EUROPEAN JOURNAL OF BIOMEDICAL AND PHARMACEUTICAL SCIENCES
http://www.ejbps.com

ISSN 2349-8870
Volume: 10
Issue: 11
324-336
Year: 2023

BIOMETRICS IS THE MEASUREMENT AND ANALYSIS OF UNIQUE PHYSICAL OR BEHAVIORAL CHARACTERISTICS BY VERIFYING PERSONAL IDENTITY

Dr. Dhrubo Jyoti Sen*

D. Pharm., B.Sc. (Hons), B.Pharm. (Hons), M.Pharm., Ph.D., FICS,
CChem FIC (India), CChem FRSC (UK), CSci (UK), AOM (USA)
School of Pharmacy, Techno India University, Sector-V, Salt Lake City, EM: 4/1, Kolkata-700091, West Bengal, India.

***Corresponding Author: Dr. Dhrubo Jyoti Sen**
D. Pharm., B.Sc. (Hons), B.Pharm. (Hons), M.Pharm., Ph.D., FICS, CChem FIC (India), CChem FRSC (UK), CSci (UK), AOM (USA) School of Pharmacy, Techno India University, Sector-V, Salt Lake City, EM: 4/1, Kolkata-700091, West Bengal, India.

Article Received on 21/09/2023 **Article Revised on 11/10/2023** **Article Accepted on 01/11/2023**

ABSTRACT
Biometrics are physical or behavioural human characteristics to that can be used to digitally identify a person to grant access to systems, devices or data. Examples of these biometric identifiers are fingerprints, facial patterns, voice or typing cadence. Each of these identifiers is considered unique to the individual, and they may be used in combination to ensure greater accuracy of identification. Because biometrics can provide a reasonable level of confidence in authenticating a person with less friction for the user, it has the potential to dramatically improve enterprise security. Computers and devices can unlock automatically when they detect the fingerprints of an approved user. Server room doors can swing open when they recognize the faces of trusted system administrators. Help desk systems might automatically pull up all relevant information when they recognize an employee's voice on the support line.

KEYWORDS: Biometrics, Finger Biometrics, Iris Biometrics, DNA Biometrics, Voice Biometrics, Vein Biometrics, Fingerprint Biometrics, Signature Biometrics, Behavioural Biometrics, Touch screen Biometrics.

INTRODUCTION
Biometrics are body measurements and calculations related to human characteristics. Biometric 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. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological characteristics which are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor/scent, voice, shape of ears and gait.

Figure 1: Biometrics.

Behavioural characteristics are related to the pattern of behaviour of a person, including but not limited to mouse movement, typing rhythm, gait, signature, behavioural profiling, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics. More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information. Biometrics are biological measurements — or physical characteristics — that can be used to identify individuals. For example, fingerprint mapping, facial recognition, and retina scans are all forms of biometric technology, but these are just the most recognized options.[1]

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control or for identifying individuals who are under surveillance. While there are many types of biometrics for authentication, the five most common types of biometric identifiers are: fingerprints, facial, voice, iris, and palm or finger vein patterns. Biometrics refers to digitally encoding physical attributes of a user to gain access to data or computer systems. Fingerprints, facial recognition, and voice patterns are among some of the most widespread uses of biometrics today in both consumer and commercial use. Aadhaar avoids errors and duplications which was the bane of earlier systems, by linking an individual's identity to biometric information which is unique to the individual. Fingerprints are a unique feature that every person has, and no two people have the same ones. Fingerprint biometrics is used to both authenticate (match a person’s biometric template) and identify (determine the identification of a person).

Figure 2: Finger Biometrics.

A person’s unique physical characteristics are called biometrics, which can be used to validate and verify identity. Fingerprint biometrics is some of the most commonly used types of biometrics for authentication and identification purposes, but facial recognition, iris scanning, and DNA are all forms of biometric identifiers as well. Fingerprint biometrics is widely distributed, cost-effective, easy to use, effective, hard to fake, and convenient, making them a secure and useful tool for authentication and identity verification.

Understanding fingerprint biometrics: Biometric technology uses unique physical or behavioral attributes that are individual and not replicable. Fingerprints are a method of identifying a person, and they are specific to each individual. No one else will have the same fingerprints that you do. Fingerprints are made up of specific patterns, including ridges, valleys, arches, loops, and whorls. For the purposes of proving identity, there are three main methods used:
Something you know, like a password
Something you possess, such as a token or keycard
Something you are, including fingerprints, face, or hand
Fingerprint biometrics involves something you are. You always have your fingerprints on you, and they belong to you alone. Fingerprint biometrics has been used for decades with recent technology becoming more and more advanced, allowing for a more technical and widespread use of this important tool.

