

Sri Lanka Institute of Information Technology

**Biometric Security Systems**

**Individual Assignment**

IE2022 - Introduction to Cyber Security

Submitted by:

|  |  |
| --- | --- |
| Student Registration Number | Student Name |
| IT20200510 | V.Jathushan |

Date of submission

**Table of Contents**

[Abstract 4](#_Toc38443029)

[1. Introduction 5](#_Toc38443030)

[2. Evolution of the topic 6](#_Toc38443031)

[3. Future developments in the area 7](#_Toc38443032)

[4. Conclusion 8](#_Toc38443033)

[5. References 9](#_Toc38443034)

# Abstract

**Biometrics is the use of biological traits or behavioral traits to verify a person's identity. Biometric authentication is becoming increasingly popular as a reliable alternative to password-based security systems. It describes, how biometric technologies work and also discusses their benefits and risks when used in the biometric security system. This article discusses the biometric system and its functions. Various biometric technologies are also discussed and compared. This Assignment describes the history of the biometric security system, At what period did it start, What kind of evolution is there in each period. It also describes a detailed description of the new technology and its functions. This assignment discussed the benefits of the biometric invention during this period.**

# Introduction

**What is Biometric Security?**

* **Biometric security is used to verify and give access to a system based on the automatic and fast verification of an individual person’s physiological or behavioral characteristics.**
* **Biometric security is primarily used in environments with critical physical security requirements or that is a high chance of data theft. Biometric security-based systems store human body characteristics that do not change over a particular person's entire lifetime. These include fingerprints, eye texture, voice, hand patterns, and facial recognition.**
* **An individual's biometric characteristics are pre-stored in a biometric security system, which may be accessed by authorized personnel. When a person walks into a system or tries to gain access to a system, the biometric scanner checks his/her biometric characteristics, Which are matched with pre-stored records. If a match is correct, the person gets access.**

**What is Biometric Security?**

# 

“Automated measurement”

* No human involvement.
* Comparison takes place in Real-Time.
* Physiological and/or behavioral characteristics in biometric security

How Does Biometric Authentication Work?

**Biometric authentication is the extreme development of modern life. It also protects people from information theft.**

Fingerprint Scanners and How They’re Stored

**The most General form of biometric scanners is fingerprint scanners. These are commonly found on a smartphone or tablet that can take your fingerprint, read it, and test what is pre-stored in the database system. The data is stored in that separated section of hardware until it is called upon by the right verification program to get access. You can’t even root or use a bootloader to get access to that data!**

Eye Scanners

**Eye Scanners Another great form of technology in the biometric security world. Iris's scan fake is very tough. The iris has a very unique shape from person to person, so the chances of you meeting someone with the same iris shape are almost unimaginable. Eye scanners are a little bit advanced than this, and we can see running safely all over the world**

How Does Biometric Authentication Work?

• Facial recognition systems

**Facial recognition technology is the most common, Phones already use people's access to their accounts. According to the latest generation of phones that have been released, facial recognition systems are capable of saying a lot of similarities on the face but avoiding them. This is the most effective form of biometrics Because all it takes is a small scan and instant access to your phone, device, and more.**

**However, there is a disadvantage, which is that the lights in a dim situation will not give you access to your account. Anyway, it is only with the low level of technology and not at the high level.**

• Signature-Based Biometric Authentication

**Handwritten signature has a deep history as a means to authenticate the identity of document verifications, credit card transactions, cheque Authentication, attendance Registering, and forensics.**

**In the Present period, signature recognition is one of the most admitted biometrics, because the majority of the users having the act of signing as part of everyday life. A signature can be easily got using an ink pen or.**

**Although the signature is still used to verify the identity of a person by visual look-over, a constantly growing interest by industry has lead to the development of systems for automatic signature-based user confirmation**

How Does Biometric Authentication Work?

