International Journal on Advances in Engineering Technology and Science
Volume: 5, Issue: 1, 2024, e-ISSN: 2455-3131
DOI: 10.5281/zenodo.10641797

Security Features in Fingerprint Biometric System

Shilpa, Kirti Jain

School of Advanced Computing, Sanjeev Agrawal Global Educational University, Bhopal

shilpajaiswar10@gmail.com
kirti.j@sageuniversity.edu.in

Abstract– **At present, embedded systems operate in every environment on the planet. Many complex applications with previously unheard-of capability have been made possible by recent technological advancements. Regardless of the ability to shield critical data from malevolent attacks, security and privacy remained a prevalent concern for these systems. These worries are warranted since horrifying tales about embedded systems are told by the past security lapses and their aftermath. With the development of technology, the attacks are gradually changing and becoming more sophisticated. As a result, fresh approaches to security implementation in embedded systems are needed. This paper uses a case study to illustrate how security features are integrated into fingerprint biometric systems during the requirements analysis stage and maintained throughout the embedded system life cycle. A comparative analysis is provided between different biometric technologies, including face, fingerprint, iris, palm print, hand geometry, gait, signature, and keystroke. In order to provide more precise safety requirements or functions, the goal of this work is to analyze, break down, and convert the risks and countermeasures found during the requirements analysis utilizing the abuse case. Additionally, by examining the system requirements and outlining the primary procedures for biometric system protection in this article, we have demonstrated how security features can be incorporated into the biometric fingerprint system.**

Keywords– Information leaks, fingerprints, abuse cases, countermeasures, and threats.

I. INTRODUCTİON

An automated biometric system authenticates an individual's identity based on a prior enrollment event by using human traits such as physiology, behavior, and biological traits. The explanation

These attributes, which include universality, uniqueness, permanence, and collectability, are what make them perfect for human identification [1]. The following is a description of these four attributes:

1. Universality: Every individual shares the same traits as a typical human being.

2. Individuality - Each person possesses a distinct quality. In other words, no two people have the same trait.

3. Permanence: This trait is independent of time. It remains constant over time.

4. Collectability - The attribute is readily obtainable and measurable in a quantitative manner.

Research on biometrics and its appropriate applications has been conducted in an outstanding and continuous manner. These are applicable to the situation at hand. Voice, face, retinal scan, iris, ear, hand & finger geometry, image, DNA, infrared facial thermography, and fingerprints are a few of the common biometrics utilized today. developments in technology have now caused this domain to grow enormously.

Biometric identification [2] refers to the process of identifying a person based on physiological and behavioral traits like face, fingerprint, hand shape, iris, keystroke, signature, voice, etc. Because biometric features cannot be missed or ignored, unlike passwords that can be lost or forgotten, it is more secure than password-based authentication. As opposed to passwords being made public on hacker websites, copying, sharing, and distribution are very challenging. Moreover, the individual who is authenticated must be present at the time and place of authentication, unlike deceitful users who deny that the password has been swapped. It's difficult to forge biometrics, and it's unlikely that a consumer will deny having their biometrics used to access digital content.

Every user eventually has a comparatively comparable level of safety since biometrics cannot be cracked faster by some than by others. As a result, few users are able to compromise biometrics that are "easy to guess". Consequently, biometric authentication will take the place of password authentication using either the complete authentication technique or the conventional

digital rights management (DRM) system cryptographic keys that protect the multimedia file [3].

In the meanwhile, technical developments have encouraged the sophistication of security assaults as well as the development of fancy functional features. Such security flaws in hardware-software systems have been documented frequently throughout history, and they appear to change over time. More specifically, in Any attacker might use a brute-force attack or just provide the system with a duplicate of a known person's biometric when employing biometrics with fingerprint authentication [4].

Biometric data is distinct since it provides a perfect means of simple authentication that may either supplement or replace passwords. The damage caused by biometric data being lost to malevolent parties, however, cannot be undone. This is so because they uphold our sense of self, making us a part of something greater than ourselves. While stolen biometric information, like fingerprints, cannot be altered or deleted, stolen passwords can be quickly updated or modified [5]. Therefore, the security issues with fingerprint-based biometric identification will be addressed by this research. This research aims to tackle the issue of side-channel information leakage in fingerprint biometric systems.

The biometric system in this work is provided in Section 2 and compares several physical features in terms of universality, uniqueness, permanence, and collectability. Section 3 of the document highlights the security characteristics of Fingerprint Biometrics, while Section 4 presents the needs analysis based on the risk associated with each component of the biometric system, including direct and indirect attacks. Furthermore, the functional analysis, threat assessment, countermeasure allocation, and physical component design synthesis of the biometrics system were illustrated in section 5 through the results and comments. Section 6 then serves as the final section of this study.

II. BİOMETRİC SYSTEM

A range of biometric technologies have been employed for diverse purposes. Each biometric has advantages and disadvantages depending on how it is used. No biometric system can adequately satisfy the requirements (e.g., cost, practicality, accuracy) of every application (e.g., welfare distribution, DRM, access control, etc.). Put another, there isn't a one "optimal" biometric. Body characteristics such as face, fingerprint, iris, palm print, hand geometry, and ear shape, as well as gait, signature, and keystroke, can be utilized for biometric identification [6].

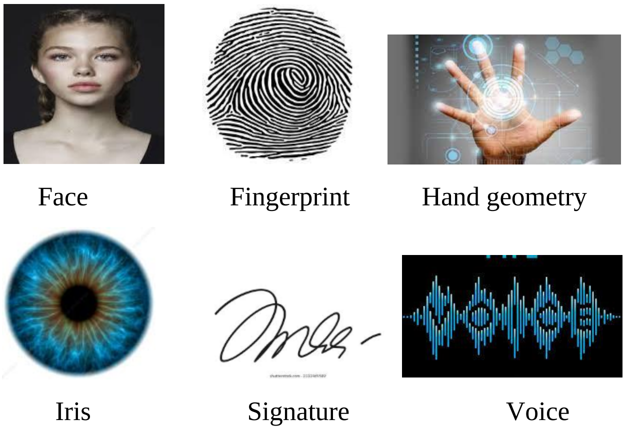

Fig. 1 – Different biometric methods

Table 1 presents a categorised comparison of several biometric methods. H, M, and L stand for High, Medium, and Low, respectively. The characteristics of the biometric feature and the needs of the application decide if a particular biometric and an application match.

