NAME: DHRUVIT KISHORBHAI VANANI

STUDENT ID: 3566984216

PAPER TITLE: BIOMETRICS IN CYBERSECURITY: CHALLENGES AND SOLUTIONS

COURSE NAME: CSci530 Computer Security Systems

I have read the Giude to Avoiding Plagiarism published by the student affairs office. I understand what is expected of me with respect to properly citing sources, and how to avoid representing the work of others as my own. The material in this paper was written by me, except for such material that is quoted or indented and properly cited to indicated the sources of the material. I understand that using the words of others, and simply tagging the sentence, paragraph, or section with a tag to the copied source does not constitute proper citation and that if such materiel is used verbatim or paraphrased it must be specifically conveyed (such as through the use of quotation marks or indentation) together with the citation. I further understand that overuse of properly cited quotations to avoid conveying the information in my own words, while it will not subject me to diciplinary action, does convey to the instructor that I do not understand the material enough to explain it in my own words, and will likely result in a lesser grade on the paper.

Signed: Dhruvit Kishorbhai Vanani

Biometrics in Cybersecurity: Challenges and Solutions

Dhruvit Vanani
Master of Science in Computer Science
University of Southern California
vanani@usc.edu

***Abstract*--The use of biometrics in various personal and commercial security systems is increasing. The number of platforms and devices joining the Internet of Things (IoT) is growing exponentially every day. Numerous gadgets, including smartphones, tablets, sensors, cloud-based services, etc., constantly send and receive information. Although passwords are troublesome and occasionally users use the same password for several devices, it is necessary to protect this data from unwanted individuals. I intend to address the most difficult problems in this study if the biometric attribute is compromised. A deeper discussion will be given on physical spoofing, deepfakes, and other privacy issues that can develop after designing a biometric system. I also go over the elements that must be considered while developing private and secure biometric authentication systems. These techniques include multi-modal biometric systems, touchless fingerprints, and hashed biometric templates. In future the use of facial, voice or other types of biometric verification will be added to security measures for gaining access to sensitive information at work, applying for a loan from a bank, or using money management systems in the future.**

Keywords--IoT; Spoofing; Deepfakes; Multi-modal

I. Introduction

Concern over security attacks related to online transactions has grown as a result of the internet's rapid expansion and the interconnectedness of computers for use in a variety of applications, including online banking, e-commerce, and mobile commerce. The rapidly expanding digital world offers huge advantages, but it also poses serious risks to the nation's administration, military, and other vital sectors. With cybercrime increasing daily, cyber-security in biometrics is a significant problem in today's digital world. Experts in the field of information security are searching for trustworthy and strong security measures as a result of the losses and distress brought on by cyber-attacks.

Even biometric technology does not ensure absolute cybersecurity. While biometric security is far more difficult to fool than password security, breaches are still possible. While high-quality cameras and other sensors are used in biometric cybersecurity, attackers can still attack them. Attackers can obtain biometric data from people without their knowledge or consent because people do not shield their gait, voice, hands, ears, or faces. Biometric scanners that use facial recognition technology can also be tricked. For example, when the researchers at the University of North Carolina were building 3-D models using 2D facial photographs, they tried to get into five security systems out of which four of them were able to bypass. When iPhone X was released, facial recognition system of Apple decided to test the system by using a 3-D printed mask. After the tests, they discovered that family members of the user such as kids or siblings can disable the face ID [2]. According to the research, removable devices are still the top threat source after the internet. 14.4% of all biometric data processing systems stopped threats coming from the internet, including phishing websites and web-based email services. 8% of all attempts to spread worms that infect computers and then download spyware and remote-access Trojans used removable media. The remaining threats come from Email clients and network folders which comprise around 8% in total.[3].

Figure 1 shows the main sources of threats to biometric data processing and storage systems in 3rd quarter of 2019.

