WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Biometric Authentication: Security, Development and Future work

Pratiksha Kamble[1], Harshal Jadhav[2] ,Dhiraj Raste[3] , Tejas Bhange [4] , Prathmesh Date[5] , Dr. Sharmila S. More[6]

Dept. of Science and Computer Science
MITACSC Pune, India
[6] Assistant Professor of Department and Computer Science

ABSTRACT :

Biometric authentication is a way of identifying and authenticating users. In this paper, we explain biometric authentication and its use in identifying users. Biometric authentication uses unique physical or behavioral characteristics, such as fingerprints, patterns of a person's face, iris patterns, and voice recognition to grant access to devices. The paper discusses the advantages of biometric authentication over traditional methods, such as passwords, PINs or smart cards, as biometric traits are difficult to replicate or steal. The paper also examines the various types of biometric authentication systems and their relative strengths and weaknesses. The paper concludes by emphasizing the potential of biometric authentication as a secure and convenient method of identification in various applications.

Keywords: Biometric authentication, physical characteristics, behavioral characteristics, identifying users, authenticating users

I. INTRODUCTION :

Every day technology grows and evolves, and with this growth, we have an increase in technology users. Users and the technology that they use produce enormous collections of data, and some of this data for whatever reason, we do not want to make it public. Here comes the question of how we will secure this data one hundred percent. This question is difficult to answer since it is theoretically not possible to be one hundred percent safe. However, to secure information, most of us have used and still use passwords, PINs, or smart cards which represent what we know and what we have in authentication systems. But we all know that some of these are breakable for example passwords - people usually associate a password with some personal event when they set a password and some can be stolen - a smart card. Knowing that we cannot rely on passwords and classic forms of information security, then cybersecurity has decided to go one step further and cooperate with the human body and behavior also known as biometrics which represents what we are in authentication systems. When biometrics are mentioned, we immediately think of human eyes, faces, ears, palms of hands, and fingerprints. These are the parts of our body that we focus on since they are unique in different persons. What is also unique is our behavior, like the way we walk, our voice, and our keystroke. It is already proven that every person has unique fingerprints, unique IRIS, forms of ears, faces, voices, and signatures. The uniqueness of these parts of our body and behavior is the reason why in the last decades the technology industry is trying to use biometric authentication, for example, the smartphone industry has focused on opening the phone using fingerprints and face recognition. With all the advantages that biometric authentication and identification give for example, we do not need to remember long and complicated passwords and carry smart cards, it has also disadvantages if we do not implement them in the right way or in the right place.

II. BIOMETRICS :

A. Definition and use

Initially, biometrics means the branch that deals with the use of the characteristics of the human body to identify a person, e.g. if a certain crime is committed and there are fingerprints, then the main suspect is the person to whom those fingerprints belong.
Fingerprints represent a unique human biometric that is being used a lot today in information security. In recent years it has been used a lot in smartphones, personal tablets, and also laptops thus enabling the opening of the device. One of the reasons why biometrics are used for such purposes is that, apart from being significantly more secure than passwords or PINs, they also save more time, and, above all, they are not something that can be forgotten since they are characteristics of the body. But in addition to the advantages that biometrics have, they also have some disadvantages, where if we take a very simple example of fingerprints, what happens if we lose a finger (e.g. in an accident) or even suffer a fingerprint burn? Well, the answer is very simple, we cannot open the phone in this case, assuming of course that the phone opens with the finger in which we have suffered an injury.