• voice recognition biometric system

**Voice recognition ( voice authentication or speaker recognition ) uses verify of a person’s voice to authenticate their identity. Speaker recognition is a sort of voice recognition technology. However, it is not the right as speech recognition, which is the technology used in speech-to-text apps and virtual assistants like Siri and Alexa.**

**Airways and tender-tissue cavities, as well as the structure and change of the mouth and jaw, influence voice patterns to develop an individual “voiceprint.” Speech recognition can make feel of verbal language, but it can’t verify the identity of the speaker based on their unique vocal attributes; voice biometrics can do it.**

• Hand Geometry Recognition

**Hand geometric biometric systems take attributes such as finger length, finger width, finger thickness, finger area, and palm width for individual recognition. These systems have gained great popularity and general acceptance from the greater deployment of applications in access control, time-visiting applications, and many authentication tasks.**

**What benefits do biometric security systems offer?**

**Quick and Accurate Identification and Authentication**

**Using passwords and codes for secure access is straightforward, but common. Anyone with a card or pass can access it. But biometric security technology refers to biological passwords that cannot be duplicated - that is, the exact identity and identification of a particular person. Because scanning is a quick and easy process, iris or facial recognition is often integrated as part of the protection process.**

**• biometric systems strengthen security**

**One of the main advantages of biometric security devices is that they can enhance your security. It is much harder to clone or steal a fingerprint than an access card. In situations where you need to increase security, biometrics can also be used for multiple factor verification. After someone presents their badge, for example, they have to provide a fingerprint to claim who they are. This is safer than using a PIN for verification because it can be easily passed on to others.**

**What benefits do biometric security systems offer?**

Biometric systems improve convenience

**Biometric security systems can also provide greater convenience to users. Forgetting a card or key is easy, but you always have your biometrics with you. Once the biometric test is implemented, all fingerprints, iris, and facial recognition are done - and the staff is good to go. It is also convenient to log in and audit the data accordingly**

* Easy to Operate and User Friendly

**Managing, fitting, and analyzing biometric verification is highly user-friendly - providing technical and accurate results with minimal need for intervention. New data can be entered quickly and records will be analyzed faster. Once the entry and exit table is created, it is easy to read and manage.**

• Additional Capacity to Accommodate Growth

**As companies grow, so does security. A key advantage of biometric verification is the ability to measure. These systems are very flexible and can easily accept additional staff data. This means that the company will grow into scales**

What are the risks of biometric security system?

Costs

**A lot of investment and costs need to develop a more advanced security system, Not surprisingly, Base on Spiceworks article, 67 percent of IT professionals said cost is the “biggest reason for not following biometric authentication”, and 47% of professionals support this system, but they are retreating, the reason the cost only**

Data breaches

**Governments and corporates companies that collect and store users' personal data continue to be vulnerable to hackers. Biometric data are unrepeatable, corporates need to manage important biometric data with high security and warning - something that is expensive and technically risks to stay ahead of fraudulent advances. If the password or pin number is negotiated, there is always a chance to change it. Biometrics of a person's physiology or behavior cannot tell this.**

What are the risks of biometric security system?

* racking and data

**As the world increases the use of biometric authentication systems such as facial recognition technology and other biometric security measures, the privacy of users should be taken into consideration. When biometrics are converted and stored as data, especially in places or countries with large surveillance activities, a user runs the risk of leaving a permanent digital record, which can be monitored by bad actors. In many cases, organizations and governments use facial recognition software to detect and identify people with intimidating accuracy that significantly compromises privacy. As surveillance increases, biometric data becomes a permanent digital tag that can be used to track someone with or without their knowledge.**

* False positives and inaccuracy

**Most general biometric verification methods rely on partial information to authenticate a user’s identity. For example, a mobile biometric device will scan an fully fingerprint when the enrollment phase, and convert it into information. Any ways, future biometric verification of the fingerprint will only use parts of the prints to verify identity so it’s faster and quicker. In 2018, a research team from New York University created an Artificial Intelligence platform that was able to fraudulently crack fingerprint authentication at a success rate of 20% by matching similarities of partial prints to the full biometric data**