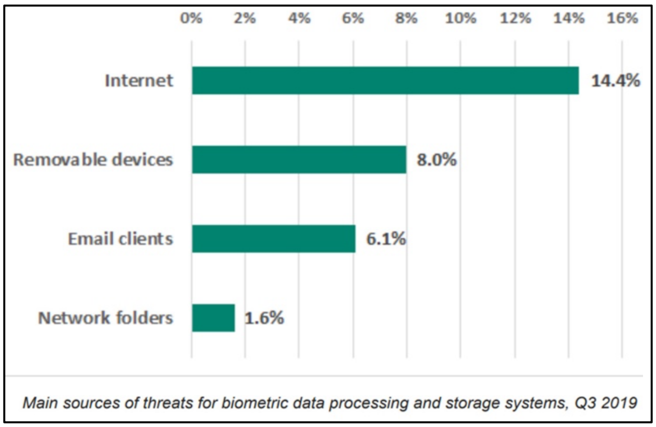

Fig.1: Sources of biometric data processing threats

This paper's main goal is to review the research on the issues occurred in biometric system authentication and how to solve them or at least try to mitigate the risk of an attack by an adversary. I also point out the positive aspects and areas for improvement in these works. We may better understand the gaps and issues with the help of this assessment.

Practically, growing numbers of passengers flying across borders, crowds in public spaces and, not least, terror-related risks – all make image processing using iris recognition methods at increasing speeds a growing necessity. For one, a broad range of adopters are concerned including, but may not be limited to, security agencies, smart device developers, smart home manufacturers and, not least, end users becoming more and more aware of security and privacy issues.

The current situation for biometric security is covered in Section 2. The main challenges in the field of biometric research security are discussed in Section 3. This covers various issues across different categories like attacks, privacy issues and limitations. Finally, in the last section, I have described various solutions to prevent biometric attacks.

II. CURRENT SITUATION

In recent years biometric recognition has been used to identify criminals, track patients in medical informatics, and personalize social services. Despite significant effort, there are still unanswered problems regarding the administration and effectiveness of biometric recognition systems, as well as the suitability and societal implications of their use. Increasing worries about national security and the tracking of people as they cross borders have led to passports, visas, and border-crossing records being connected to biometric data as biometric technologies now seem ready for wider adoption. The military has started using biometric techniques to identify people as allies or enemies in order to combat terrorism and insurgencies. Commercially, a large number of laptop computers, handheld gadgets, mobile phones, and other consumer electronics increasingly have finger-imaging sensors due to their lower cost and smaller physical size.

III. CHALLENGES FACED IN BIOMETRIC SYSTEMS

Like many other technologies, biometrics can provide problems for attacks from adversaries. It is important to highlight those biometrics are not intrinsically incompatible with privacy; rather, how systems are developed and implemented determines how much privacy is enhanced or violated by biometrics.

ATTACKS ON BIOMETRIC SYSTEMS

A. *Spoofing*

One of the most frequent risks is spoofing, in which the biometric templates of individuals can be utilized improperly. During enrollment, a fraudster may create false biometrics. Impostor templates can take the place of legitimate templates to grant access to restricted areas. To trick the system into thinking an impostor is a real user, a spoofing attack replays either raw data or biometric traits gleaned from raw data. The well-known gummy bear spoof was created by Japanese researcher Tsutomu Matsumoto in 2002. It employed a latent fingerprint on glass, gelatin from Gummy Bear candies, and a plastic mould to trick 4 out of 5 fingerprint sensors at the time. A pulse, temperature, and capacitance may now be detected by fingerprint sensors, verifying the presence of a live person and enhancing robustness to "gummy bear" derivative assaults[5].

B. *Denial of Service (DoS) Attacks and Replay Attacks*

An attacker may exhaust all available system resources to the point where legitimate users who need access are turned away. For instance, a server that handles access requests may be inundated with a high number of fraudulent requests, overtaxing its computational capacity and hindering the processing of legitimate requests. No staff can access network resources during an assault, and in the case of Web servers hosting eCommerce websites, no customers can make purchases or get support. Companies can lose as much as $20,000 per hour in the event of a successful attack, while the exact amount varies.