Biometric authentication & security: Biometrics uses a statistical analysis and measurement of physical or behavioral characteristics as a security feature to authenticate and identify an individual. Fingerprint biometrics can be a frictionless form of security that is easy and seamless to use. Fingerprint scanners can be used to secure physical access to locations as well as to devices. Fingerprint biometrics is a security feature that cannot be forgotten or misplaced like a password or hardware token. Biometric security can be more secure than other forms of authentication, as biometric information is linked to a specific individual and

therefore more difficult to steal, lose, or compromise. This can improve reliability and simplify security processes. There are some flaws to fingerprint biometrics, however, and cybercriminals can find ways around this form of security. If the wrong person enters their fingerprints matched to your data, for example, it is harder to invalidate these biometric authentication details. Also, if someone does gain access to your fingerprint data, which is left anywhere you touch and can be fairly easily obtained, this data is not changeable. You cannot change your fingerprints, so replicas will be able to access anything that is fingerprint-protected. Master fingerprints have been able to "fool" smart devices, and software flaws can present issues for fingerprint biometric security.

How fingerprint biometrics work: Fingerprint biometrics uses some form of a scanner to obtain an image of your fingerprint. Methods include the following:

Optical scanner: This takes a digital image of your fingerprint by lighting up the finger through a prism and reading the way the ridges and valleys reflect the light. This information is then converted into an image.

Capacitive scanner: This generates a small electric charge through miniature built-in capacitors that store electricity. The capacitors are discharged when the finger touches the scanner.

A higher level of discharge is created by fingerprint ridges, which have a greater contact surface, and less by the valleys, which create gaps in the skin. The difference between these is measured to determine a pattern.

Ultrasound scanner: An ultrasound signal is used to record the echo the fingerprint creates, as ridges and valleys create different echoes. This scanner does not need to be in direct contact with the finger to get a reading and also has the benefit of reading in a more three-dimensional manner.

Thermal scanner: This uses heat to measure the temperature difference between the ridges and valleys of the fingerprint. It creates the image of the fingerprint based on the contrast between the two.

After fingerprints are scanned, they can then be matched based by pattern matching, which compares two images looking for similarities. More commonly, minutiae-based matching is used, which looks more closely at the direction and location of the points. The unique data and specific characteristics of the fingerprint are filtered and then saved as a mathematical representation (algorithm) or as an encrypted biometric key. The fingerprint image itself is not saved, only the binary code (or series of numbers) is retained and used for verification purposes. This algorithm cannot be reverse engineered to recapture the image of the fingerprint and thus cannot be duplicated. Fingerprint data is generally stored on the device itself and not in the cloud.

Benefits of fingerprint biometrics: Overall, fingerprint biometrics is considered to be highly secure and a common method of protection. For the highest level of security, they can be used as part of a dual or multi-factor authentication (MFA) model that includes the use of at least one other method as well, such as a password or token.

Benefits of fingerprint biometrics include the following

Fingerprints cannot be lost or misplaced, and they are always with the person.
Fingerprints are hard to fake and more secure than a password or token.
Fingerprint patterns cannot be guessed and are non-transferable.
Fingerprint biometrics offers a high level of security for identity verification.
Fingerprint biometrics is user-friendly and convenient.
Fingerprint biometrics is easily deployable and cost-effective.
Use of fingerprint biometrics can provide accountability.
Fingerprints take work to steal or spoof.
Fingerprint biometric techniques are fast, simple, and easy to use.

Fingerprint biometrics usage: Biometric technologies, and fingerprint biometrics specifically, are used across a wide variety of fields and industries for the purpose of authentication and identity verification. These are examples:

1. Law enforcement and public security: Fingerprints are a common method of identifying suspects and criminals. The IAFIS (Integrated Automated Fingerprint Identification System) is the national computerized system that stores, compares, and exchanges digital fingerprints for the purpose of matching them to a known party in the database.
2. Military: Fingerprint identification can be used to identify non-U.S. citizens on the battlefield, to help determine military allies and enemies. The Defence Forensics and Biometric Agency (DFBA) stores biometric information, including fingerprints as a matter of national security.
3. Border control and travel: The Department of Homeland Security (DHS) runs the Automated Biometric Identification System (IDENT) to store and process biometric information, such as fingerprints for immigration and border control, intelligence, background information for national security clearances, law enforcement, and for the purposes of national security. DHS also issues e-Passports in the United States to be used for international travel, which contain an electronic chip that holds biometric information of the holder, like fingerprint data. Airport security can also use fingerprints and other biometrics to authenticate travellers.

Health care: Biometric ID cards containing fingerprints can be used to access health care services and resources to ensure the right person is receiving treatment. Hospitals, pharmacies, and clinics also often have fingerprint scanners to match a patient to their patient records.

Facilities: Fingerprint biometrics can be a form of physical access control used by companies and organizations to grant and deny access to actual locations based on who a person is and not what they have or know.