Table 1 – Comparison of different biometric methods

Biometric Identifier	**Universality**	**Uniqueness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**
Face	H	L	M	H	H	H
Fingerprint	M	H	H	M	M	M
Hand Geometry	M	M	M	H	M	M
Iris	H	H	H	M	L	L
Signature	L	L	L	H	H	H
Voice	M	L	L	M	H	H

Based on particular physiological and behavioral traits, biometric systems identify a person using the pattern-recognition technique. Verification and recognition are the two ways that biometric systems operate. In contrast to the latter, which searches the entire database for a perfect match, the former compares the biometric feature that was taken with the biometric template that was already saved in the database. Block diagram for identifying and validating user data for enrolling is shown in Fig. 2.

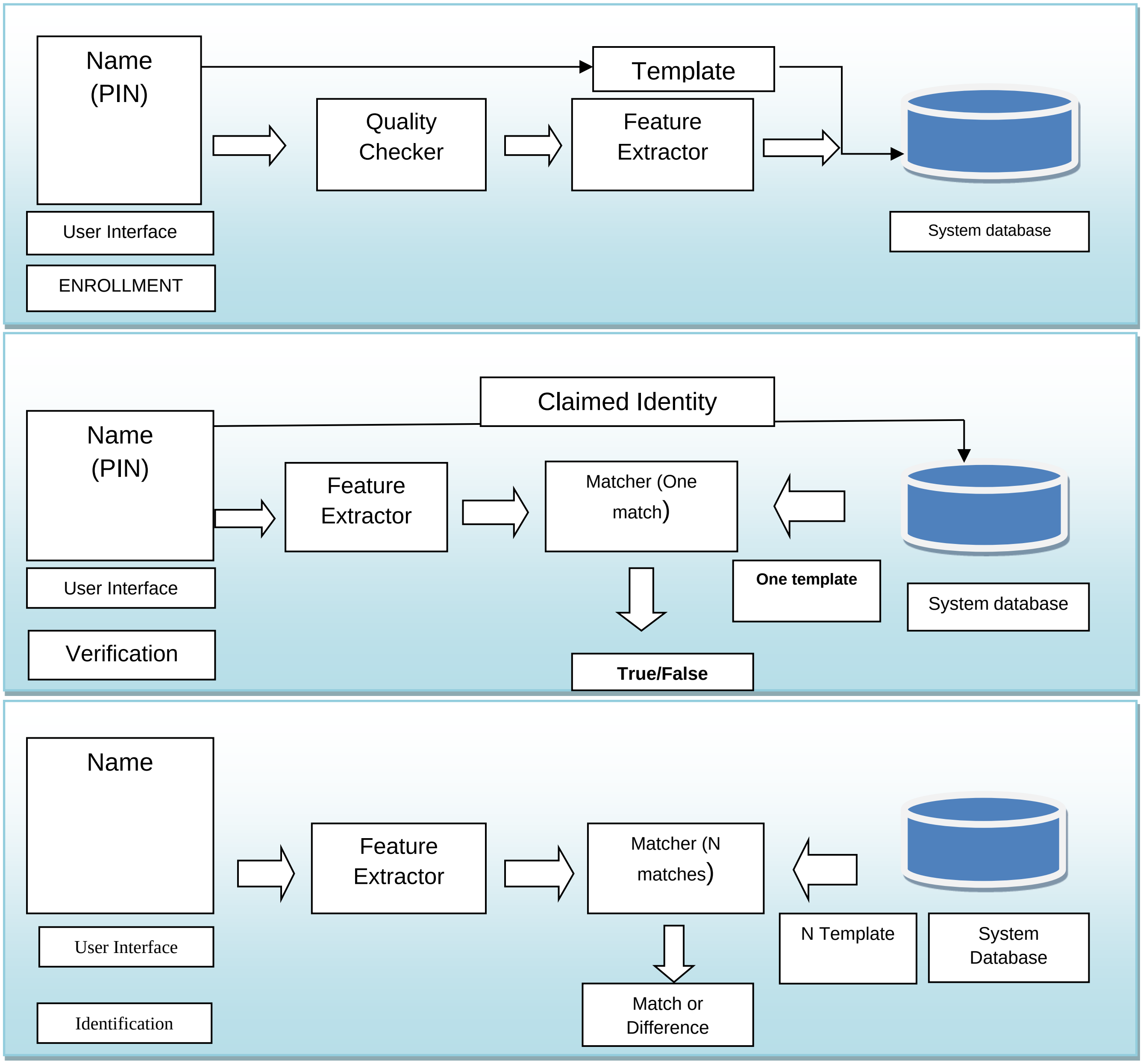

Fig. 2 - Enrolment, Verification, and Identification Task Block Diagram

When a consumer enrols, the fingerprint image is captured from the sensor panel when they place their finger on the sensor. To generate prototype data for comparison during verification, some features of the obtained fingerprint image are taken out and altered or converted. The sensor module gathers the fingerprint image of an application during verification. The enrollment level and the functional representations of the database fingerprint image go through the identical steps to obtain query data. Next, the test data are examined to see if the outcomes match those of the template data. (8).