In a Replay attack, the biometric system's data stream is injected between the sensor and the processing system. Two to three stages can be included in a repeat attack. It initially duplicates or intercepts the sensor transmission, adjusts the data, and then replays the information. The key to thwarting such an assault is using the proper encryption technique. When keys are decoded from encrypted communications at the conclusion of the transmission, they unlock the message. Whether the person who intercepted the initial transmission can read or interpret the key is irrelevant in a replay attack. He or she only needs to copy everything, including the message and key, and send it again.

C. *Trojan Horse Attack*

To create the needed features and add them to the existing database, the feature extractor is itself replaced in a Trojan horse assault. Spoof detection technology has become an essential component of biometric systems to identify, control, and minimize biometric attacks in light of growing security concerns. Trojans are a type of malware that, like most malware, can harm files, reroute internet traffic, track user behavior, steal sensitive data, or create backdoor entry points to the system. Trojans are capable of deleting, blocking, altering, leaking, or copying data, which can later be returned to the user for ransom or sold on the dark web. Diverse fresh strategies are being developed by researchers for a safe biometric system.

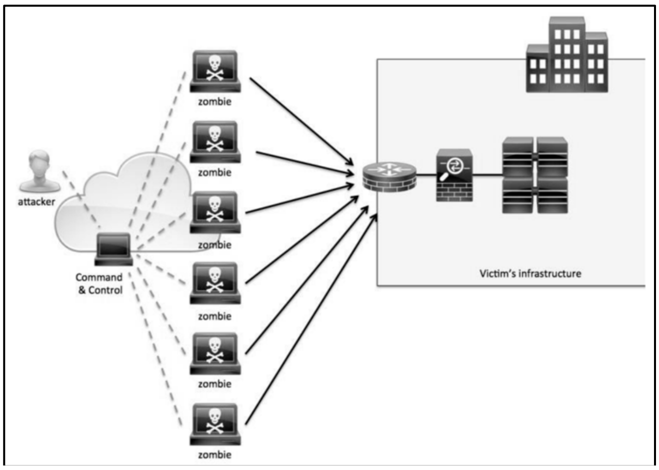

Fig.2: DoS Attacks in biometric systems

D. *Masquerade Attack*

In a Masquerade attack, a fingerprint template could be used to build a digital artefact image, and when this artefact is presented to the system, a match will result. The item might not even resemble the original photograph. Remote authentication devices are significantly threatened by this assault. A hacker only needs access to the templates kept on a distant server since he doesn't even need to bother getting a legitimate biometric sample. It mostly serves to increase the existing face or iris biometric databases or to verify the security of biometric recognition systems. Synthetic photos can be easily distinguished from actual photographs since an existing state-of-the-art method tends to overlook the perceptual quality of synthetic biometric images used in the attack. There is a new target combining semantic invariability