Computer systems and networks: Smartphones, laptops, and computers all often use a form of biometrics, such as a fingerprint, to unlock them, granting access to only that specific user. This is called logical access control. Fingerprint data is stored directly in the device itself, making it more secure and less prone to potential privacy issues or data breaches.

Commercial applications: Many different commercial and retail industries use fingerprint biometrics to verify a customer's identity and authenticate a user. Banks and financial institutions can require fingerprint access for transactions, for example, as can credit card readers or retail establishments. Fingerprint biometrics can be used to authenticate a person based on matching the data within a system, or it can be used as a method of identity verification to ensure that a person is who they say they are. Fingerprint biometrics can add an extra layer of security over password and token security measures. Fingerprint scanners are dropping in price, making them more widely available and accessible for a wide range of businesses, organizations, and industries.

Fingerprint biometrics is a commonly used form of biometric security that is easy to use, hard to fool, and often a cost-effective strategy, relying on something a person has. Fingerprints cannot be forgotten or lost like a password or ID card, and no two people share fingerprints, guaranteeing that they are unique to each individual. Fingerprint biometrics use a scanner that can be small and freestanding or contained within a device directly, such as a smartphone, security system, or computer. Fingerprint scanners take a digital rendering of the fingerprint and convert it to a digital algorithm for storage.

In this way, fingerprint data is safe from reverse engineering. Even if a bad actor obtains the fingerprint data through a breach or theft, it cannot be turned back into the fingerprint image and used. A security feature that is convenient, easy to use, and user-friendly, fingerprint biometrics is used across a wide range of applications to both verify and authenticate identities. Biometrics is a growing field as well, and the use of biometric identifiers, such as facial recognition, iris scans, and behavioural biometrics including typing patterns, online interactions, and device handling, are all being explored for even more uses than they are used for today. Biometrics can offer a high level of security that is unique to the individual user and harder to compromise. Fingerprint biometrics continue to advance with evolving technology. More companies and industries are adopting this form of biometric authentication. When coupled with other security protocols, such as strong passwords or tokens, fingerprint biometrics are even more secure.

Figure 3: Iris Biometrics.

The use of biometrics as a tool for identification and security purposes began in the late 19th century with the work of Alphonse Bertillon. **Alphonse Bertillon** (22 April 1853 – 13 February 1914) was a French police officer and biometrics researcher who applied the anthropological technique of anthropometry to law enforcement creating an identification system based on physical measurements. Anthropometry was the first scientific system used by police to identify criminals. Before that time, criminals could only be identified by name or photograph. The method was eventually supplanted by fingerprinting. He is also the inventor of the mug shot. Photographing of criminals began in the 1840s only a few years after the invention of photography, but it was not until 1888 that Bertillon standardized the process.

Figure 4: Voice Biometrics.

The person submitting biometrics should bring the appointment notice and valid, unexpired photo identification (for example, Permanent Resident Card (Form I-551), passport, or driver's license), or other identity documentation as authorized by USCIS to the appointment. Biometric technology uses unique physical or behavioural attributes that are individual and not replicable. Fingerprints are a method of identifying a person, and they are specific to each individual. No one else will have the same fingerprints that you do. Biometrics are biological characteristics of an individual, such as face or fingerprint, which can be used to verify their identity. Use of fingerprint or face recognition for device authentication is now commonplace on smartphones and tablets. It is also increasingly becoming available on laptops.[2]

Figure 5: Alphonse Bertillon: Biometrics Scientist.

Iris recognition is widely considered to be the most accurate modality of biometric identification. Yes, biometrics are generally more secure, but they aren't fool proof. Hackers can spoof biometric data by using various techniques like downloading or printing a person's photo, using a fake silicone fingerprint, or a 3D mask. Such attacks are known as presentation attacks. In biometrics industry, researchers are using AI to improve the accuracy and performance; at the same time developing different biometric methods such as behaviour recognition. H. M. Smith, of the Bureau of Identification, Tacoma, Washington, then offered an amendment that the fingerprint be one of Sir Francis Galton's (often referred to as the "Father of Fingerprints"). Vein recognition, otherwise known as vascular biometrics, refers to technology that measures parts of a subject's circulatory system which is a s unique to her as a fingerprint. The iris is the colored, donut-shaped portion of the eye behind the cornea and surrounds the pupil. A person’s iris pattern is unique and remains unchanged throughout life. Also, covered by the cornea, the iris is well protected from damage, making it a suitable body part for biometric authentication.

Features of iris recognition

1. Highly accurate and fast, iris recognition boasts of having top-class precision among different types of biometric authentication technologies.
2. Remains unchanged throughout life. (This does not constitute a guarantee.)
3. Since the iris is different between the left and right eye, recognition can be performed separately by each eye.
4. Possible to distinguish twins.