# Evolution of the biometric security systems

* **When we hear the word biometric, we have an image of a fingerprint on our Thoughts, but first, biometrics is a word connect to our anatomy characteristics. The native term "biometrics" literally mentions appraisal and various types of calculations related to body characteristics. It is the appraisal of body characteristics in the structure of a matrix. Biometric measurements are individual depending on their sort. This is why modern-day verifications biometrics measurements make sure high ability.**
* **Bio The term "biometrics" is received from the Greek terms "bio" it called life another one "measurements" it called a measure. Biometric automation systems have only been obtainable for the past few decades due to notable advances in technology. Anyways, these recent automation manners are based on concepts that came up with the idea hundreds, thousands of years ago.**
* **Throughout the history of civilization, many pieces of biometrics evidence have been used as a formal authentication system**
* **Many paintings have been created by primal people who lived there in a cave 300000000 years old. There are lots of fingerprints around these paintings that make it feel like an unforgettable signature of the owner of painting.**
* **If we want to identify a person about 500 years ago there is evidence that fingerprint was used for that, Also Babylonian merchants recorded clay plates fingerprints**
* **"Jamehole-Tawarik" The 14th-century Persian book said we can identifying an individuals based on fingerprints**
* **In the early history of Egypt, stockbroker were found by their bodily characteristics in order to understand themselves**

**Evolution of the biometric security systems**

**Time period of Biometrics security History**

# • 1858 – The first analytical take of hand images for verification goal is documented

# Sir William Herschel, who works in the Indian civil service, signed the back of the contract to identify each employee on payday. That was the earliest recorded system take of hand and finger

# • 1883 – Twain writes about fingerprints in the book “Life on the Mississippi”

# In one of the sequence stories in Mark Twain's "Life on the Mississippi", the writer wrote about fingerprints and explained the procedure of extracting those. 1894's "Foot Head Wilson's Tragedy", the writer pointed the use of fingerprints to authandicate again. In the story, a person on inquiry proves his innocence by comparing his fingerprints with that left at the crime place.

Evolution of the biometric security systems

**Time period of Biometrics security History**

**• 1903 – Bertillon System crashes**

**The two-person, who were decided to be identical clones, was blamed on a U.S. prison in Leavenworth and were initiate to have almost the same appraisal using the Bertilon method. Anyways the basis of this story was later difficult, this story was used to declare that Bertilon's appraisal were not enough to differentiate between these two clones.**

**• the 1960s – Face recognition becomes semi-automated**

**The first semi-automated face recognition system was made by Woodrow W. Bellow in a contract with the U.S. government. Developed by Pletso. This system needed the director to discover features such as eyes, ears, nose, and mouth in photos.**

**• 1960 – First Structure of acoustic speech production is developed**

**.A professor, Gunnar Fond, announced a structure explaining the human's body characteries parts of sound speech creation. His decisions were based on the investigation of x rays of individuals making particular phonic sounds. This kind of things we're used to good understanding the biological parts of speech**

Evolution of the biometric security systems

**Time period of Biometrics security History**

* **1965 -Automated signature recognition analysis starts**

**In 1965, North American aviation developed the first signature system**

**• the 1970s – Face Recognition takes one more footfall close to automation**

**Goldstein, Harmon, and Lesk used 21 specific internal stage pointers examples for hair color and lip thickness to automate facial authentication. The issue with those both initial results is that the appraisals and areas were calculated manually.**

**• 1970 – A behavioral segment of speech is the first developed**

**The primordial prototype of audio talk production, made in 1960, was accrescent by Dr. Joseh Barkel, who used X-rays for movement and attached the tongue and jaw. This structure gave a comprehensive understanding of the multiplex behavior and biological parts of speech.**

**• 1985 – The idea that no two irides are alike is suggested**

**Dr. Ophthalmologists Leonard Flum and Aran Sapphire suggested that the both irons were not identical.**

# Evolution of the biometric security systems

**Time period of Biometrics security History**

**1988 – Developed Eigenface technique**

**Kirbie and Serovich used a standard linear algebra principal component analysis for the face authentication problem. This was a Landmark because it displayed that lower than a hundred values are needed to close to a properly aligned and normalized facial image.**