B. Specifications

Biometrics are divided into physiological and behavioral. Common biometrics that is used for authentication and identification are:

Physiological

- Fingerprint recognition
- Hand geometry
- Iris recognition
- Facial recognition
- Signature recognition
- Vein recognition
- Retina recognition
- DNA recognition
- Blood type

Behavioral

- Typing rhythm
- Mouse dynamics
- Keyboard dynamics
- Voice recognition
- Walking style
- Personality

An ideal biometric system would posses several key characteristics:

1. Universality: The biometric should be applicable to all individuals, regardless of age, gender, race or other demographic factors.
2. Uniqueness: The biometric should be able to distinguish one individual from all other, with a low rate of false matches.
3. Permanence: The biometric should remain stable over time, so that it can be used for identification and authentication in the long-term.
4. Collectabillity: The biometric should be easly collectable and measurable using non-intrusive methods.
5. Performance: The biometric should have a high level of accuract and reliability, with low rastes of false matches and false non-matches.
6. Acceptability: The biometric should be socially and culturally acceptable, with a low level of perceived instrusiveness or privacy invasion.
7. Circumvention: The biometric should be difficult to circumvent or forge, ensuring the system's security.
8. Interoperability: The biometric should be able to work with a variety of different systems and devices, allowing for east intefration and use.
9. Robustness: Biometric systems should be resilient to variations in environmental conditions (such as lighting or noise), as well as changes in the user's physical or behavioral characteristics. Robustness ensures consistent performance under diverse operating conditions.
10. Security: Biometric systems must incorporate strong security measures to protect biometric data from unauthorized access or tampering.

By embodying these characteristics, biometric systems offer an effective and reliable means of authentication and identification, enhancing security, convenience, and user experience across various applications and industries.

C. Biometrics vs passwords

Passwords have been in use since the legend of Ali Baba. However, we have long been told that passwords are outdated, inconvenient, and a security risk. Whenever news on a password security breach circulates, some commentator, vendor, or expert comes forward and says 'biometrics is the solution'. Historically, biometric solutions have always been launched with the claim of achieving the highest security, while traditional passwords were known for their shortcomings. Unfortunately, security attackers do not simply give up their self-enriching efforts and go home defeated.

Aspect	Biometrics	Passwords
Maturity	Developing	Ubiquitous
Discrimination	Medium to high • Depends on modality	High • Large password space results in high entropy
Technical strength	Medium • Prone to spoofing • Depends on hardware quality	Strong • Long string leads to high entropy • Long computation time to exhaust • Cryptographically strong algorithms can't be reverse engineered
Procedurally	Strong • Not much dependence on human discipline • Inherently good	Weak • Short passwords leads to low entropy • Easy-to-guess passwords gives low or zero entropy • Zero entropy if: ◦ written down ◦ revealed to someone • Vulnerable to social engineering attacks

Table 1. Strength comparison of biometrics and passwords

Passwords are disliked by many people (users and experts) but have proven to be a strong contender. Biometric schemes are not the only systems that have failed to supplant them. None of the proposed alternative authentication mechanisms can match the security evaluation statistics that traditional passwords already provide. Despite countless efforts to supplant them, their continued ubiquity speaks volumes about their credibility and accomplishments. In particular, passwords are not the problem: rather it is the way we interact with them. Like them or loathe them, passwords are here to stay for the foreseeable future, where the objective is not impenetrable security but reducing harm at an acceptable cost: on the other hand, biometrics has major potential for areas such as law enforcement, identity management, airport security, counter-terrorism, child recovery, healthcare, etc. In these and similar cases, biometrics achieve implicit credibility. However, privacy will always remain the key concern for these systems' implementation, besides possibly empowering inappropriate approaches of stigmatization and exclusion (eg, racism or ageism) using ancillary biometric information.

III. SECURITY :

We know that despite the greater security of biometrics, these are also falsifiable and someone else can be identified instead of someone else. If we take some examples e.g. Fingerprints can be easily taken from a glass that we drank water and identified as us, our face is also very easy to take, where only a qualitative picture of us is enough to be identified, the retina also by means of a picture can be provided, so as we can see that even by these metrics we are down. In addition to fakes, we also have cases when the system itself gives access to someone else, if we take an example of facial identification on a fake phone, there are cases that guarantee someone else access due to the similarity of the face with the owner of the phone, but this happens very rarely, since biometrics have a property of updating, selflearning or evolution, thus guaranteeing access only to the authorized person, because if there was no evolution, then only with the aging of the owner, the owner of the phone would not have the opportunity to open the device.