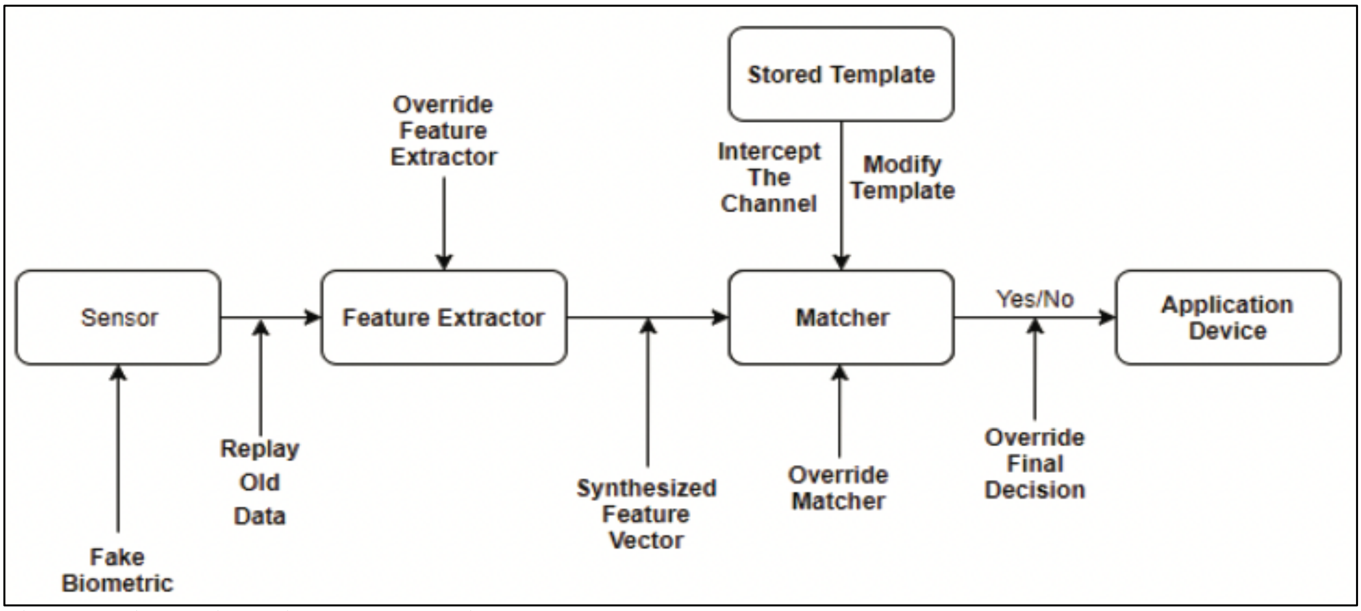

Fig.3: Attacks on Biometric Systems at each stage

in hashing space and perceptual similarity in biometric space in order to produce a high-perceptual-quality image that can simultaneously pass the validation of the recognition system.

E. *Sensor Output Interception*

The data output from the sensor may be modified or intercepted by an attacker. At enrollment, an acquired biometric sample might be replaced with biometric information from a different person or a previously captured sample could be replayed. An attacker could utilize intercepted data to gather an enrolled person's biometric details for use in subsequent attacks. To prevent sensor output interception, built-in security capabilities supporting secure biometric data collection and processing on mobile devices can be used.

F. *Reference and Database-related vulnerabilities*

A hacker may target data while it is being transmitted or while it is being stored by the biometric system. For instance, an impostor's biometric characteristics could be added to a biometric reference in the enrollment database. A hacker in possession of a device, such as a mobile phone, passport, or ID card, in implementations where the biometric data is stored, would have unrestricted access to the data unless it is secured by built-in security mechanisms. Holding biometric data centrally and ensuring its secure transmission and storage is one way to protect it on the sensor including fake face masks, silicon fingerprints that aren't real, iris lenses, and others.

LIMITATIONS

While biometric systems are becoming more effective as technology advances, they are not fool-proof methods of authentication or identification. Mentioned below are a few of the limitations an individual can face while enrolling or after enrolling into a biometric system. It has been divided into three parts: Failure to enrol, FAR and cannot cancel.

A. *Failure to enrol*

When a template for biometric data cannot be correctly constructed, failure to enrol happens. A person may not be able to enrol in the system due to a physical or medical problem, low-quality reference information, for instance, as a result of sensors or poor ambient circumstances, such as lighting or any number of other reasons [7]. The efficient operation of a biometric verification or authentication system depends on effective enrollment rates. Technical problems, physical or physiological ailments, as well as cultural or religious restrictions, may prevent a group or individual from using or enrolling in a biometric system. For instance, some cultures or faiths may view the gathering of a facial image or other kinds of physiological information as undesirable.