III. FİNGERPRİNT BİOMETRİC SECURİTY FEATURES

This work aims to integrate the security design elements of a biometrics fingerprint authentication system from its early stages of development through the design phase, using a case study as support. The "Fingerprint Biometric Authentication System for Students Electronic Examination" is the system that [9] proposed and is the foundation of this work. This study will just look at the fingerprint portion of the system**.**

There are significant privacy concerns with biometrics, some of which include the following biometrics key issues: Every data collection is susceptible to hacking at some point. Hackers may find particularly appealing data that is well-known. The good news is that sensitive information is safer. However, as biometrics are becoming more widely used, they might be accessible in other places where the same safe storage standard isn't followed.

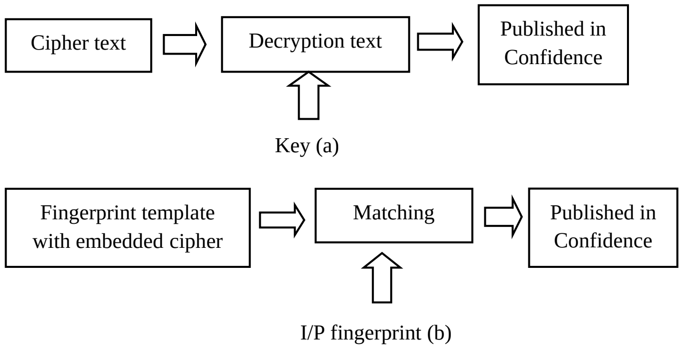

Fig. 3 - A general representation of basic conventional and biometric DRM systems with password- and fingerprint-based authentication, respectively [10]

IV. EVALUATİON OF REQUİREMENTS:

At this point, the requirements for putting the fingerprint biometric system's security into practice will be examined in light of the risks connected to each component. The aim is to detect potential system threats and thereafter develop appropriate countermeasures. As illustrated in Fig. 4, potential security breaches involving fingerprint biometrics may arise at specific points throughout the system, according to [11].

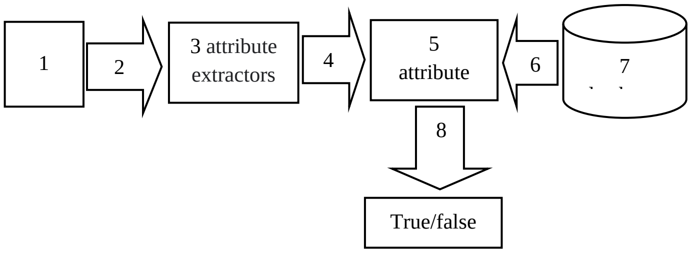

Fig. 4 – Potential assaults against fingerprint biometrics are depicted in [11]

Although they are more secure than conventional methods, biometric technologies nevertheless have significant drawbacks [12]. As seen in Fig. 5, there

are eight threat spots in the biometric approach that can be targeted. These attack sites fall into two groups: direct threats and indirect threats.

Persistent Danger (Direct Threat):

Threats like matching algorithms and vector format functions are examples of those that don't require specialized understanding of the system function. The "Sensor Threat," or Risk 1, is the only one present.

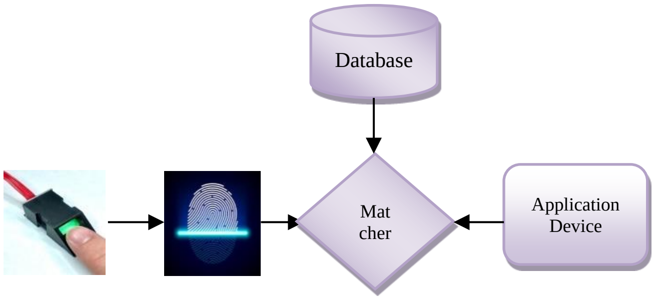

Fig. 5 - Biometric system threat points [13]

The first danger, referred to as the "Threat to the sensor," poses a vulnerability to the sensor module. A phony biometric feature, such as a fake finger or face image, is presented to the sensor in this threat in order to evade detection systems [14]. The system could sustain physical harm from an imposter and get overloaded with bogus queries. Since no specific understanding of how the gadget operates is required, attacking the sensor is quite easy. When digital security techniques like watermarking are unavailable, sensor-level cryptography is employed. A person's facial image and phony fingerprints can readily mislead the sensors, which are unable to distinguish between actual and fake people.

Asymmetrical assaults (Indirect attacks):

Risk 1: Unlike direct attacks, these attacks need knowledge of the internal workings of the authentication mechanism. It encompasses all seven additional threat points (2, 3, 4, 5, 6, 7, 8) in the biometric authentication system that could be targeted by a fraudster.

Risk 2: Upon acquiring unprocessed biometric data, a sensor transmits said data to the feature extractor module over a communication channel for preliminary processing. The sensor and the extractor feature are separated by the channel. An intercept and storage of the biometric feature occurs. The function extractor takes the place of the previously stored biometric feature in order to avoid the sensor. A "replay threat" is what is meant by this [14].

Risk 3: The extractor module is susceptible to the "Threat to the extractor module features" peril 3. Once the sensor has collected raw biometric data, it sends the data to an extractor module. Instead of producing values retrieved from the original sensor data, the imposter's feature extractor module is under pressure to produce the function values chosen by the intruder.

Risk 4: This is similar to Threat 2 in that a fraudster eavesdrops on the function extractor and match modules' communication channel in order to obtain the feature values of a genuine user [14]. The title is "Threat to the channel between the extractor and the play".

Risk 5: Known as the "Threat to the Matcher Module," a matcher module can be exposed to this danger [15]. No matter what value is entered, the imposter will generate a high matching score to get around the biometric authentication mechanism.

Risk 6: The impostor takes advantage of database secrecy by erasing old templates, creating new ones, and changing existing ones [15]. Attacking system databases using techniques like watermarking and other digital methods is not a simple undertaking. Successful attacks on the system database must require a certain level of understanding of the underlying operations of the system.

Risk 7: The prototype can only be transmitted through a channel interaction between the match module and the device database. This occurs when the importer tampers or alters the communicated template's content.

In order to steal, replace, or change the biometric template, a fraudster intercepts the canal. "Attack on the communication channel between device and match database" is how it is called.