**• 1993 – Face Recognition Technology program is started**

**In an attempt to encourage the development of face verification algorithms, The Face Recognition Technology rating has been awarded by the protection-led investigation Products Institute (DARPA) since 1993-1997 and the DoD Counterdrug Technology Development Project Office.**

**• 1994 – Palm System is standard**

**The first known automated fingerprint verification process develop-in help of palm printing is trusted to have been developed by a Hungarian company called Recowaer Ltd. In late 1994, inactive professionals in the US assessed thee**

# Evolution of the biometric security systems

**Time period of Biometrics security History**

* **2001 – Face recognition is used at the Super Bowl in Tampa, Florida**

**In an effort to identify the "desired" people entering the stadium, Face recognition was established in January 2001 at the Super Bowl in Tampa, Florida. There are no "desired" people in this demonstration, But was able to misidentify a dozen innocent sports fans**

**• 2011 – Biometric verification used to identify Osama bin Laden dead body**

**The CIA of US used facial authentication technology to spot the remains of Osama bin Laden with 95 % surety. CIA used DNA to ensure.**

**• 2013 – Fingerprint scanners introduce by Apple into smartphones**

**Touch is a fingerprint authentication feature, created and published by Apple corporation., that was developed possible on the iPhone 5S,6, 6 Plus, and the iPad. Touch is heavily complained into iOS devices, allowing users to unlock their device**

**The Evaluation of biometric security in present time period**

**1. Airport Security**

**Biometric technology has been in airports for some time. The goal is to make travel through airports as unobtrusive as possible shared by airports around the world. The use of biometric technology to verify the identity of passengers has been used at some major airports around the world for many years, and the use of the technology is now becoming more widespread.**

**2.Bank**

**Bank customers are tired of the need to prove their identity - however, without it, the threat of identity theft will continue to rise. Therefore, there is a need for biometric security systems for banks. Many banks with mobile applications allow user authentication via biometrics such as facial recognition, fingerprint scanning and voice verification. Other banks use a combination of these biometrics; Multi-factor recognition, when combined with biometrics, can create almost impossible security.**

**The Evaluation of biometric security in present time period**

**3. Mobile access and authentication**

**One of the most common applications of biometric technology is smartphone security. Apple, which first introduced the Touch ID using fingerprint recognition technology - has since developed mobile phone security to use a number of biometric technologies, including face recognition, iris recognition and voice recognition.**

**4. Home Assistants**

**Every one familiar with Google Home, Alexa and Siri is already accustomed to using voice recognition as a biometric identifier. Google Assistant is compatible with a wide range of IoT (Internet of Things) devices, including lights, door locks, security cameras, security lights, and more that empower the assistant on Google Home and Android devices.**

**The Evaluation of biometric security in present time period**

**5.Cash protection**

**We mentioned how biometrics is used by banks; However, there is another financial application: biometric tariff protection. This technology has been integrated during transaction authentication processes and, now, mostly involves fingerprint scans.**

**6.Home security**

**Biometric technology allows a person to enter a home once its scanning unit has verified their identity. Access to office buildings, entire homes or specific rooms can be controlled by biometrics. Biometric locks deny the need for a key, which is instead activated by a fingerprint swipe.**

# THE FUTURE OF BIOMETRIC SECURITY

**I firmly believe that Biometrics is the future of e-security systems and a lot of companies are joining in Biometrics day by day. Windows 10 OS also incorporates a biometric security platform. Biometrics is used in stadiums, airports, and banks around the world.**

**Government agencies and law enforcement have shifted to biometric systems - therefore, more and more companies are likely to follow suit in the future.**

**While bio-biometric security systems are not stupid, they are still faster, less expensive (longer lasting), and more accurate than traditional security methods.**

