern of privacy rights violations.

Any of these situations could lead to regulatory fines, lawsuits, or significant public embarrassment for the company that collected the data.

B. Cyber security threats.

Human characteristics are unique, but they are not immune to attacks by criminals. For example, a fingerprint can be obtained by a criminal from a glass in a restaurant.

As with other types of authentication solutions, user data is stored in databases for comparison. Such data can be captured during transmission to the central database and later used in a fraudulent transaction.

C. Measures to mitigate such threats.

There are a few recommendations to mitigate the risks and threats identified with the use of biometrics. These are some of them:

1. Multimodal biometrics

This method combines several biometric sources, such as face and fingerprints to increase security and accuracy. Such systems significantly reduce errors like "false negatives" of "false positives."

2. Use multi-factor authentication

To further improve accuracy and thwart hackers from circumventing access control systems, adding other inputs like geolocation, tokens, or pins can create a powerful combination to authenticate users securely.

3. Use local or device-based authentication.

Local or device-based authentication eliminates the possibility of hackers "eavesdropping" on the data transferred to a remote database for comparison. Today, smartphones use the most common example of a local authentication mechanism. User information, such as a fingerprint or facial scan image, is stored in a module inside the smartphone during the first setup of the security feature of the phone. When authentication is required, biometric information is collected by the camera or fingerprint reader in the smartphone, and the security module compares it with the original. Therefore, the raw biometric information never leaves the smartphone and is never available to any software or system outside the device. This is so effective that smartphone security modules are used to provide authentication for third-party applications.

Similar technology is used by other devices like tablets and laptops, where fingerprint scans of facial recognition are used to grant access to the device.

4. Tighten laws and regulations

Unfortunately, the level of the legal protection of biometric data differs from country to country and in the United States, depending on the legislation of each state. As of 2019, only three states (Illinois, Washington, and Texas) had some legislation protecting biometric data.

Outside the United States, we could only identify The General Data Protection Regulation, applicable in all 27 Member States of the European Union and the U.K., clearly identifying and protecting biometric data.

Current regulations loosely refer to personal data with no real binding to biometric data protection.

VII. Conclusions and recommendations.

Biometric access control is one of the most popular types of security systems on the market. They combine security and convenience like no other access control system can.

The possibility of using human characteristics that cannot be lost or need replacement makes biometrics the best choice for office building access control systems, law enforcement, and national security agencies.

Like any other technology solution, biometrics has its advantages and disadvantages. Accuracy and reliability can be an issue since lower-cost sensors, for example, would be more prone to "false positive" or "false negative" errors. Better precision implies more expensive systems.

It can also be subject to attacks by cybercriminals trying to breach the databases storing biometric data. Hashing doesn't work with biometric data, so organizations must use more complex methods to make sure such data is adequately encrypted.

The best option for biometric control is an iris scan. It provides the highest reliability due to the fact the iris cannot be lost, stolen, or counterfeited. It also is non-contact and can measure from about 30cm away. However, the initial investment required for reliable scanners makes it a bit difficult to choose.

Facial recognition, on the other hand, has already been adopted by many applications and systems, for example, our smartphones. It is simple to use and provides high enough reliability and accuracy. We believe facial recognition will continue to grow as the preferred option for access control systems based on biometrics.

There are many concerns about loss of privacy since all the biometric data collected by these systems for future authentication could be used by unauthorized entities like marketing firms, the government, or hackers.

Biometrics are here to stay, and we need to adapt to the changes it is already creating in our way of life. We must remain vigilant to protect our privacy rights but embrace technology as it develops.

VIII. References

Baker, H. (2021, August 7). *Do identical twins have identical fingerprints?* Livescience.com. https://www.livescience.com/do-identical-twins-have-identical-fingerprints.html

Biometrics | Homeland Security. (2021, December 14). Homeland Security. https://www.dhs.gov/biometrics#:%7E:text=Biometrics%20are%20unique%20physical%20characteristics,be%20used%20for%20automated%20recognition.&text=This%20system%2C%20called%20the%20Automated,operated%20and%20maintained%20by%20OBIM

Biometrics: definition, use cases, latest news. (2021, November 9). Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

Gudino, M. (2020, June 8). *How Do Fingerprint Scanners Work? Optical vs. Capacitive*. Arrow.com. https://www.arrow.com/en/research-and-events/articles/how-fingerprint-sensors-work

Karlskin, B. (2021, September 16). *Biometric Access Control Systems: Everything You Should Know*. Keyo. https://www.keyo.co/biometric-news/biometric-access-control-systems-101-everything-you-should-know

Kumar, M. (2019, July 20). *First Phone with fingerprint scanner*. Article | ATG. https://www.atg.world/view-article/6667/first-phone-with-fingerprint-scanner#:%7E:text=The%20world's%20first%20phone%20with,authentication%20and%20fingerprint%20speed%20dialing

La Estrella de Panamá, G.-L. E. (2022, February 2). *Autoridades detuvieron a 38 migrantes irregulares con nexos terroristas en 2021*. La Estrella de Panamá. https://www.laestrella.com.pa/nacional/220202/220201-autoridades-detuvieron-38-migrantes-irregulares?utm_medium=email&utm_campaign=Daily%20GESELa%20Estrella&utm_content=Daily%20GESELa%20Estrella+CID_08757ec94198bff56fd9a45c3d524d26&utm_source=Email%20newsletter&utm_term=Terroristas%20intentan%20llegar%20a%20Norteamrica%20a%20travs%20del%20Darin

Morais, L. (2020, May 6). *Biometric Data: Increased Security and Risks*. 2020–05-06 | Security Magazine. https://www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks

RecFaces. (2022, January 18). *Palm Vein Scanning & Recognition: What It Is & How It Works*. https://recfaces.com/articles/palm-vein-scan

RecFaces. (2022, January 18). *What Are Iris and Retina Scanners, and How Do They Work?* https://recfaces.com/articles/iris-scanner

RecFaces. (2022, January 18). *Is Facial Recognition Better and Safer Than Fingerprint Biometrics?* https://recfaces.com/articles/facial-vs-fingerprints-biometrics

RecFaces. (2022, January 18). *How Facial Recognition Works: Technology Explained in Detail.* https://recfaces.com/articles/how-facial-recognition-works

RecFaces. (2022d, January 18). *The History of Biometrics*. https://recfaces.com/articles/history-of-biometrics

What Are Biometrics? The Pros/Cons of Biometric Security. (2021, May 24). Auth0 - Blog. https://auth0.com/blog/what-are-biometrics-the-proscons-of-biometric-security/