Risk 8: The outcome that the corresponding module states will be overridden by a fraudster. This attack has the ability to stop the match score from being sent via the communication channel between the application device and the matching module. The match score is altered in order to reverse the module's initial acceptance/rejection decision. It is discovered that adversaries most frequently target models that are present in the database after looking through these eight attack sites. One can modify the templates present in the database by either adding new templates, making changes to the ones that already exist, or completely removing the templates from the database [16].

Instances of Use and Misuse:

Use cases are a great tool for determining what users and other stakeholders actually need. According on the use case, one or two users interact with the software to do a task. A structured collection of use cases representing device interface details from the viewpoints of the various user classes make up the use case analysis of the program's technical specifications. Any use case typically depicts the manner in which a single user will interact with the software. A use case comprises a case diagram together with a sample definition for every possible scenario. In most case descriptions, one or two alternative scenarios are included in addition to the normal scenario.

Misuse cases are a reflection of threats: the various ways that an intruder interacts with the system to go around, break, damage, take advantage of, or abuse the program. When an agent who is opposed to the program being designed uses it, it is considered misuse [17]. The goal of a misuse is to interfere with the consumer situation's system functioning, which is a hostile agent, rather than to supply system functionality. Furthermore, inadvertent or inadvertent software errors and omissions are frequently included in abuse instances.

An overview of the properties to be covered, along with risk management and risk analysis, usually precedes the determination of protection requirements. This omission is specifically addressed by misuse case-based hazard recognition. We propose the following approach to incorporate security requirements and hazards into use cases and abuse scenarios:

1. Establish a strong framework and participant definitions first (representing customer classes).

2. Consider every use scenario and determine whether any negative actors try to undermine their goals or frustrate the procedures outlined in the use scenario definition; this aids in the most serious instances of misuse. The goal of the brainstorming sessions will be to identify the several ways that an attacker could compromise the service that the aim event provides. We can decide on the specifics of these attacks later. Determining security threats from a range of potential risks, including unauthorized internal and external access, denial-of-service attacks, privacy violations, confidentiality and reputation breaches, and hackers, is the goal of defining security threats against each feature, location, procedure, data, and transaction in the use case. The approach will attempt to monitor both the device replies and possible user errors in addition to attack types. Such mistakes could also seriously impair the functionality or health of the system.

3. As in Fig. 6, show the connections between the usage cases and the pertinent instances of misuse. Using words like "threat" and "steal" to describe the relationships shown will be simpler.

4. Once misuse cases have been created, specify how protection cases will be used to counter or obstruct the intended outcome of the misuse case. Figure 7 illustrates the implementation of a novel security use case named "Encrypt the Message" in order to prevent the misuse of the "Tap Communication" scenario. Since the additional use cases don't correspond to the system's functional needs, they are referred to as "security use cases."

5. For every significant use case, repeat steps (2) through (4) until you are satisfied that: (a) all relevant risks to particular program functions and resources (as defined by the use case model) are listed and explained as instances of misuse; and (b) every threat has been neutralized by one or more recently introduced "security use cases." Microsoft's new threat analysis methodology provides some helpful guidelines for categorizing hazards in usage instances.

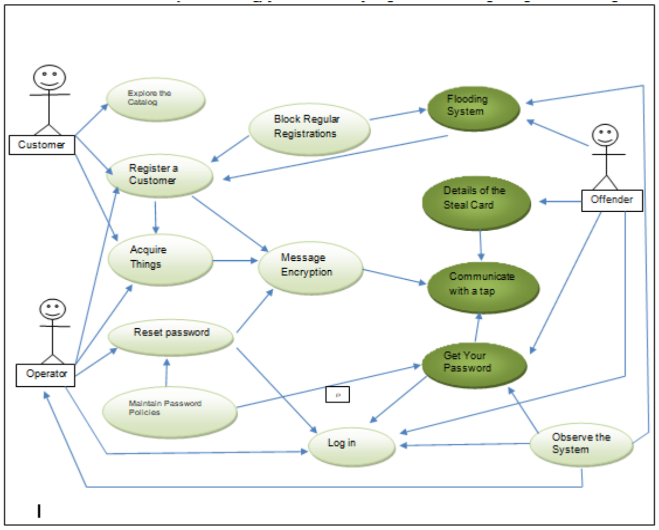

Fig. 7 - Flow Diagram for instances of usage and misuse

The main goal of security standards should be to identify the resources and services that need to be safeguarded as well as the dangers to public safety that these resources and services pose. Certain linkages between assets and services, as illustrated in Fig. 8, are susceptible to safety concerns and necessitate security requirements as well as protective measures in order to resolve and subsequently secure assets and services.

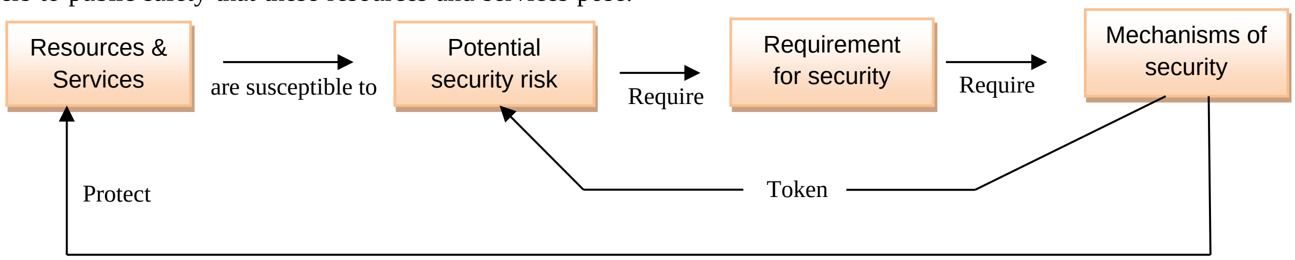

Fig. 8 - Security Risks, Needs, and Procedures

In order to secure sensitive assets and resources by addressing recognized security threats, security engineering has historically placed a strong emphasis on the development and use of diverse protection mechanisms. Significantly less attention was paid to the analysis and reporting of security risks and specifications. One relatively new method of tackling security threat assessments was creating cases of abuse. As seen in Fig. 9, misuse cases are particular situations that are examined and security threats are identified. Misuse cases focus on interactions between the program and those trying to circumvent its security, as opposed to standard use cases, which record interactions with an application and its users. Cases of misuse are extremely helpful in identifying security vulnerabilities because a successful assault on an application is the only condition for success. However, they are insufficient for the analysis and formulation of protection standards. Alternatively, security use cases can be used to specify requirements so that the software can successfully protect itself against the security dangers that are unique to it.