**Many biometric services are currently under development and testing. However, in a few years, these biometric technologies will be introduced everywhere. Plastic cards will soon fade into the background and fingerprint scanning will become a standard daily activity.**

**From monitoring your heartbeat to chips fitted under your skin, as well as scanning your intraocular vessels, tests are underway on the shape of your ear canals and more.**

**Banking's biometric future**

**Biometric technology will soon be the norm in the banking industry. According to Acute Market Intelligence 1, physical credentials such as money and bank cards will disappear in the next decade or 'virtual credentials' - iris, voice, finger nerve - will last until 2030. By 2025, Equity predicts trillions of quality authentication transactions are biometric.**

**Overall, while the public recognizes that data security is increasingly important, they are concerned that passwords and PINs are not evidence of fraud - and that biometrics responds by providing a quick, easy, and secure authentication process.**

**More specifically, the adoption of biometric technology is accelerated by the transition from external aspect recognition to internal (e.g., voice neurological recognition), which provides a highly streamlined and interesting customer experience..**

# The role of biometrics in cloud computing in the future

# Cloud computing has become a new nature for most businesses. Nowadays, businesses of every size and industry use different cloud computing applications.

# Cloud computing solutions have many advantages such as more time, mobility and reduced cost, but one of the biggest challenges for this technology is security. Has the ability to take cloud computing to the next level, improving the overall security of the cloud operating system.

# One of the main reasons why bio biometric recognition is so successful is that it uses unique human characteristics for each person. Properties such as fingerprints and facial recognition are used in biometric authentication

# You should know that biometric concept started with fingerprints and then with the advancement of technology facial recognition will also become a part of biometric authentication

# The role of biometrics in cloud computing in the future

**There is no denying that the M biometric solution is one of the most secure authentication methods, but it can become a very serious issue if anyone accesses the templates stored by the cloud provider.**

**This is why encryption is used to ensure that even if an unauthorized person accesses fingerprint templates, it is of no use to them. In encryption mode, the fingerprint templates and cloud provider stored at the end of the cloud user are encrypted.**

**In order to enhance security in biometric authentication, a multi-finger protection model system is used. In this unique model, the cloud user has to register three fingerprint templates and then the user chooses a number for each fingerprint template.**

**Type This type of biometric authentication makes the cloud operating system more secure and terms such as unauthorized access are meaningless.**

**Biometric e-Passports**

• **Also known as an e-passport or digital passport, a biometric passport contains an embedded microchip that keeps our personal information. It looks like a traditional old passport, but it has an international biometric logo on the bottom of the front cover. E-Passports launched to combat identity theft and terrorist threat**

How do biometrics work?

• **Biometrics investigate the unique physical characteristics of every human and contain retinal scans and fingerprints. The embedded chip in our e-passport holds information about your faces, such as the distance between your eyes, nose, mouth, and ears, got from the digital photo you give when you apply for your passport.**

What’s the use of a biometric passport?

**Adopting to ePassports was primarily to improve safety and security. The embedded chip can keep a large amount of special data in it, making the passport too harder to remodel or forge. It’s also much easy to find people using the detailed set of information stored through biometrics.**

**• You'll sence the advantage of taking with a digital passport when you can to use the ePassport gate in border control which makes getting airport security too much convenient. Artificial intelligence (AI) will transform security, authentication**

**fraud is not an insurmountable problem, AI will help. Companies can stack AI in ways that help them change their customer experience and services and protect data. Biometrics is one such example, which involves various methods such as voice, behavior and facial recognition for customer recognition. Help identify and promote best practices and mitigate safety risks. AI and biometrics together prevent billions of dollars from fraud. With the help of AI and biometrics, we will build a more secure, more digital, foundation for the future.**

**Biometric Car Technologies**

**Many automakers are now introducing this technology to vehicles to avoid many problems such as vehicle theft. You can open your vehicle very easily by using your smartphone or Bluetooth device. After that, when you get in the car, it checks that you are the right person and will alert you in case of emergency.**