As long as the eyes are exposed, iris recognition can be used even when the subject is wearing a hat, mask, eyeglasses or gloves. Because of using an infrared camera, recognition is available even at night or in the dark. Without the need to touch the device, contactless authentication is possible, making it hygienic to use.

Figure 6: Vein Biometrics.

Hugh McCormick Smith, also H. M. Smith (November 21, 1865 – September 28, 1941) was an American ichthyologist and administrator in the United States Bureau of Fisheries. Ichthyologists study all aspects of fish biology including anatomy, behaviour and environment of fishes, how fishes interact with other organisms. The advantages that biometrics provides are that the information is distinctive for every person and it can utilized as a technique for individual identification. The top benefits of Biometric technology are authentication, privacy or data discretion, authorization or access control, data veracity, and non-repudiation. The ready availability of the technology, its increasing adoption, and enhanced security have made biometrics an integral part of current cyber security frameworks. Verdict reported that the use of facial recognition for secure payments is expected to double by 2025.

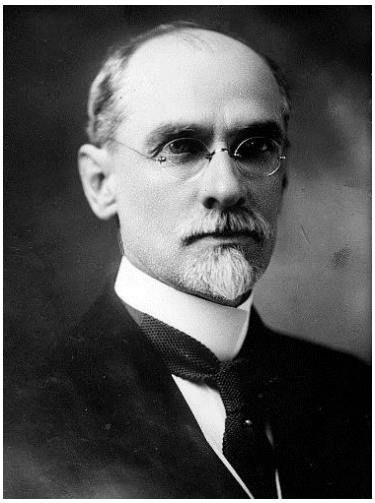


Figure 7: Hugh McCormick Smith: American ichthyologist.

Biometric identification consists of determining the identity of a person. The aim is to capture an item of biometric data from this person. It can be a photo of their face, a record of their voice, or an image of their fingerprint. Amit Agrawal is the Chief Executive Officer of the Unique Identification Authority of India. A biometric signature basically is defined as a method for the signing of electronics documents based on the handwritten signature with using a tablet, computer screen, or similar electronic devices. Following to hand writing, the signature transforms to a simply PDF document and your biometric signature is ready! First-time enrolment is free of cost. Further demographic updates cost ₹50 (63¢ US) and biometric updates cost ₹100 (US$1.30). Aadhaar is the world's largest biometric ID system. Biometric devices have been in use for thousands of years. Non-automated biometric devices have in use since 500 BC, when ancient Babylonians would sign their business transactions by pressing their fingertips into clay tablets. A biometric device is a security identification and authentication device.[3]

Such devices use automated methods of verifying or recognising the identity of a living person based on a

physiological or behavioural characteristic. These characteristics include **fingerprints, facial images, iris and voice recognition**. There are two categories of biometric devices,

1. Contact Devices - These types of devices need contact of body part of live persons. They are mainly fingerprint scanners, either single fingerprint, dual fingerprint or slap (4+4+2) fingerprint scanners, and hand geometry scanners. Slap fingerprints, or "simultaneous plain impressions," are simply multiple flat fingerprints captured at the same time.

2. Contactless Devices - These devices don't need any type of contact. The main examples of these are face, iris, retina and palm vein scanners and voice identification devices.

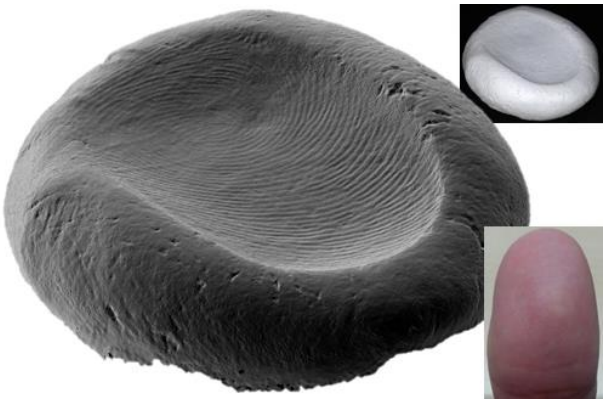


Figure 8: Fingerprint on clay for biometrics.

Types of biometrics: A biometric identifier is one that is related to intrinsic human characteristics. They fall roughly into two categories: physical identifiers and behavioural identifiers. Physical identifiers are, for the most part, immutable and device independent:

Fingerprints: Fingerprint scanners have become ubiquitous in recent years due to their widespread deployment on smartphones. Any device that can be touched, such as a phone screen, computer mouse or touchpad, or a door panel, has the potential to become an easy and convenient fingerprint scanner. According to Spiceworks, fingerprint scanning is the most common type of biometric authentication in the enterprise, used by 57 percent of companies.

Photo and video: If a device is equipped with a camera, it can easily be used for authentication. Facial recognition and retinal scans are two common approaches.

Figure 9: Signature Biometrics.