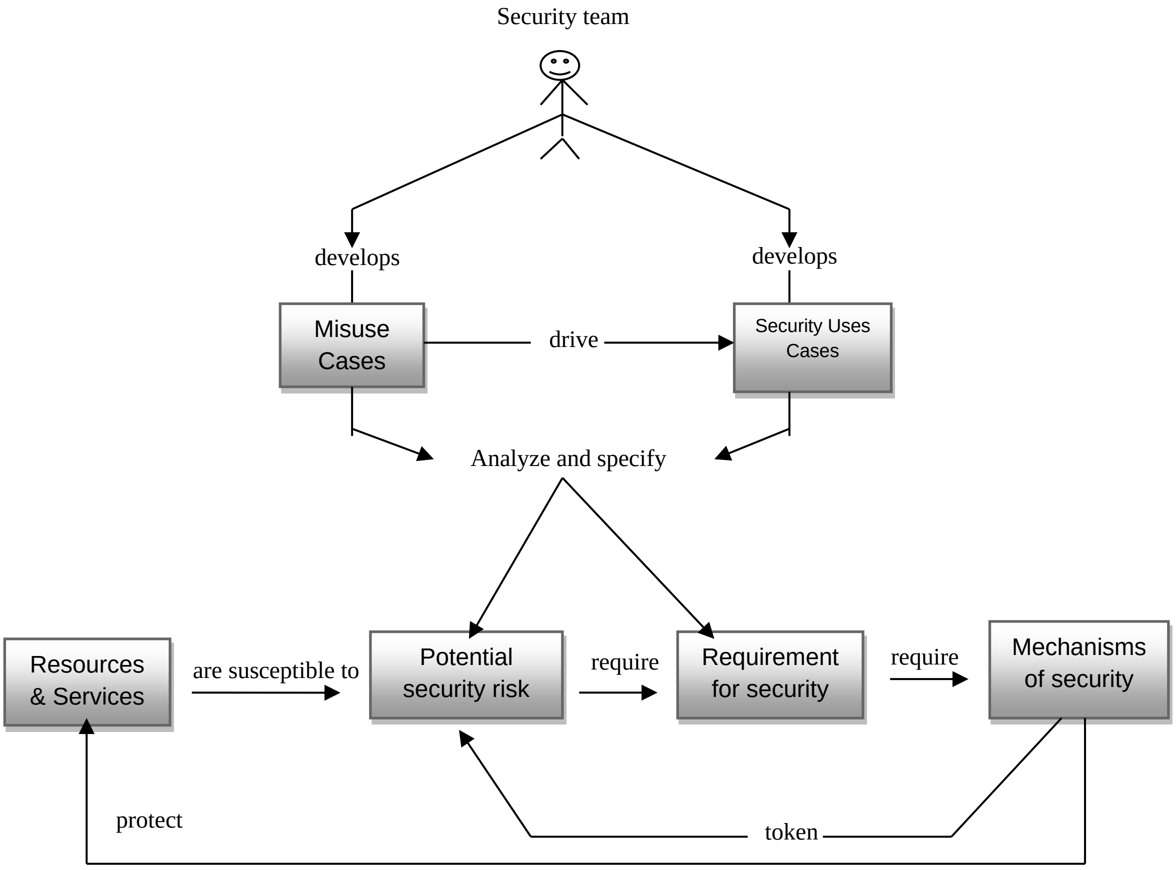

Fig. 9 - Security Use Cases and Misuse Cases

V. CONCLUSİONS AND TALKS

Analysis and Allocation Functionality

The purpose of this part is to break down and convert the threat and countermeasures found during requirements analysis utilizing misuse cases into more focused security needs or functionality. See [18–19] for further information on abuse cases and security use cases.

Figures 10 and 11 display the abuse cases that were created in response to the threat that was discovered and the countermeasures that were put in place. The security use cases that are required to stop the misuser's attacks are known as green use cases. The steps that a misuser could take to compromise the system, including injecting a pre-selected feature that was pilfered during transmission between the feature extractor and the comparison component, are referred to as abuse scenarios, or orange use cases.