**Car owners can set up biometric settings such as fingerprints or retina scans. After that, no unauthorized person can open the car. Similarly biometric technology will be embedded in the seats, which will be very helpful in monitoring driving stress and tension. With that, there will always be physical changes in the automobile.**

**Biometric technology can collect data on everything, including the steering, accelerator and many other components to determine. Also, if there are signs of anxiety, the car will suggest that the driver take a few minutes to rest.**

**New Technologies in Biometrics**

**Palm Vein Scan**

**A palm nerve scan is a forceful new biometric it uses the nerve structure of our palms to verify us. For example for a fingerprint, a person's palm nerve structure is individual and will not change in a lifetime period in that human. Anyway, this unique authentication system has some key security and privacy benefits that classic biometrics ( fingerprint and face base authentication) can't provide.**

**How palm vein scanner work?**

**A palm nerve scan is a biometric that takes more than five million data points using “infra light” to point the uncommon nerve shape of our palm nerve. The palm nerve scanner then remodel these data points into a unique encryption codes, That becomes our biometric unique ID.**

**Palm nerve authentication is an important factors that sets it different from other security technologies. Unlike our fingerprint, iris, or face, The palm nerve system is an internal part of the human’s body.**

**Because your palm nerve system is cover in our hand, it doesn't reveal like other biometrics technologies. It gives so many unique advantages, making it one of the most advanced biometric technology in the biometric world**

**Which points are determined Palm Vein is the powerful Biometric?**

1. High Security to data

**palm nerve scan is highly secure other biometric technologies because it is doesn’t exposed to out of the world. for example for password-like biometrics. But instead of using login codes, you are using our own anatomy. But some biometrics, such as facial authentication, have one major disadvantage: they are exposed. Palm nerve, because your biometric code is hide in our hand, it is very tough for a looter to take this kind of model and make a copy with it.**

2. Accuracy

**The palm nerve scanner, for example, can take a vast number of data points because the palm has a large range than the fingers or iris. This provides accurate benefits compared to other biometric technologies. Kyo's palm nerve scanner captures more than 6 million data marks in the palm of the hand, giving unmatched accuracy.**

**Which points are determined Palm Vein is the powerful Biometric?**

3. Privacy

**Since the palm nerve is inner to the body, that can only be taked via a close-up, camera in conjunction with “ultraviolet light”. So if we do not intentionally scan our hand on the palm nerve scanners, it will be very problematic to take it.**

**This has lots of advantages for companies that want to appliance palm nerve in their organization:**

**Because it is a privacy center, the palm nerve can be considered very trustworthy by clients and/or employees, thus making it easy for them to connect it.**

**Since consensus is at the forefront of privacy rules in the world level, palm-nerve acceptance based on design makes it easy to comply with these rules and avoid legal problems.**

4. Reliability

**Person Each person's palm nerve shape doesn't change throughout his lifetimeperiod, so the user is less likely to rejoin in the future. Some other biometric technologies are more likely to shift all time.**

**Fingerprints, for example, cuts and erosion on the finger make it a chance for a verified user to identified by fingerprint scanner devise and miscalculation ban access. Palm Ween has been very consistent over time.**

**3D Face Recognition**

**Face recognition has become a popular research direction in both industry and education. It benefits from traditional 2D face recognition such as the natural authentication process and a wide range of applications. Furthermore, 3D facial recognition systems can accurately identify human faces even under dim lighting and with different facial expressions and expressions, which makes it difficult for 2D face recognition systems to operate in such conditions.**

**A growing trend in facial recognition software is to use a 3D model, which claims to offer greater accuracy. Real-time 3D imaging of a person's facial surface uses 3D facial recognition to distinguish facial features - where hard tissue and bone are most clearly visible, such as the curves of the eye socket, nose and chin. All of these areas are unique and will not change over time.**

**Before to this, investigating officers had to manually spot a person that took too long and did not of high accuracy. But today, the facial verification method takes a short time period to find thief but is incredibly accurate**