B. *High False Acceptance Rate*

Two basic mistakes can be made by biometric systems. In contrast to a false negative, which occurs when the system is unable to discover a match between an input and a matching template, a false positive occurs when the system wrongly matches an input to a non-matching template. Such mistakes in a biometric system could occur for a variety of reasons. Various people may have comparable biometric traits, for instance, it can be challenging to tell identical twins apart using facial biometrics, or user engagement with a sensor varies between the enrolment and recognition stages (for example, a person may pose differently) Between the enrollment and recognition stages, a person's biometric characteristics may alter as a result of additional circumstances including ageing, trauma, or medical conditions. A probabilistic calculation is used to match a person with a template that is stored in a biometric system. The ethnic or age features of the sample data used to train the system, as well as the lighting conditions and body posture of the person at the moment of enrollment or later identification, can all affect the margins of error[8]. Any biometric implementation must focus on lowering the rates of false

Serial No.	Attacks	Examples	Typical Defences	Cost of Implementing Defence Systems
1	**Client Attack**	False Match	Large entropy; limited attempts	High
2	**Host Attack**	Template Theft	Capture device authentication	Low
3	**Eves-dropping, theft and copying**	Copying (spoofing) biometric	Copy-detection at the capture device and capture device authentication	Medium
4	**Replay**	Replay stolen biometric template response	Copy-detection at capture device and capture device authentication via challenge-response protocol	Medium
5	**Trojan Horse**	Installation of rogue client or capture device	Authentication of client or capture device; client or capture device within trusted security perimeter	Low
6	**Denial of service (DoS)**	Locked by multiple failed authentications	Multi-factor with token	High
7	**Masquerade Attacks**	Fingerprint template could be used to build a digital "artefact" image	AI-based Intrusion Detection System (IDS); 2FA	High

Table 1: Attacks on Biometric systems and their defences

positives and false negatives. In the graph below EER refers to an Equal error rate. We utilize scores to quantify how closely a pattern resembles a biometric template. The resemblance between them increases as the score rises. Therefore, a person is only allowed access to the system if their score for identification against a trained person or for verification against a person is higher than a certain level.

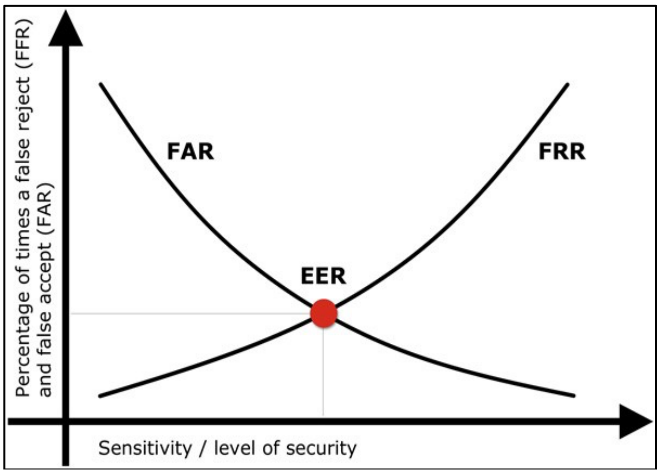

Fig.4: Percentage of times FAR occurs vs FRR occurs

C. Biometrics cannot be reused or cancelled

The inability to reissue or cancel biometric characteristics, in contrast to passwords or ID tokens, is another drawback of biometric systems. It can be exceedingly difficult, if not impossible, to replace a person's fingerprint or other physiological biometric if that feature has been compromised. This can be a concern if that biometric trait is later used for authentication.

PRIVACY ISSUES

Like much other technology, biometrics can provide problems for privacy. It is important to highlight those biometrics are not intrinsically incompatible with privacy.

A. Function Creep

When data is utilized for purposes other than those for which it was originally acquired, this is known as function creep. While the secondary use is not disclosed to the individual when they are giving their information, this becomes a problem. For authentication purposes, such as allowing entrance to a building, an organization might, for instance, gather a worker's facial biometric data [9]. Then, this information may be used for a separate secondary objective, such as keeping track of the employee's start and end timings.

B. Consent

The secret or passive gathering of people's biometric data without their knowledge, participation, or agreement poses another privacy danger. For instance, latent fingerprints can be lifted to gather biometric data long after a person has made contact with a hard surface, and facial biometric data can be obtained from images that people are unaware are being shot.