Figure 1. Forgery of fingerprints

The biometric system must verify liveness, otherwise, the system can be fooled with duplicate biometric features. Sometimes the vitality test can be replaced by a guard(human), however, it is debatable whether a guard can protect against more advanced biometric forgeries (like a thin layer of silicon on fingerprints).

A. Applications

Some of the applications where biometrics are used are:

- Computer/Network Security
- Online transactions
- Security of the physical area
- Bank(ATM)
- Voting

Then taking into account the digitization of almost every service that we have developed in the traditional way (physically waiting for an order for a service), now most of them are done online, therefore transactions are also requiring a biometric authentication to verify identity, or Banks are deciding even fingerprint identifiers in ATMs or facial recognition, or a very targeted application would be electronic voting, which is going more and more every day around such a vote, also in prisons by identifying visitors who enter.

B. Behavioral authentication

So far we have only talked about biometrics such as fingerprints, facial recognition, retinal scanning, and so on, but these are physical characteristics of the human body that already exist. Another biometric is the authentication through the behavior of the individual, which means that we do not need to perform the authentication by taking any action, such as giving a password or scanning the finger but only want to access somewhere that we have performed the authentication. Although it seems a bit strange at first, it turns out to be very successful. Even this method of authentication has already come into use, such as in institutions with high security. This authentication can be developed in several ways, some of which we will mention below, e.g. the way an individual walks can be a type of password that can be detected through the sensor of smartphones, knowing that smartphones have this type of sensor that is used to track our activity during the day, another authentication can be even the way we type on our computer keyboard, i.e. the

location of our fingers, the speed of writing, etc. Another authentication is done by moving the cursor, i.e. the way we move it, also the way we grab the phone and hold it, another way can be the way we speak, for example, which vowels we pronounce more or similar characteristics.

These systems use AI and ML in order to learn our behaviors continuously since they can change over time, so they are not like a password that has a certain value, and they are also not like physical characteristics that have a certain pattern that does not change. Also, a nice advantage of these systems is that we are continuously in the process of authentication, so even after authentication where we have gained access somewhere, we may be denied access later, because e.g. we pass the authentication with facial recognition on the phone, and someone else can freely use my phone since there is only one authentication at the beginning, while through behaviors if someone else picks up our phone, based on their behaviors the system understands that is not authorized to use that device. But of course, despite the advantages that this type of authentication has, it also has its own disadvantages, because in the event of an accident, our walk is not the same, nor are our behaviors, also in the event of an illness, authentication through speech will not work, or even in case of the influence of any narcotic substance or alcohol, the authentication will also not work.

General Scenario: Human gesture/gait has been used as a modern method to identify/authenticate individuals' identities. Due to the increased demand for employing an efficient technology that provides a high level of security, gait recognition received significant attention from various security research communities. It is an emerging technology that showed an acceptable performance in video surveillance. Fig.3, shows the basic mechanism of the gait recognition system.

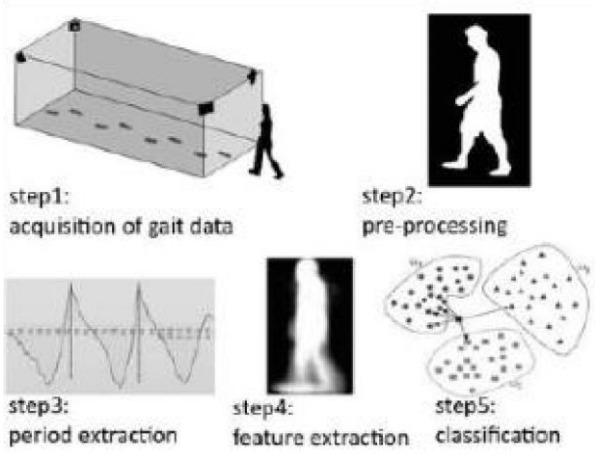

Figure 2. Block diagram of gait recognition system

Identifying/recognizing a person based on his/her style of walking is one of the behavioral biometrics techniques since it depends on the analysis of body structures or body movements. As a general idea, limb movements in any living organism refer to the ability of walking which is also known among human beings as human locomotion. In order to provide a unique identity, an extraction of body movements can be obtained from a repeated style of walking (gait cycle) that comes from balanced cooperation among a human legs, body, and arms.

