Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

An Extra Security Measurement for Android Mobile Applications Using the Fingerprint Authentication Methodology

Mohammad Algarni*
Department of Computer Science, Al-Baha University, Al-Baha, Saudi Arabia.

Received 30 Oct. 2023; Accepted 26 Nov. 2023; Available Online 12 Dec. 2023.

Abstract

This research discusses the development of an Android application through the integration of fingerprint recognition technology for user authentication as a way of improving security in the system. The app serves as an additional security layer, requiring users to verify their identity before gaining access to any installed applications on their Android device. The use of technologically developed devices with fingerprint scanners that have the capacity for analyzing biological traits facilitates a strong user verification process. The process makes use of a fingerprint previously registered by the user to authenticate user legitimacy, hence providing an efficient authentication process. A set of metrics was introduced and verified against a legacy system, proving that the proposed system surpasses the legacy system. This new approach offers the advantage of serving as an alternative to using PIN numbers or pattern unlocking on Android smartphones.

I. Introduction

In recent years, the surge in phone and tablet applications has entirely reshaped how we handle sensitive information, conduct our financial transactions, and communicate on a personal level. As our reliance on these applications grows, it is becoming increasingly crucial to prioritize their security.

Numerous studies conducted over the last decade have shed light on the vulnerabilities found within applications, thus emphasizing the need for robust security measures. Research explores the escalating concern regarding the security of making payments via apps within the ecosystem. By analysing the third parties involved in the app payment systems on Android and iOS, the study underscores the need for essential security measures. The results highlight the vulnerabilities existing within multiple integrated apps, thus emphasizing the shared responsibility of developers, cashiers, and merchants [1].

Biometric authentication has emerged as a secure method for user recognition, especially in light of recent security breaches. Biometrics encompass characteristics such as fingerprints, iris patterns, voice recognition and DNA analysis. All these distinct traits are utilized for individual identification purposes and constitute the foundation for the data used during the verification process [2].

Keywords: Authentication, Security, Android, Smartphones, Biometrics, Mobile Applications, Privacy.

Production and hosting by NAUSS

* Corresponding Author: Mohammad Algarni
Email: malgarni@bu.edu.sa
doi: 10.26735/EPZF6556

In biometric systems, data is stored to verify individuals' identities. When people attempt to enter a system, they provide their traits, which are then compared with the stored data. If there is a match, they gain access, while their activity logs are also tracked [3].

A. What are Biometrics?

The security discipline utilizes three distinct types of verification and authentication:

- Something you know: a PIN, password, or personal information (such as your grandfather's first name).
- Something you have: a card key, smart card, or token (Secure ID card) [4].
- Something you are: a biometric trait, known as one of the most secure and convenient verification/ authentication tools. It cannot be stolen.

Biometrics assess individuals' unique biological or behavioral characteristics to distinguish or verify/ authenticate their identity [2].

Of all the authentication methods, biometrics are extremely convenient and secure. Unlike other methods, biometrics cannot be stolen, borrowed, or simply forgotten. It is extremely difficult to forge an identification. Biometrics involve measuring the characteristics of individuals to authenticate or recognize their identity [4].

1) Common Biological Biometrics

This category utilizes characteristics and features of the human body for authentication and identifications purposes. Popular examples include palm geometry, fingerprints, the hand and/or retina, facial characteristics, or the iris [2].

2) Common Behavioral Characteristics

This category encompasses keystroke pattern, gait, signature, and voice. Technologies related to individuals' signatures and voices are the most strongly developed among this category of biometrics [2].

3) Fingerprint Recognition Systems

Human fingerprints are highly detailed, unique, difficult to alter, and remain consistent throughout an individual's lifetime. This makes them a reliable, long-term marker of one's identity. Law enforcement and other authorities often use fingerprints to identify individuals who intentionally hide their identity or are incapacitated or deceased and unable to identify themselves following natural disasters. Fingerprint analysis has been in use since the last century and has played a significant role in solving several crimes. Consequently, many criminals consider wearing gloves to conceal their identity.