COMPROMISED BIOMETRIC SENSORS

The major issue is the validity of biometric authentication: For remote and unsupervised users on their mobile phones, there is always this risk of device compromise**.** Particularly susceptible to camera pipeline hijacking are browser-based biometric security techniques. This is so because the real camera cannot be accessed by the operating system. Free virtual camera software enables users to add images to the program whose real source is completely undetectable by the program. In these situations, the digital service provider can’t know with certainty how or when the data that reaches its servers was recorded. This implies that images from a successful claim could be captured and stored. The application or network server connection will receive the image or video at the appropriate time, completely excluding the camera. Replay attacks like this one would get through any PAD security. Replay attacks are qualitatively identical to videos of real biometrics.

Similar to this, malware on the device may record images taken by the camera during a successful authentication claim and play them back programmatically later. Cybercriminals find this strategy to be very alluring because it is simple to scale. The scale-up of the exploit to thousands of users can be done at a low incremental cost after it has been proven to work.

There are many established biometric technologies. The accuracy of biometric technologies such as fingerprinting and facial recognition has improved throughout the years due to technological advancements. The accuracy of fingerprinting is greater than 98%, according to research by the National Institute of Standards and Technology [11].

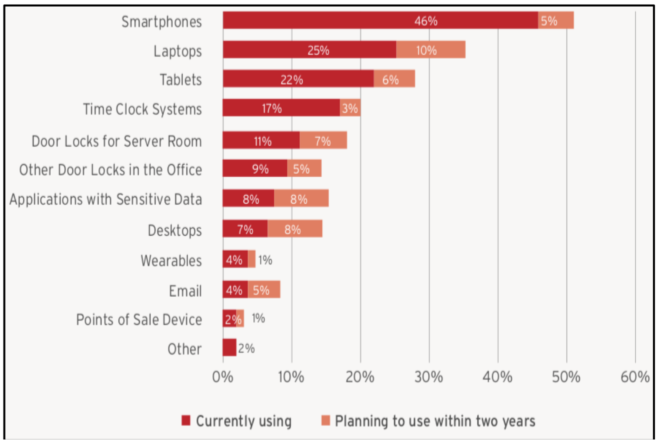

Fig.5: Percentage of times biometrics is used vs will be used in 2 years

However, it appears that the COVID-19 pandemic has now created an increasing demand for biometric authentication technology. We've already discussed how one of the biggest barriers to the adoption of biometric authentication technology is the misconception surrounding the security of the technology. The figure above shows how biometric technologies will be used more in various devices in the coming 2 years.

IV. Solutions to Biometric Attacks

The protection of biometrics data in both local and cloud storage has been advocated using a variety of strategies. We examine a multi-modal biometric strategy, liveness detection, and biometric template encryption strategies.

A. *Liveness Detection Test and Anti-Spoofing Device*

Biometric Authentication Systems are susceptible to spoofing attacks. An anti-spoofing gadget that detects pulses from genuine human fingers can be used to assess the liveness of a finger for a biometric authentication system based on the fingerprint. It is a cheap, easy-to-implement method that can be used to increase the security of fingerprint scanners and stop spoof attacks using fake or gummy fingers.

By distinguishing between real and fake fingerprints based on the number of pores, it is possible to determine the liveness of a fingerprint[13]. When compared to a phoney fingerprint, an actual fingerprint has more pores. As a result, for the liveness of fingerprints to determine if the fingerprint is coming from an actual finger or a finger produced from a spoofing material like silicone, clay, etc., detecting sweat pore patterns along the ridges should be quantified.

B. *Multimodal Biometrics*

To use multiple biometric modalities in a single identification system, multimodal biometrics must be used. This approach can be used when dealing with extremely sensitive data. An increase in recognition accuracy is achieved by combining various modalities. Additionally, the system's security is increased because it is highly challenging to fabricate several biometric features. Multiple biometric qualities are randomly requested from users by multimodal biometric systems, ensuring strong liveness detection to ward off spoofing or hackers.

A multimodal biometric system is ubiquitous in that it can still be used for authentication even if a person is unable to supply one form of biometric data due to a disability or disease.