C. Ear Recognition

Another biometric authentication technique is conducted based on the recognition of the unique shape and appearance of the human being's ear. Naturally, a person is born with a visual shape of his/her ears. However, the human ear is not subject to change while a person's growth and even aging. It has dependable stability which increases its level of security as a proposed method for the security identification/verification of individuals.

D. Retina Geometry Technology

It is based on the blood vessel pattern in the retina of the eye as the blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person (figure 3). The retina is not directly visible and so a coherent infrared light source is necessary to illuminate the retina. The infrared energy is absorbed faster by blood vessels in the retina than by the surrounding tissue. The image of the retina blood vessel pattern is then analyzed.

Figure 3. Image of retina

Retina scans require that the person removes their glasses, places their eye close to the scanner, stares at a specific point, remain still, and focus on a specified location for approximately 10 to 15 seconds while the scan is completed. A retinal scan involves the use of a low-intensity coherent light source, which is projected onto the retina to illuminate the blood vessels which are then photographed and analyzed. A coupler is used to read the blood vessel patterns. A retina scan cannot be faked as it is currently impossible to forge a human retina. Furthermore, the retina of a deceased person decays too rapidly to be used to deceive a retinal scan. A retinal scan has an error rate of 1 in 10,000,000, compared to fingerprint identification errors sometimes as high as 1 in 500.

E. Signature dynamics

The signature dynamics recognition is based on the dynamics of making the signature, rather than a direct comparison of the signature itself afterward. The dynamics are measured as a means of the pressure, direction, acceleration, and length of the strokes, dynamics number of strokes, and their duration. The most obvious and important advantage of this is that a fraudster cannot glean any information on how to write the signature by simply looking at one that has been previously written. Special pens are able to capture movements in all 3 dimensions. Tablets have two significant disadvantages. First, the resulting digitalized signature looks different from the usual user signature. And input devices second, while signing the user does not see what he/she has written so far. He/she has to look at the computer monitor to see the signature. This is a considerable drawback for many (inexperienced) users. Some special pens work like normal pens, they have ink cartridges inside and can be used to write with them on paper. The accuracy of the signature dynamics biometric systems is not high, the crossover rate published by manufacturers is around 2%, but according to our own experience, the accuracy is much worse.

F. DNA Analysis

This method of verification is mostly used in criminal cases. DNA of the user in the form of blood, tissue, hair, and nails is collected for confirmation. DNA analysis takes time. DNA also is a unique characteristic but a hair or nail can be stolen.

First of all, DNA differs from standard biometrics in several ways:

- DNA matching does not employ templates or feature extraction but rather represents the comparison of actual samples.
- DNA requires a tangible physical sample as opposed to an impression, image, or recording.
- DNA matching is not done in real-time, and currently, not all stages of comparison are automated.

Regardless of these basic differences, DNA is a type of biometric inasmuch as it is the use of a physiological characteristic to verify or determine identity. DNA testing is a technology with a high degree of accuracy however, the possibility of sampling contamination and degradation will pose an impact on the accuracy of the method [10]. IV. RECENT ADVANCES IN THE USE OF BIOMETRIC TECHNOLOGY IN DEVICES
Recent advances in the use of biometric technology in devices include:

- Smartphones: Biometric sensors such as fingerprint scanners, facial recognition cameras, and iris scanners are becoming increasingly common in smartphones. These sensors are used to unlock the device and authenticate mobile payments.
- Laptops and tablets: Laptops and tablets are also adopting biometric technology, such as fingerprint scanners, facial recognition cameras, and iris scanners, to enhance security and convenience for users.
- Smart home devices: Smart home devices, such as door locks and security cameras, are using biometric technology to enable secure and convenient access for authorized users.
- Internet of Things (IoT) devices: Biometric technology is being integrated into IoT devices to improve security and personalization. For example, biometric sensors in smartwatches can be used to authenticate mobile payments and track fitness.
- Automotive: Biometric technology is being used to enhance the security of connected cars. Some carmakers have started to use fingerprints and facial recognition technology to unlock and start the car,
- and to personalize settings such as seat and mirror positions.
- Banking: Biometric technology is being increasingly used in the banking sector, such as fingerprint and facial recognition to authenticate transactions, along with other biometric identification methods such as voice and iris recognition.

Overall, the use of biometric technology in devices is becoming more prevalent as it improves the security and user experience, and the technology is becoming more affordable and accessible.

Table 2. Biometrics in commercial devices

Provider	Solution name	Sensor	Modality	Application
Samsung	Intelligent Scan	Infrared camera module and an infrared LED	Iris and face	Smartphone screen unlock, Secure Folder access, Samsung Pay
	Fingerprint scanner	Capacitive sensor	Fingerprint	
Huawei	Face unlock	RGB camera	Face	Smartphone screen unlock
	Fingerprint scanner	Capacitive sensor	Fingerprint	
Apple	Face ID	TrueDepth Camera	3D Face	Smartphone screen unlock, Apple pay, unlock banking app and Paypal
	Touch ID	Capacitive sensor	Fingerprint	
Vivo	Face ID	Time of Flight (TOF) 3D depth-sensing system with 300,000 sensor points	3D Face	Smartphone screen unlock
	Fingerprint scanner	Qualcomms ultrasonic In-Display Fingerprint Scanner	Fingerprint	
OnePlus	Face unlock	RGB camera	Face	Smartphone screen unlock
Google	Smart Lock	Depends on the smartphone	Voice, fingerprint, or face	Smartphone screen unlock

The **iPhone** 13 includes the latest version of Apple's Face ID technology, which uses facial recognition to unlock the device and authenticate user actions. This technology uses a TrueDepth camera system that projects and analyzes over 30,000 invisible dots to create a precise depth map of the user's face, which is then used to authenticate the user. The Face ID system is designed to be fast, secure, and easy to use, and it can be used to unlock the device, make purchases, and access password-protected apps.

Additionally, the iPhone 13 also includes Touch ID, which is a fingerprint recognition system that allows users to unlock their devices and authenticate purchases by placing their fingers on the home button. The Touch ID system is also fast, secure, and easy to use, and it provides an alternative means of authentication for users who prefer not to use facial recognition.

It's important to note that, while iPhone 13 includes both Face ID and Touch ID, the biometric features may vary by region, carrier, or model of the device.

Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a type of user credential that is tied to a device and uses a biometric or PIN.

- Facial recognition. This type of biometric recognition uses special cameras that see in IR light, which allows them to reliably tell the difference between a photograph or scan and a living person. Several vendors are shipping external cameras that incorporate this technology, and major laptop manufacturers are incorporating it into their devices, as well.
- Fingerprint recognition. This type of biometric recognition uses a capacitive fingerprint sensor to scan your fingerprint. Fingerprint readers have been available for Windows computers for years, but the current generation of sensors is more reliable and less error-prone. Most existing fingerprint readers work
- with Windows 10 and Windows 11, whether they're external or integrated into laptops or USB keyboards.
- Iris Recognition. This type of biometric recognition uses cameras to perform scans of your iris. HoloLens 2 is the first Microsoft device to introduce an Iris scanner. These iris scanners are the same across all HoloLens 2 devices.