Fingerprint authentication is an automated method that validates whether two human fingerprints match. Fingerprints are one type of trait used to identify individuals and confirm their identity [2].

A fingerprint is characterized by the distinct arrangement of ridges and valleys on the fingertip. Fingerprint recognition or authentication involves the process of comparing a known fingerprint with another fingerprint to ascertain whether the imprints originate from the same finger [5]. To match fingerprints for identification purposes, the analysis usually involves comparing the features found within the fingerprint pattern. These features include characteristics known as patterns that appear in ridges (see Fig. 1 [5]). Unique attributes called minutia points are found within these patterns. There is a sufficient number of similarities and features identified in the ridge patterns found on individuals' fingertips that can be categorized. Fingerprints exhibit three fundamental patterns, namely loops, whorls, and arches, observable within the ridges of the fingertips. (see Fig. 2). These patterns are formed during fetal development and remain virtually unchanged throughout a person's lifetime. Additionally, understanding the properties and structure of the skin is critical when utilizing certain imaging technologies [5].

Fig. 1. An Image Of A Fingerprint Created By The Friction Ridge Structure [5].

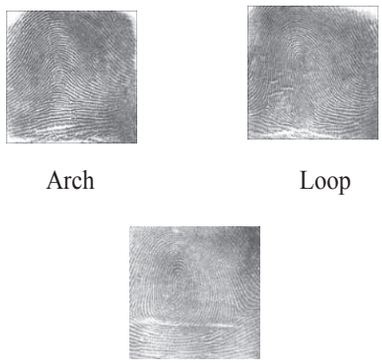

Fig. 2. Fingerprint Types.

4) Fingerprint Log-in Authentication

Electronic fingerprint readers have been implemented in security applications, specifically for log-in authentication to identify computer users. Nevertheless, certain less advanced technologies have been found to be vulnerable to relatively straightforward fraud attempts, such as the use of counterfeit fingerprints created using gel substances.

The utilization of fingerprint sensors in the notebook PC market experienced a surge in popularity throughout 2006. Computers, including models such as ThinkPad, VAIO, HP Pavilion, and EliteBook, feature integrated sensors that serve the dual purpose of detecting motion and facilitating document scrolling, similar to the functionality of a scroll wheel [6].

On September 21, 2013, following the launch of the iPhone 5S, a collective of German hackers publicly disclosed their successful circumvention of Apple's recently introduced Touch ID fingerprint sensor. Their method involved capturing a fingerprint image from a glass surface using photography, which was subsequently employed as a means of verification. The representative of the organization expressed the expectation that this development would effectively eliminate any misconceptions regarding fingerprint biometrics, emphasizing the imprudence of using an immutable, ubiquitous item as a security token [7].

5) Fingerprint Types

Prior to the advent of computerization, huge fingerprint repositories relied on manual filing systems. The classification approaches employed in the past were manual and relied on overall ridge patterns observed on multiple or all fingers, such as the identification of circular patterns [8]. This system facilitated the organization and retrieval of paper documents within vast collections, solely based on the analysis of friction ridge patterns [2].

B. Advantages and Disadvantages of the Biometric Security System

1) Advantages

The primary advantage of using this technology is the uniqueness that biometric traits offer, making biometric technology increasingly important in our lives Given the uniqueness of biometric technology, an individual's traits become the single most effective way to identify that user. The probability of two users exhibiting the same traits in a biometric security system is near zero [9].

Secondly, the highly secure method of identifying users makes this technology less prone to users sharing access to highly sensitive data. Each trait used during the identification process is a singular property of that user. In other words, it is extremely challenging, if not impossible, to duplicate or share biometric traits to access other users' data. This enhances security, ensuring that user information and data remain strongly protected from unauthorized users [10].

Furthermore, the identification of users through biometrics cannot be lost, stolen, or forgotten. This aspect of biometric technology makes it a popular identification method [11]. This method of identifying and then granting access to users greatly facilitates user identification. Finally, the majority of biometric security systems are easy to install and require only a small amount of funding for equipment (except for modern biometric technology, such as DNA/retinal/iris recognition) [10].