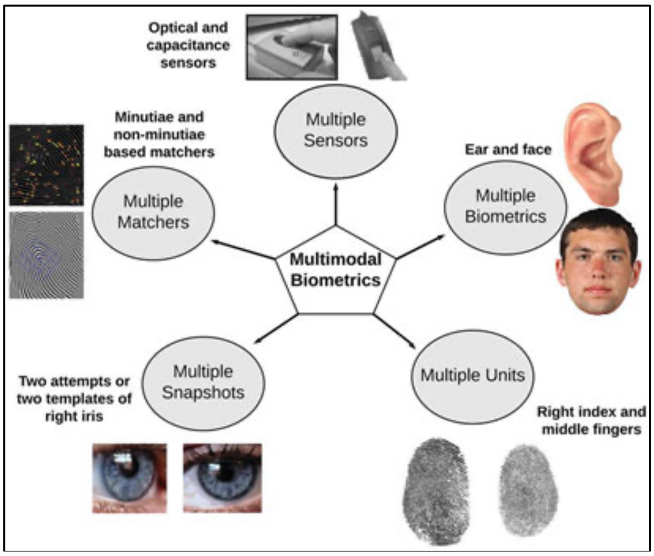
Optical and capacitance sensors
Multiple Sensors
Minutiae and non-minutiae based matchers
Multiple Matchers
Ear and face
Multiple Biometrics
Multimodal Biometrics
Two attempts or two templates of right iris
Multiple Snapshots
Multiple Units
Right index and middle fingers

Fig.6: Multimodal Biometric Categories

The typical fingerprint identification system has several problems, including dry or damp fingers, dust particles, etc. that distort the image that is being taken. Using a digital camera to take pictures of fingerprints was the solution to these problems. Pre-processing, Feature Extraction, and Matching are the three core modules of this system.

C. *Using an algorithm with increased security*

Elliptical Curve Cryptography uses only 224–255 bits, whereas the RSA approach needs a key size of 2048 to reach a security level of 112. A strong algorithm created today may be easily broken in the future due to the increase in computer processing power. Algorithm selection and updating are therefore essential.

D. *Eliminate Hill Climbing and Replay Attacks*

Using a challenge-response mechanism ensures that the image is coming from the fingerprint sensor and that the attacker has not circumvented it: After the client starts the transaction, the server creates a pseudo-random challenge. The intelligent sensor receives the challenge from a secure server. The sensor gathers the fingerprint image and calculates the challenge response. The problem could be a group of samples from the image, the checksum of a particular image segment, etc. The server receives both the answer and the perceived image. A validity check is done on the response/image pair. In a hill-climbing attack, the attacker essentially uses an iterative optimization method, where the fitness function is defined by the similarity score between the modified version of the original biometric's current estimate and the stored template. Only a rough quantized version, not the exact matching scores, is revealed. This might make the attack based on ascending hills impractical or impossible.

E. *Security measures used while storing biometric data in the database*

The biometric data stored in the database must be secured such that even if a hacker has access to it, they will not be able to use it to reproduce the original biometric pattern to gain access to the system. The security of the system can be increased for fingerprint-based identification systems by storing a virtual composite biometric template in the database that combines features from two separate fingerprints. A combined template created utilizing the orientation values and minute points from two separate fingerprint patterns is the virtual biometric pattern[15]. Even if the hacker gains access to the virtual biometric kept in the database, he or she won't be able to recreate the original fingerprint patterns.

F. *Watermarking Techniques*

The term digital watermark refers to the data that will be included in a signal, while in some circumstances it also refers to the distinction between the watermarked signal and the cover signal. The host signal is the one into which the watermark is to be inserted. Embedding, attack, and detection are the three distinct phases of a watermarking system. An algorithm creates a watermarked signal by accepting the host and the data to be incorporated. The watermarked digital signal is then sent or stored, usually to a different recipient. An alteration made by this person is referred to as an assault. The term attack comes from copyright protection applications where third parties may try to remove the digital watermark through modification, even though the modification may not be malevolent.