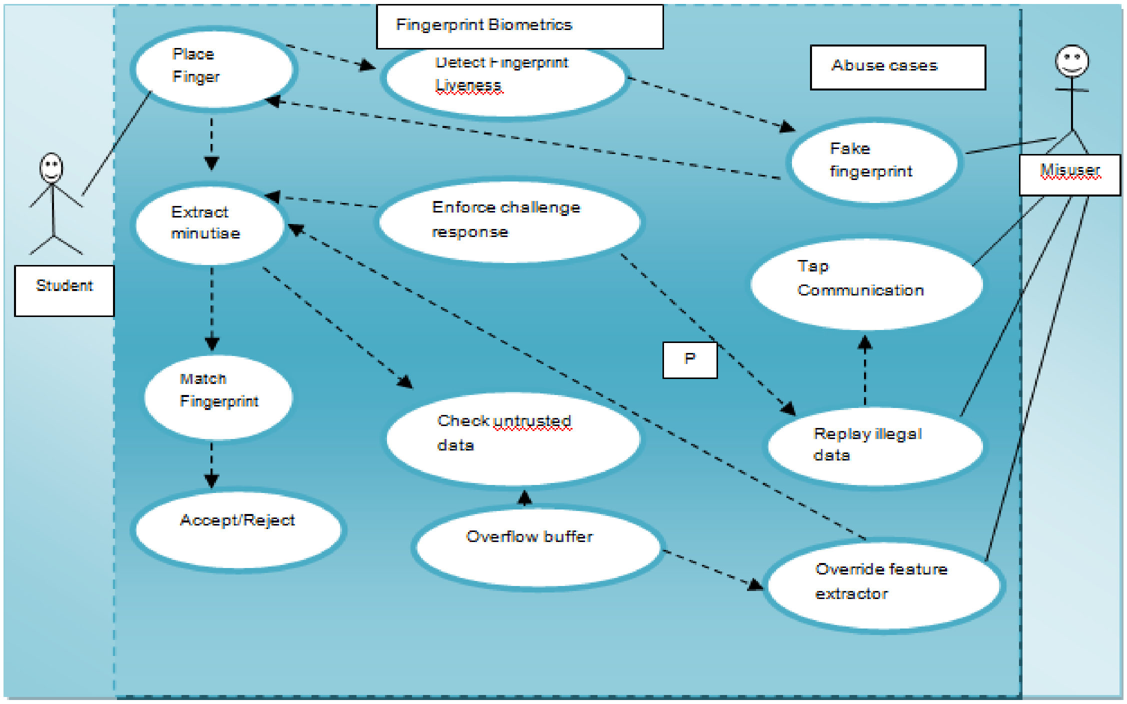

Fig. 10 - Security use cases and abuse situations (part 1)

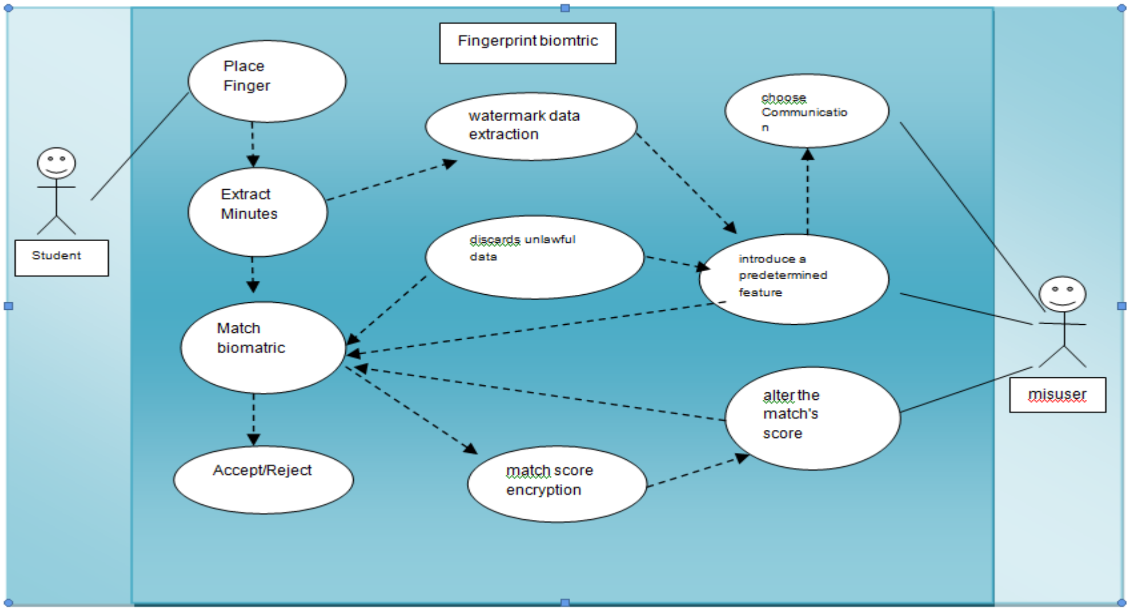

Fig. 11 - Abuse cases and security use cases (part 2)

Synthetic Design

This section provides an overview of the physical components that comprise the fingerprint biometric system, representing the system's abstract

Every component carries out the task assigned in the previous phase, each modeled with its own security aspect. As seen in Fig. 12, the components of the feature extraction and matching algorithm were used to model the physical components of the biometric system using component diagrams. Subsequently, the biometrics system's architecture was represented as the deployment diagram, as displayed in Fig. 13.

Three typical design stages—requirements analysis, functional analysis, and design synthesis—were used to demonstrate how the fingerprint biometric system's security characteristics were enhanced early in the system life cycle. The effectiveness of designing security and other functional and performance requirements for embedded systems at different stages of the system life cycle has been established. Iterative processes are typically involved in system development, and it's possible that this case study just represents the first iteration of the system life cycle process.

The concept of integrating security into the design process has been introduced through the fruitful research provided in this paper. Early on in the requirements analysis, the identification of potential threats and the implementation of suitable countermeasures might potentially steer the progress by improving system security and making the work of engineers and designers easier.

It can operate with the fingerprint of an image of low quality thanks to the correlation-based matching algorithm. Fingerprint image authentication is highly precise thanks to the host pictures' functionality analysis. The accuracy of a biometric device when selecting the correct choice is heavily impacted by fabricated and falsifiable errors. The challenge to scalability offers a question about the effect of the number of registered users making the proper selection. Safeguarding the biometric device against intrusions and maintaining user privacy is crucial.

Smartphones, tablets, and PCs now come equipped with fingerprint detecting features because biometric security measures like fingerprint authentication have shown to be safer and more practical than passwords. Biometric safeguards are the most effective way to address the security concerns associated with fingerprint authentication. To ensure security, there can be divided into three primary steps [20].