One significant advantage of implementing this type of technology is the uniqueness of traits it possesses, increasing the importance of biometric technology in our everyday lives.

Moreover, by implementing user identification protocols, the security of this technology is enhanced, reducing the possibility of users sharing

access to sensitive data. Each characteristic used in the identification process represents an attribute of an individual. Therefore, it becomes extremely challenging or even impossible for someone to replicate or share biometric access data with others.

Lastly, utilizing biometrics for user identification guarantees that such information cannot be lost, stolen, or overlooked. This particular characteristic contributes to the increasing dominance and application of this technology [11]. This approach simplifies the process of identifying individuals and granting user privileges.

To sum up, biometric security systems are known for their easy installation and affordable equipment costs. However, it is worth noting that advanced biometric technologies, such as DNA, retinal and iris recognition, can be more expensive [10].

2) Disadvantages

While there are certainly advantages associated with security systems, it is important to acknowledge that there also exist some fundamental problems. Every approach to using biometrics has its vulnerabilities, creating challenges for users [12]. For example, if a biometric security system relies on fingerprints for user identification and a user suddenly loses a finger, this can cause difficulties during the verification process [13]. Similarly, certain illnesses, like strep throat, can pose challenges for authorized users when utilizing speech recognition systems.

Many individuals still have concerns about implementing biometric technology in domains such as security, keeping up with advancements, scalability, accuracy, privacy, and other related issues.

C. Related Works

Authors in [15] surveys existing authentication methods on mobile devices, categorizing them into knowledge-based, physiological biometric-based, behavioral biometrics-based, and two/multi-factor authentication. It compares their usability and security levels, reviews vulnerabilities and attacks, and suggests a future trend towards multi-factor authentication. This approach integrates multiple authentication metrics (e.g., combining behavioral biometrics with knowledge-based methods) for enhanced security without burdening the user with multiple inputs.

A research article by Yıldırım and Varol [14] delves into the development of an Android application that utilizes fingerprint recognition to validate web logins. They specifically focus on leveraging the fingerprint feature and IMEI number of the Samsung Galaxy S5 to generate one-time passwords, enhancing the security of accounts in sectors like the government and banking. The authors highlight the increasing significance of security in devices by proposing a robust, user-friendly authentication method. The operational process of this Android application is thoroughly explained, encompassing IMEI registration and fingerprint authentication for password generation. The study emphasizes the role played by several features, particularly fingerprint recognition, in strengthening the security of mobile applications. The coding and development were carried out using Java on the Eclipse platform, making use of the Samsung Pass SDK for fingerprint recognition. In summary, the authors underscore the importance of incorporating features to strengthen mobile application security and present their Android app as an example showcasing these features for secure user authentication on web-based platforms. Additionally, they suggest leveraging software development kits, such as Samsung Pass SDK, to enhance mobile app security.

In another study conducted by Wang et al. [15], a comprehensive survey is presented on the user authentication methods employed on their mobile devices. These techniques are categorized into four types: knowledge-based approaches, biological biometrics-based methods, behavioral biometrics-based techniques, and multi-factor authentication systems. Knowledge-based approaches involve using text or graphics as inputs, commonly used but susceptible to attacks. Biological biometrics-based methods rely on traits such as fingerprints or iris scans, offering higher levels of security but may require specialized hardware. Behavioral

biometrics-based authentication captures user behaviors like typing patterns which, although secure, can be influenced by low quality sensor data. Multi-factor authentication combines metrics to enhance security and can pose challenges for users. The article emphasizes the importance of incorporating integrated authentication metrics to enhance security while minimizing user effort. It also discusses vulnerabilities and challenges, such as preventing replay attacks and creating a balance between security and usability. Overall, the article highlights the evolving landscape of user authentication and underscores the significance of developing approaches to meet the changing demands of mobile device security.

In [14], authors in their study focused on developing a web login authentication mobile app utilizing fingerprint scanning and recognition technology. The proposed study employs the Samsung Galaxy S5's fingerprint feature and the device's IMEI number to generate single-use, time-limited secure passwords for signing into various online user accounts, including government, banking, and education. The study highlights the growing trend of using biometric security, specifically fingerprint authentication, in mobile devices and its potential widespread application in user authentication.