V. RECENT DEVELOPMENTS IN BIOMETRIC AUTHENTICATION

Recent developments in biometric authentication include:

- Face recognition: Advancements in deep learning and artificial intelligence have led to significant improvements in facial recognition technology. This has made it possible to identify individuals from a distance, in poor lighting, or with masks on.
- Behavioral biometrics: Behavioral biometrics is the process of identifying individuals based on their unique behavior, such as keystroke dynamics, mouse movement, and gait analysis. These methods are becoming increasingly popular as they can be used to authenticate users without the need for physical contact.
- Multi-modal biometrics: Multi-modal biometrics involves the use of multiple biometric traits, such as fingerprint and facial recognition, to identify an individual. This approach is more secure than using a single biometric trait and can also improve the user experience.
- Biometric liveness detection: Liveness detection is used to ensure that the biometric data being used is from a live person and not a fake or spoofed biometric.
- Fusion of biometrics with other authentication methods: Biometric authentication is increasingly being combined with other authentication methods, such as knowledge-based authentication (KBA), to create more secure and convenient authentication systems.
- Biometric on Edge: Biometric authentication on edge devices such as smartphones, tablets, and laptops is becoming more common. The use of edge-based biometrics reduces the need for a centralized database and helps to protect users' privacy.

VI. FUTURE WORK :

Considering that authentication based on biometrics is developing every day and more, of course, it will advance even more in the future, thus making authentication and the security of sensitive information even more secure.

Some of the future trends for biometric authentication include the following:

- Physical Identity Verification: The expansion of AIdriven biometrics, particularly facial and behavioral biometrics (gait, voice, and accent recognition), will fuel new forms of real-time biometric identity verification through on-premises cameras.
- Advanced Biometric Authentication: While there are reliable forms of biometrics and biometric passwords in the market now, new technologies are focusing on drawing even more advanced biometric markers from the body, each providing another hard-to-fake marker to use for secure authentication. These can include odor recognition, heartbeat pattern recognition, hand geometry, and DNA signature reading.
- Identity Proofing: One of the strengths of biometric authentication is the assumption that the user must be physically present to provide biometric data. Even stronger measures, like live identity verification or AI-driven video identity verification, layer additional “liveness” testing into the processes to thwart emerging forms of identity fraud.
- Continuous Authentication: Authentication usually happens once, during login, or multiple times based on user access to different resources. Continuous authentication uses behavioral patterns or other markers to maintain authentication to guarantee continued user verification over time periodically.

Regarding the issues where biometric authentication will be applied, it is likely that the use of this technology will increase initially in banks, electronic voting in countries where such voting is allowed, and high-security institutions where only persons must enter authorized, it can also be applied to educational or similar institutions (driver's license), in cases of testing, and also not to forget the airports, since only airports use such technologies.

VII. CONCLUSIONS :

The security of personal or sensitive information has a much earlier history than today, or better we can say in the last two centuries, where often even short but more important information has given another direction to the history of humanity and wars differently. This is also the main reason that today one of the main focuses of technology is that only authorized persons have access to this information and that no one else has the opportunity to provide access in any other way. Therefore, through authentication, we must identify ourselves as the one who has access to that information, as we know that until recently and even now, authentication was initially done with a password, but the password presented a
problem to society since people usually create the password they enter something related to them, for example, NameSuraname1980, something that is very predictable from the attackers to find that password, another problem is that often out of fear of forgetting the password they also write it on a piece of paper, thus exposing the password to a second person. Although passwords have recently started to become more complex and also two-factor authentication, reducing the possibility of attacks by hackers, for example, a typical password today contains at least 8 characters, one uppercase letter, one lowercase letter, a number, and at least one symbol. To avoid passwords and any type of password attacks or even the monotony of writing them, we have reached biometrics as a much safer form of authentication, where every day we are avoiding passwords or PINs by replacing them with one of the biometrics that is being offered to us. Well, is this also 100% safe, of course not! Immediately with the introduction of biometrics in the industry, hackers also began to find new ways of attacking and breaking them, where in fact sometimes it seems very simple to break them. Biometrics were also categorized into two categories, such as physical biometrics and non-physical (behavioral) biometrics, as one of the safe and unique physical biometrics that provides authentication only for an individual was fingerprinted, but even this began to be forged by stealing from us the knees simply from a glass of water we drank. Then also comes into play the scanning of the retina, the face, then from the non-physical biometrics, walking, the way of speaking, behavior, etc. But with biometrics, a new problem arose, since people often hate being tracked in any way, so why give their fingerprints, face, or any physical characteristic of their body or behavior? But on the other hand, of course, these features are more secure than passwords. In this paper, we have tried to explain what biometrics are, tell about their types, which are more suitable for use, which require fewer resources, how safe they are, how they can be stolen or forged, and how they can fail. their functionality, their application, and the future of this type of authentication.
From the knowledge and study we have developed, we think that no matter how secure biometrics are, they also have their weaknesses and sometimes their non-functionality, where attackers will always use them, but of course, our duty is to let's make this process as difficult as possible, therefore for the most secure authentication and the security of the private data of an individual, business, or institution, of course, we must have authentication with two factors or multifactor where these factors can there are combinations of passwords and biometrics or combinations of different biometrics. In this way, it will be a much more secure authentication in the future.