V. Results

It is preferable to have a multimodal system and to carry out liveness detection tests to make the system secure if biometric authentication is being utilized to guard extremely important information. Because the fingerprint scanner doesn't always interpret inputs accurately, there is a potential for false rejections in a Unimodal System if the fingerprint is the modality being considered. A Multimodal System, however, gets around the majority of the drawbacks of a Unimodal System. For instance, it is preferable to have Multimodal systems, use a strong encryption method to keep samples in the database and execute a liveness detection test to make the system secure while employing biometrics in the retail business for payments. However, a unimodal system with many samples kept in the database is sufficient if biometric authentication is being utilized to safeguard a digital device.

VI. Conclusion

Systems using biometric authentication are superior to those using a PIN or password. They successfully shorten the time it takes to accurately identify and authenticate a person. These systems do, however, have several security vulnerabilities that need to be resolved. The environment in which biometric authentication systems are used, the financial resources at hand, and the viability of deploying hardware, applications, etc., all affect how accurate they are. Different systems will therefore have different options for increased security depending on these considerations. The electronic financial transaction model uses biometrics and an encrypted one-time password, making it more secure than the PIN/password-based mechanism now employed in electronic data capture (EDC) machines.

VII. References

[1] Kour, Jaspreet, M. Hanmandlu, and A. Q. Ansari. "Biometrics in Cyber Security." *Defence Science Journal* 66.6 (2016).

[2] Alanezi, Nuha A., et al. "POSTER: a brief overview of biometrics in cybersecurity: a comparative analysis." *2020 First International*

[3] *Conference of Smart Systems and Emerging Technologies (SMARTTECH)*. IEEE, 2020.

[4] Jain, Anil K., Arun Ross, and Sharath Pankanti. "Biometrics: a tool for information security." *IEEE transactions on information forensics and security* 1.2 (2006): 125-143.

[5] Alzahrani, Bayan, and Fahad Alsolami. "Biometric System: Security Challenges and Solutions." *16th International Conference on Information Technology-New Generations (ITNG 2019)*. Springer, Cham, 2019.

[6] Bhartiya, Namrata, Namrata Jangid, and Sheetal Jannu. "Biometric authentication systems: security concerns and solutions." *2018 3rd international conference for convergence in technology (I2CT)*. IEEE, 2018.

[7] Kaur, Harshdeep. "Literature Review on Security Issues and Limitations in Biometric Applications." (2020).

[8] Jain, Anil K., Arun Ross, and Umut Uludag. "Biometric template security: Challenges and solutions." *2005 13th European signal processing conference*. IEEE, 2005.

[9] Narayanan, Aparna, and Gunjan Chhabra. "Reducing cyber threats: Via a multimodal biometric system." *International Journal of Artificial Intelligence and Neural Networks–IJAINN* 3 (2013): 10-14.

[10] Pujari, Mr Vinayak, Rajendra Patil, and Mr Shailesh Sutar. "Research paper on biometrics security." *Contemporary Research in India* (2021).

[11] Alguliyev, Rasim, Yadigar Imamverdiyev, and Lyudmila Sukhostat. "Cyber-physical systems and their security issues." *Computers in Industry* 100 (2018): 212-223.

[12] Gomez-Barrero, Marta, et al. "Biometrics in the era of COVID-19: challenges and opportunities." *IEEE Transactions on Technology and Society* (2022).

[13] Bhattasali, Tapalina, et al. "A survey of security and privacy issues for biometrics based remote authentication in the cloud." *IFIP International Conference on Computer Information Systems and Industrial Management*. Springer, Berlin, Heidelberg, 2015.

[14] Arora, Shefali, and M. P. S. Bhatia. "Challenges and opportunities in biometric security: A survey." *Information Security Journal: A Global Perspective* 31.1 (2022): 28-48.

[15] Yadav, Garima. "Application of Biometrics in Secure Bank Transactions." *International Journal of Scientific and Technology Research* 7 (2013): 124-127.