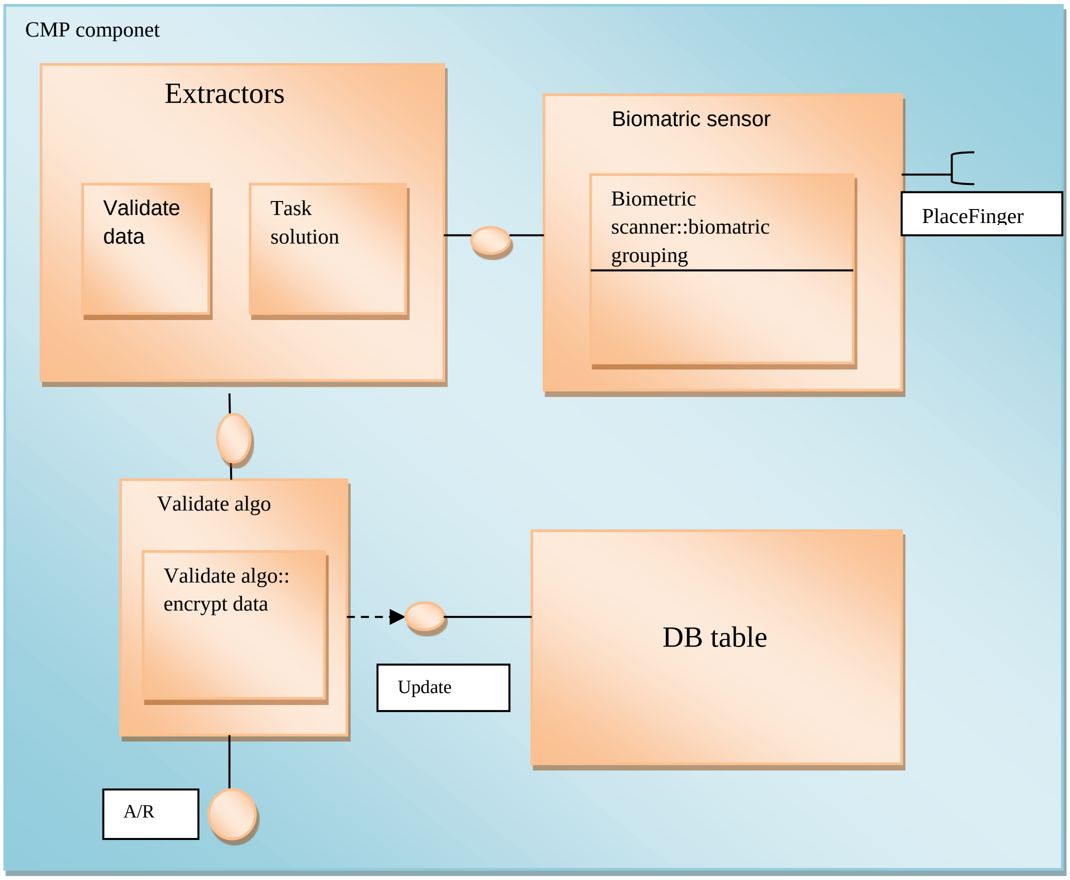

Fig. 12 - Fingerprint Biometric System Component Diagram

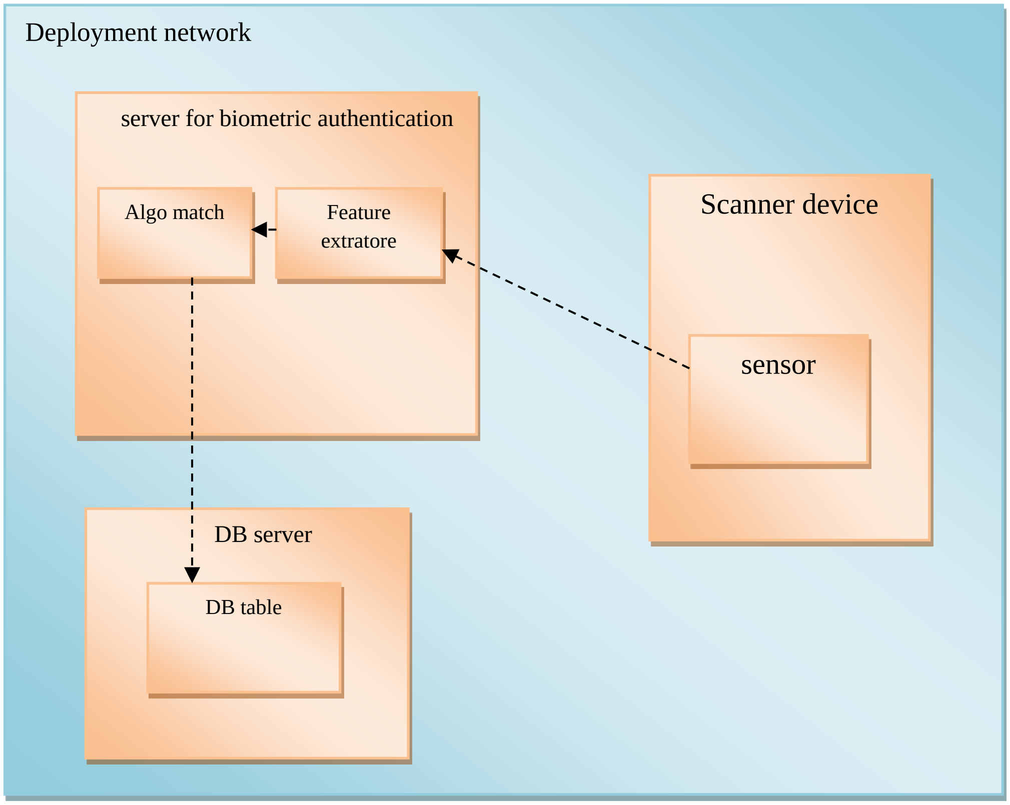

Fig. 13 - Deployment Diagram biometric system

Modification cryptography key management

Fig.14 - Three primary security procedures designed with biometrics in mind [20]

i. Modification:

The user is protected from identity theft by this one-way conversion of biometric data into a proprietary prototype format, which prevents recreation, reverse engineering, or unintentional usage.

ii. Cryptography:

To prevent fraud, abuse, and eavesdropping, every biometric piece of information is digitally signed and encrypted using the 256-bit Advanced Encryption Standard and Transport Layer Protection.

iii. Key Management:

One-time encryption keys generated by hardware ensure that biometric data stays entirely within the host's secure execution environment, where it is only accessible by programs that are referred to as trusted.