REFERENCES :

1. J.D. Ross, A. Jain, and R. Bolle, "The ideal biometric trait," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 36, no. 3, pp. 303-316, May 2006.
    A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Commun. ACM, vol. 43, no. 2, pp. 90-98, 2000.
2. K. Siddique, Z. Akhtar, and Y. Kim, "Biometrics vs passwords: a modern version of the tortoise and the hare," Computer Fraud & Security, pp. 13-17, 2017.
3. M. Espinoza, Ch. Champod, and P. Margot, "Vulnerabilities of fingerprint reader to fake fingerprints attacks," 2011.
4. V. Matyas and Z. Riha, "Security of biometric authentication systems," 2010.
5. V. Pujari, R. Patil, and Sh. Sutar, "Research paper on biometrics security," 2021.
6. Alsaadi, "Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: a review," 2021.
7. Alsaadi, "Physiological biometric authentication systems, advantages, disadvantages, and future development: a review," International Journal of Scientific & Technology Research, vol. 4, 2015.
8. K. Gupta, "Review paper on biometric authentication," International Journal of Engineering Research & Technology (IJERT) VIMPACT – 2017 (Vol. 5, Issue 23).
9. S. Bhable, S. Kayte, R. Maher, J. Kayte, and C. Kayte, "DNA biometrics," 2015.
10. N.K. Ratha, J.H. Connell, and R.M. Bolle, "Recent advances in biometrics: a survey," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 36, no. 3, pp. 303316, May 2006.
11. S.K. Sharma, K.N. Plataniotis, and A.N. Venestsanopoulos, "Recent developments in biometric on edge: a review," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 46, no. 1, pp. 3-17, 2016.
12. [Online]. Available: https://support.apple.com/enus/HT208108#:~:text=The%20technology%20that%20enables%20Face,infrared%20image%20of%20your%20face.
13. [Online]. Available: https://learn.microsoft.com/enus/windows/security/identity-protection/hello-for-business/hellooverview
14. X. Liu, J. Wu, and Y. Wang, "Recent advances in face recognition: a survey," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 4, no. 2, pp. 168-186, 2020.
    A. Ross and N.K. Ratha, "Recent advances in behavioral biometrics: a survey," IEEE Transactions on Information Forensics and Security,
15. vol. 11, no. 6, pp. 1460-14
16. K. W. Bowyer, K. I. Chang, P. Yan, and P. J. Flynn, "Multi-Modal
17. Biometrics: An Overview," IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 297-314, 2007.
18. Xing Liu, Qiang Ji, and Anil K. Jain, "Recent Developments in Biometric Liveness Detection: A Review," IEEE Transactions on Information Forensics and Security, vol. 15, no. 12, pp. 3196-3211, 2020.

19. Ahmed Bouridane, David Zhang, and Farzin Deravi, "Recent Developments in Fusion of Biometrics with Other Authentication Methods: A Review," International Journal of Computer Science and Biometrics, vol. 8, no. 4, pp. 1-20, 2020.