Physiological recognition: Facial recognition is the second most common type of authentication, according to Spiceworks, in place at 14 percent of companies. Other image-based authentication methods include hand geometry recognition, used by 5 percent of companies, iris or retinal scanning, palm vein recognition, and ear recognition.

Voice: Voice-based digital assistants and telephone-based service portals are already using voice recognition to identify users and authenticate customers. According to Spiceworks, 2 percent of companies use voice recognition for authentication within the enterprise. Voice biometrics is the science of using an individual's voice to authenticate them. This biological characteristic, along with fingerprint, facial, and palm characteristics, is increasingly being used to provide access to virtual and physical spaces.

Signature: Digital signature scanners are already in widespread use at retail checkouts and in banks and are a good choice for situations where users and customers are already expecting to have to sign their names. Signature recognition is an example of behavioural biometrics that identifies a person based on their handwriting. It can be operated in two different ways:

Static: In this mode, users write their signature on paper, and after the writing is complete, it is digitized through an optical scanner or a camera to turn the signature image into bits. The biometric system then recognizes the signature analysing its shape. This group is also known as "off-line".

Dynamic: In this mode, users write their signature in a digitizing tablet, which acquires the signature in real time. Another possibility is the acquisition by means of stylus-operated PDAs. Some systems also operate on smart-phones or tablets with a capacitive screen, where users can sign using a finger or an appropriate pen. Dynamic recognition is also known as "on-line". Dynamic information usually consists of the following information.[4]

Figure 10: DNA Biometrics.

DNA: The biometrics refers to technologies that measure and analyse human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Biometrics has been in the development for many years and with the recent advancements in technology has made some biometrics affordable and more reliable. Our goal is to show how DNA biometrics can improve the network security scheme of an organization. The process of biometrics will be broken down by its process and limitations, accessibility, accuracy, and use with applications. That's why DNA Biometric is essential to make for best recognition. Today, DNA scans are used primarily in law enforcement to identify suspects — and in the movies.[5]

Figure 11: Behavioural Biometrics.

Behavioural identifiers: These are a newer approach and are typically being used in conjunction with another method because of lower reliability. However, as technology improves, these behavioural identifiers may increase in prominence. Unlike physical identifiers, which are limited to a certain fixed set of human characteristics, the only limits to behavioural identifiers is the human imagination. Today, this approach is often used to distinguish between a human and a robot. That can help a company filter out spam or detect attempts to brute-force a login and password. As technology improves, the systems are likely to get better at accurately identifying individuals, but less effective at distinguishing between humans and robots. A touchscreen or touch screen is the assembly of both an input ('touch panel') and output ('display') device. The touch panel is normally layered on the top of an electronic visual display of an electronic device. The display is often an LCD, AMOLED or OLED display. A user can give input or control the information processing system through simple or multi-touch gestures by touching the screen with a special stylus or one or more fingers. Some touchscreens use ordinary or specially coated gloves to work, while others may only work using a special stylus or pen. The user can use the touchscreen to react to what is displayed and, if the software allows, to control how it is displayed; for example, zooming to increase the text size. The touchscreen enables the user to interact directly with what is displayed, rather than using a mouse, touchpad, or other such devices (other than a stylus, which is optional for most modern touchscreens). Here are some common approaches:

1. Typing patterns: Everybody has a different typing style. The speed at which they type, the length of time it takes to go from one letter to another, the degree of impact on the keyboard.

2. Physical movements: The way that someone walks is unique to an individual and can be used to authenticate employees in a building, or as a secondary layer of authentication for particularly sensitive locations.

3. Navigation patterns: Mouse movements and finger movements on track pads or touch-sensitive screens are unique to individuals and relatively easy to detect with software, no additional hardware required.

4. Engagement patterns: We all interact with technology in different ways. How we open and use apps, how low we allow our battery to get, the locations and times of day we're most likely to use our devices, the way we navigate websites, how we tilt our phones when we hold them, or even how often we check our social media accounts are all potentially unique behavioural characteristics. These behaviour patterns can be used to distinguish people from bots, until the bots get better at imitating humans. And they can also be used in combination with other authentication methods, or, if the technology improves enough, as standalone security measures.[6]

Figure 12: Touch screen Biometrics.

Reliability: Authentication credentials such as fingerprint scans or voice recordings can leak from devices, from company servers or from the software used to analyse them. There is also a high potential for false positives and false negatives. A facial recognition system might not recognize a user wearing makeup or glasses, or one who is sick or tired. Voices also vary. People sound different when they first wake up, or when they try to use their phone in a crowded public setting, or when they're angry or impatient. Recognition systems can be fooled with masks, photos and voice recordings, with copies of fingerprints, or tricked by trusted family members or housemates when the legitimate user is asleep. Experts recommend that companies use multiple types of authentication simultaneously and escalate quickly if they see warning signs. For example, if the fingerprint is a match but the face isn't, or the account is being accessed from an unusual location at an unusual time, it might be time to switch to a backup authentication method or a second communication channel. This is particularly critical for financial transactions or password changes. The security of the biometric authentication data is vitally important, even more than the security of passwords, since passwords can be easily changed if they are exposed. A fingerprint or retinal scan, however, is immutable. The release of this or other biometric

information could put users at permanent risk and create significant legal exposure for the company that loses the data.