The problems with cyber security these days are enormous. As technology progressed as was inevitable, security sophistication increased as well. In the realm of embedded systems, security lapses are intolerable.

Embedded systems typically handle sensitive data or information due to their inherent nature.

As a result, it is vital to design security into embedded systems early in the development process or throughout the system life cycle. As a result, the biometric fingerprint system is thoroughly reviewed, and the various security characteristics of the software. Additionally, threat models featuring direct and indirect biometric system assaults have been employed to illustrate the security flaws in biometric frameworks. Next, by examining the system's requirements, we have highlighted the addition of security elements to fingerprint biometric systems and have offered the primary security measures for the biometric system. In conclusion, we have examined and modified the risks and defences. converted into more precise safety criteria or functionalities during the requirements analysis utilizing the misuse case. As a result, in this article, we have demonstrated how to incorporate security elements into the biometric fingerprint system by examining the system's needs and outlining the primary security measures.

REFERENCES

[1] Willins, B., Sharony, J. and Wang, H., Symbol Technologies LLC. (2006). Cryptographic architecture for secure, private biometric identification. U.S. Patent 6,990,587

[2] Umer, S., Dhara, B.C. and Chanda, B. (2017). A novel cancelable iris recognition system based on feature learning techniques. Information Sciences, 406, pp.102-118

[3] Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S. (2003). Fingerprint Matching. Handbook of Fingerprint Recognition, pp.131-171

[4] Castiglione, A., Choo, K.K.R., Nappi, M. and Narducci, F. (2017). Biometrics in the cloud: challenges and research opportunities. IEEE Cloud Computing, 4(4), pp.12-17

[5] B. Schneier, "Stealing Fingerprints," Schneier on Security, (2015). Available: https://www.schneier.com/blog/archives/2015/10/stealing_finger.html.

[6] Nandakumar, K. and Jain, A.K. (2015). Biometric template protection: Bridging the performance gap between theory and practice. IEEE Signal Processing Magazine, 32(5), pp.88-100.

[7] Kirti Jain, Pinaki Ghosh, Shital Gupta "A Hybrid Model for Sentiment Analysis Based on Movie Review Datasets" in international journal on recent and innovation trends in computing and communication, Scopus Indexed Journal ISSN: 2321-8169, Vol 11 No 5 (2023).

[8] Jin, Z., Teoh, A.B.J., Goi, B.M. and Tay, Y.H. (2016). Biometric cryptosystems: a new biometric key binding and its implementation for fingerprint minutiae-based representation. Pattern Recognition, 56, pp.50-62

[9] Yang, W., Wang, S., Hu, J., Zheng, G. and Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. Symmetry, 11(2), p.141

[10] Kirti Jain "A Transfer Learning Based Machine Learning Approach to Solve Problems of Ecommerce: Image Search" published in Proceedings of International Joint Conference on Advances in Computational Intelligence indexed on Springer Book series ISBN 978-981-99-1435-7, June 2023

[11] Schaumont, P., Hwang, D., Yang, S. and Verbauwhede, I. (2006). Multilevel design validation in a secure embedded system. IEEE Transactions on Computers, 55(11), pp.1380-1390

[12] Yang, W., Wang, S., Hu, J., Zheng, G. and Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. Symmetry, 11(2), p.141

[13] Kocher, P., Lee, R., McGraw, G. and Raghunathan, A. (2004), June. Security as a new dimension in embedded system design. In Proceedings of the 41st annual Design Automation Conference (pp. 753-760)

[14] Alaswad, A.O., Montaser, A.H. and Mohamad, F.E. (2014). Vulnerabilities of biometric authentication threats and counter measures. International Journal of Information & Computation Technology, 4(10), pp.947-58

[15] Jain, R. and Kant, C. (2015). Attacks on biometric systems: an overview. International Journal of Advances in Scientific Research, 1(07), pp.283-288

[16] Latha, M.U. and Rameshkumar, K. (2013). A study on attacks and security against fingerprint template database. International Journal of Emerging Trends Technology in Computer Science (IJETTCS), 2, p.37

[17] Mwema, J., Kimwele, M. and Kimani, S., (2015). A simple review of biometric template protection schemes usedin preventing adversary attacks on biometric fingerprint templates. International Journal of Computer Trends andTechnology, 20(1), pp.12-8

[18] Akhtar, Z. (2012). Security of multimodal biometric systems against spoof attacks. Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy, 6

[19] Ramesh, M.R. and Reddy, C.S. (2016). A survey on security requirement elicitation methods: classification, merits and demerits. Int. J. Appl. Eng. Res, 11(1), pp.64-70

[20] M. Damodaran. (2006). Secure Software Development using Use Case and Misuse Case, Issues Inf. Syst., vol. 7, no. 1, pp. 150–154

[21] I Park, J.H. and Park, J.H. (2017). Block chain security in cloud computing: Use cases, challenges, and solutions. Symmetry, 9, 164

[22] Ibrahim, M.B., Designing A Fingerprint Biometric Authentication System for Students Electronic Examination.

[23] Protecting Your Biometric Identity, Available: https://www.synaptics.com/technology/security-suite, 6th Feb, 2020

[24] Yang, W., Wang, S., Hu, J., Zheng, G. and Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. Symmetry, 11(2), p.141

[25] Hadid, A., Evans, N., Marcel, S. and Fierrez, J. (2015). Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Processing Magazine, 32(5), 20-30

[26] A. K. Jain, K. Nandakumar, and A. Nagar. (2008). Biometric template security. EURASIP J. Adv. Signal Process,2008, 113:1–113:17