**DNA biometrics**

**Considering that 0.10 percent of a person's entire gene is unique to them, DNA testing can be very difficult and accurate. Two people sharing the identical DNA structure is less than one in a hundred billion if we match 26 different groups.**

**However, even the most basic DNA testing requires sophisticated and expensive technology. Obviously, this requires a physical model, so the person must be physically fit with the test equipment and can be the most aggressive way to test.**

**Although this process is very precise, it is not as accurate as DNA fingerprinting. According to national standards and technology institutes, fingerprint comparisons are 98.6% accurate on one finger. DNA fingerprinting time is 99.9% accurate.**

Keystroke biometrics

**Keystroke authentication is defined as the procedure of measuring and evaluating typing rhythms on digital devices, including keyboards, phones, and touchscreen stage. Keystroke dynamics uses an individual biometric template to find based on typing, rhythm and speed.**

**Typing patterns can be incompatible because the contractile muscles and sweaty hands can seriously change a person’s typing patterns. However, MIT showed that typing methods vary depending on the type of keyboard, which can complex authentication.**

**The software can accurately measure the occurrence of key pressures in milliseconds. Therefore, one's keystroke pattern cannot be copied at such a high resolution.**

# Conclusion

**Despite many doubts about the biometric security system, biometric security systems identify individuals with the highest level of certainty.**

**Mainly fingerprint biometric provides a very robust mature solution to biometric technology.**

**All though many new biometric technologies will be used in the future, fingerprint systems will mainly use in day-to-day life.**

**Many companies still don’t have access to biometric technology due to the fact the employers have many security concerns about biometric technologies, but in the future, many companies will use biometric technology as a shield to allay their fears. biometrics remains a growing way to verify identity for cybersecurity systems.**

**Biometric technologies provide highly demonstrative solutions to security despite the risks the system is flexible and difficult to duplicate in addition this system will achieve very long-term growth in the future.**

**For my thoughts, in the future, there will be a situation where we have to live with biometric technology facilities day to day, Because biometric technology is becoming an integral part of most basic needs, from medical banking vehicle, travel, and money, etc.**

# References

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

<https://recfaces.com/articles/biometric-trends#:~:text=in%20payment%20systems%3F-,The%20Future%20of%20Biometric%20Security,become%20a%20standard%20daily%20operation>.

<https://www.globalsign.com/en/blog/7-benefits-security-with-biometrics>

<https://link.springer.com/article/10.1007/s11831-019-09376-2>

<https://www.nec.co.nz/market-leadership/publications-media/the-top-9-common-uses-of-biometrics-in-everyday-life/#:~:text=Biometrics%20is%20widely%20used%20across,utilising%20biometrics%20in%20criminal%20investigations.&text=The%20most%20common%20biometric%20technologies,%2C%20gait%2C%20and%20voice%20recognition>.

<https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics>

<https://www.biometricupdate.com/201802/history-of-biometrics-2>

<https://readwrite.com/2020/05/13/biometrics-what-the-future-holds-for-identity-verification/#:~:text=The%20Future%20of%20Biometrics&text=Users%20can%20now%20utilize%20several,going%20anywhere%2C%20any%20time%20soon>.

<https://techmonitor.ai/techonology/cybersecurity/voice-dna-fingerprint-and-others-how-5-biometric-security-solutions-compare-4842316>

<https://keyo.co/biometric-news/5-reasons-why-palm-vein-scan-is-the-best-biometric>

<https://www.securitymagazine.com/articles/94548-ai-and-biometrics-in-2021-predictions-trends-and-insights-for-what-might-lie-ahead>

<https://www.nedapsecurity.com/insight/biometric-security/>

<https://www.m2sys.com/blog/important-biometric-terms-to-know/the-history-of-biometrics-technology/>

<https://recfaces.com/articles/biometric-trends#:~:text=in%20payment%20systems%3F-,The%20Future%20of%20Biometric%20Security,become%20a%20standard%20daily%20operation>.