Privacy risks: Some users might not want companies collecting data about, say, the time of day and the locations where they typically use their phones. If this information gets out, it could potentially be used by stalkers or, in the case of celebrities, by tabloid journalists. Some users might not want their family members or spouses to know where they are all the time. The information could also be abused by repressive government regimes or criminal prosecutors overstepping boundaries. Foreign powers might use the information in an attempt to influence public opinion. Unethical marketers and advertisers might do likewise. Last year, a fitness app was discovered to be collecting information about user locations and exposing it in a way that revealed the location of secret U.S. military bases and patrol routes.

Any of these situations could potentially lead to significant public embarrassment for the company that collected the data, regulatory fines, or class-action lawsuits. If DNA scans become widespread, they give rise to a whole new area of privacy concerns such including exposure of medical conditions and family relationships.[7]

Local or device-based authentication: The most common example of a local authentication mechanism is the hardware security module in a smartphone. User information — such as a fingerprint scan, facial image or a voice print — is stored inside the module. When authentication is required, biometric information is collected by the fingerprint reader, camera or microphone and sent to the module where it's compared to the original. The module tells the phone whether or not the new information is a match to what it already had stored. With this system, the raw biometric information is never accessible to any software or system outside the module, including the phone's own operating system. Smartphone manufacturers are also in the middle of an arms race to make their technology better and easier to use. No other industry — or individual company — can match the scale of mobile investment or the usability and security testing that phones receive. Finally, phone authentication offers users maximum flexibility. They can opt for phones with face ID, fingerprint scanners or voice recognition, or some other new technology that hasn't been invented yet but will dominate the market tomorrow. However, using a third-party mechanism like consumer smartphones puts the authentication process outside enterprise control. Another downside to device-based authentication, in general, is that the identity information is limited to that one device. If people use a fingerprint to unlock their smartphone, they can't then also use that same fingerprint to unlock their office door without separately authorizing the door lock, or to unlock their computer without separately authorizing their PC's fingerprint scanner.[8]

Companies that need to authenticate users or customers on multiple devices in multiple locations need to either have some kind of centralized mechanism to store the authentication credentials or leverage a device that the user carries with them at all times. For example, companies can put the authentication mechanism inside a smart badge that employees wear around the office. They can also use a smartphone to authenticate the employee, then communicate the identity confirmation to other devices and systems via Bluetooth, NFC, WiFi or the internet.

While applying for marriage, either the bride or the groom now needs to provide their biometric details. During registration, however, the couple and their three witnesses have to get their biometrics recorded. The marriage registrars will now be present with their laptops and fingerprint scanners.

Figure 13: Biometrics in marriage.

Tokenization or encryption: Another approach to allowing new devices to recognize existing authorized users is tokenization, one-way encryption, or hashing functions. Say, for example, retinal, voice or fingerprint identification is used to recognize and authenticate employees wherever they might go within a company, but the company doesn't want to have the image or audio files stored on servers where hackers or malicious employees might misuse them. Instead, the company would use a device that, say, scans a person's face or fingerprint, converts that image into a unique code, then sends that code to the central server for authentication.

Any device that uses the same conversion method would then be able to recognize the employee, and the raw identification data is never available on any system. The downside to this approach is that the company is then locked into a single proprietary authentication mechanism.[9]

Advantages and disadvantages of biometrics

The use of biometrics has plenty of advantages and disadvantages regarding its use, security and other related functions. Biometrics are beneficial for the following reasons:

Hard to fake or steal, unlike passwords;
Easy and convenient to use;
Generally, the same over the course of a user's life;
Non-transferable; and
Efficient because templates take up less storage.

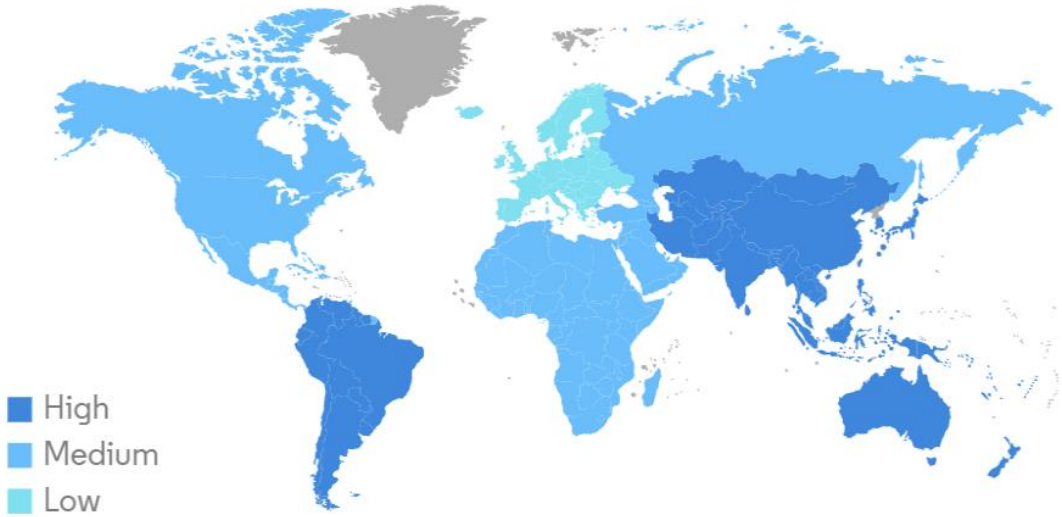
Disadvantages, however, include the following:

It is costly to get a biometric system up and running.
If the system fails to capture all of the biometric data, it can lead to failure in identifying a user.

Databases holding biometric data can still be hacked.
Errors such as false rejects and false accepts can still happen.
If a user gets injured, then a biometric authentication system may not work -- for example, if a user burns their hand, then a fingerprint scanner may not be able to identify them.[10]

Countries using biometrics include Australia, Brazil, Bulgaria, Canada, Cyprus, Greece, China, Gambia, Germany, India, Iraq, Ireland, Israel, Italy, Malaysia, Netherlands, New Zealand, Nigeria, Norway, Pakistan, Poland, South Africa, Saudi Arabia, Tanzania, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States and Venezuela.

Among low to middle income countries, roughly 1.2 billion people have already received identification through a biometric identification program. There are also numerous countries applying biometrics for voter registration and similar electoral purposes. According to the International IDEA's ICTs in Elections Database, some of the countries using (2017) Biometric Voter Registration (BVR) are Armenia, Angola, Bangladesh, Bhutan, Bolivia, Brazil, Burkina Faso, Cambodia, Cameroon, Chad, Colombia, Comoros, Congo (Democratic Republic of), Costa Rica, Ivory Coast, Dominican Republic, Fiji, Gambia, Ghana, Guatemala, India, Iraq, Kenya, Lesotho, Liberia, Malawi, Mali, Mauritania, Mexico, Morocco, Mozambique, Namibia, Nepal, Nicaragua, Nigeria, Panama, Peru, Philippines, Senegal, Sierra Leone, Solomon Islands, Somaliland, Swaziland, Tanzania, Uganda, Uruguay, Venezuela, Yemen, Zambia, and Zimbabwe.



CONCLUSION

The technology is **mainly used for identification and access control or for identifying individuals who are under surveillance**. The basic premise of biometric authentication is that every person can be accurately identified by intrinsic physical or behavioral traits. Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control or for identifying individuals who are under surveillance. The basic premise of biometric authentication is that every person can be accurately identified by intrinsic physical or behavioral traits. The term biometrics is derived from the Greek words bio, meaning life, and metric, and meaning to measure. Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point-of-sale applications. In addition to security, the driving force behind biometric verification has been convenience, as

there are no passwords to remember or security tokens to carry. Some biometric methods, such as measuring a person's gait, can operate with no direct contact with the person being authenticated. Components of biometric devices include the following:
A reader or scanning device to record the biometric factor being authenticated;
Software to convert the scanned biometric data into a standardized digital format and to compare match points of the observed data with stored data; and
A database to securely store biometric data for comparison.
Biometric data may be held in a centralized database, although modern biometric implementations often depend instead on gathering biometric data locally and then cryptographically hashing it so that authentication or identification can be accomplished without direct access to the biometric data itself.

Types of biometrics: The two main types of biometric identifiers are either physiological characteristics or behavioral characteristics. Physiological identifiers relate to the composition of the user being authenticated and include the following:
Facial recognition
Fingerprints
Finger geometry (the size and position of fingers)
Iris recognition
Vein recognition
Retina scanning
Voice recognition
DNA (deoxyribonucleic acid) matching
Digital signatures

Behavioural identifiers include the unique ways in which individuals act, including recognition of typing patterns, mouse and finger movements, website and social media engagement patterns, walking gait and other gestures. Some of these behavioural identifiers can be used to provide continuous authentication instead of a single one-off authentication check. While it remains a newer method with lower reliability ratings, it has the potential to grow alongside other improvements in biometric technology. Biometric identifiers depend on the uniqueness of the factor being considered. For example, fingerprints are generally considered to be highly unique to each person. Fingerprint recognition, especially as implemented in Apple's Touch ID for previous iPhones, was the first widely used mass-market application of a biometric authentication factor. Other biometric factors include retina, iris recognition, vein and voice scans. However, they have not been adopted widely so far, in some part, because there is less confidence in the uniqueness of the identifiers or because the factors are easier to spoof and use for malicious reasons, like identity theft.

Stability of the biometric factor can also be important to acceptance of the factor. Fingerprints do not change over a lifetime, while facial appearance can change drastically with age, illness or other factors. The most significant privacy issue of using biometrics is that physical attributes, like fingerprints and retinal blood vessel patterns, are generally static and cannot be modified. This is distinct from nonbiometric factors, like passwords (something one knows) and tokens (something one has), which can be replaced if they are breached or otherwise compromised. A demonstration of this difficulty was the over 20 million individuals whose fingerprints were compromised in the 2014 U.S. Office of Personnel Management data breach.

The increasing ubiquity of high-quality cameras, microphones and fingerprint readers in many of today's mobile devices means biometrics will continue to become a more common method for authenticating users, particularly as Fast ID Online has specified new standards for authentication with biometrics that support two-factor authentication with biometric factors. While the quality of biometric readers continues to improve, they can still produce false negatives, when an authorized user is not recognized or authenticated, and false positives, when an unauthorized user is recognized and authenticated. While high-quality cameras and other sensors help enable the use of biometrics, they can also enable attackers. Because people do not shield their faces, ears, hands, voice or gait, attacks are possible simply by capturing biometric data from people without their consent or knowledge. An early attack on fingerprint biometric authentication was called the gummy bear hack, and it dates back to 2002 when Japanese researchers, using a gelatin-based confection, showed that an attacker could lift a latent fingerprint from a glossy surface. The capacitance of gelatin is similar to that of a human finger, so fingerprint scanners designed to detect capacitance would be fooled by the gelatin transfer. Determined attackers can also defeat other biometric factors. In 2015, Jan Krissler, also known as Starbug, a Chaos Computer Club biometric researcher, demonstrated a method for extracting enough data from a high-resolution photograph to defeat iris scanning authentication. In 2017, Krissler reported defeating the iris scanner authentication scheme used by the Samsung Galaxy S8 smartphone. Krissler had previously recreated a user's thumbprint from a high-resolution image to demonstrate that Apple's Touch ID fingerprinting authentication scheme was also vulnerable.

REFERENCE

1. Cao, Liling; Ge, Wancheng. "Analysis and improvement of a multi-factor biometric authentication scheme: Analysis and improvement of a MFBA scheme". Security and Communication Networks, 2015; 01(4): 617–625.
2. Alzubaidi, Abdulaziz; Kalita, Jugal. "Authentication of Smartphone Users Using Behavioral Biometrics". IEEE Communications Surveys & Tutorials, 2016; 18(3): 1998–2026.
3. Jain, A. K.; Bolle, R.; Pankanti, S., eds. Biometrics: Personal Identification in Networked Society.

Kluwer Academic Publications, 1999. ISBN 978-0-7923-8345-1.
4. Sahoo, Soyuj Kumar; Choubisa, Tarun; Prasanna, SR Mahadeva. "Multimodal Biometric Person Authentication: A Review". IETE Technical Review, 2012; 29(1): 54–75.
5. Haghighat, Mohammad; Abdel-Mottaleb, Mohamed; Alhalabi, Wadee. "Discriminant Correlation Analysis: Real-Time Feature Level Fusion for Multimodal Biometric Recognition". IEEE Transactions on Information Forensics and Security, 2016; 11(9): 1984–1996.
6. Arnau-González, Pablo; Katsigiannis, Stamos; Arevalillo-Herráez, Miguel; Ramzan, Naeem. "BED: A new dataset for EEG-based biometrics". IEEE Internet of Things Journal. (Early Access), 2021; 15: 12219–12230.
7. Breckenridge K. "The Biometric State: The Promise and Peril of Digital Government in the New South Africa". Journal of Southern African Studies, 2005; 31: 2, 267–82.
8. Dr. Sampa Dhabal, Kushal Nandi, Amrita Chakraborty, Dr. Dhrubo Jyoti Sen, Dr. Khokan Bera, Arpita Biswas, Suprodip Mandal and Dr. Dhananjoy Saha; CSI (Crime Scene Investigation): first step to unfold the network of crime: Journal of Forensic Science and Legal Medicine, 2021; 1(2): 05–16.
9. Ratha, N. K., J. H. Connell, and R. M. Bolle. "Enhancing security and privacy in biometrics based authentication systems". IBM Systems Journal, 2001; 40(3): 614–634.
10. Prof. Dr. Dhrubo Jyoti Sen; Think of ink gives a link to make a mind pink and eyes to blink: European Journal of Biomedical and Pharmaceutical Sciences, 2016; 3(12): 01–07.