Unlike the literature on various aspects of biometric security, this article introduces an advancement in mobile application security by implementing fingerprint authentication as an additional layer of protection. While other articles focus on different aspects of security, this specific article targets Android applications and provides a more detailed level of defense. This approach ensures that if a device is unlocked, unauthorized access to individual applications is effectively prevented.

With its integration into Android systems, it provides a more secure user experience. By utilizing the built-in fingerprint sensors, it ensures accessibility without the necessity for specialized hardware. This particular emphasis on application-level security distinguishes article three, as it addresses a relevant issue; namely, security.

II. Research Objectives

A. Research Proposal

The research objective is to develop an Android app that aims to enhance security by implementing biometric authentication before using apps. The app will be developed so that users are required to authenticate using their fingerprint before accessing any app installed on their Android smartphone. The integration will prevent unauthorized usage of installed apps. This research is driven by the growing need for user identification using their biological characteristics. The proposed system utilizes data associated with these characteristics to offer alternatives to traditional PIN codes or pattern methods.

B. Research Objectives

The primary objective is to overcome the vulnerabilities of application authentication, thereby strengthen the security of user applications by using fingerprints as an extra authentication layer before individuals can access a certain application.

The proposed research objectives are as follows:

- To enhance smartphone security against data hacking and stealing.
- To utilize fingerprint scanners on Android smartphone.
- To increase the difficulty of forgery.
- To identify the real identity of users, as falsifying fingerprints is challenging.
- To provide an additional security measure for certain applications.

C. Expected Output and Research Contributions

Applications

- Providing users with an extra security layer for their Android applications.
- Optimizing users' time and effort by facilitating the authentication phase when they log into their applications.
- Utilizing the device's capabilities, as it uses the fingerprint sensor already built-in the smartphone.

- Reinforcing and promoting the usability of applications through the fingerprint authentication process.
- Providing an additional level of both privacy and security for Android applications users, ensuring better protection of data on the smartphone.

Research Outputs:

- A methodology applicable to Android smartphones using built-in biometric traits scanners (e.g., face and iris).
- A methodology applicable in different venues with widely used biometric traits in iOS smartphones and tablets.

D. System Vision

The core of this design is linear in nature, with vendor fingerprint libraries, the fingerprint sensor, and fingerprint services providing functional wrapping of the well-known fingerprint authentication processes [16].

It implements high-level authentication logic using specific applications by invoking vendor unprotected APIs [4].

However, there are somewhat limited publicly identified core weaknesses that can be exploited to root the majority of Android devices [16]. For example, attackers can acquire the fingerprint data if they root the device.

E. Research Feasibility

Many of us are keen our mobile phone information private, and technology has helped us retain this privacy through using fingerprint technology on the mobile phones.

- Technical Feasibility: This research requires programmers to develop an application that allows users to protect more than one application.
- Economic Feasibility: This application is based on identifying the user of the Android smartphone and utilizing the fingerprint sensor to its peak.
- Operational Feasibility: This application will provide users with protection from intrusion by adding another security measure to their applications.

III. System Analysis

A. Methodology

In a study by Sporild [17], several metrics were introduced to help evaluate the effectiveness of security measures. By applying these metrics to the proposed system, we can assess its strength when comparing it with legacy password systems that use a password as an additional security layer for Android applications.

To evaluate each metric, we will assign scores to both the proposed system and the password-based system. The scores are based on how each authentication method fulfils the purpose of the metric.

1) Metrics and Results:

Metric M 1: This metric measures the effectiveness of the system based on its authentication method, with a maximum achievable score of 5. In the proposed system, we suggest using a combination of "something you are" (fingerprint) and knowledge-based identification (knowledge of which finger's fingerprint is used) earning a full 5 points according to this metric criterion. On the one hand, if a textual password is used in systems, it would score only 1 point according to the provided table.

Metric M 2 aims to evaluate the strength of the client server communication. It includes questions about the encryption algorithm, size, authentication algorithm, and key size. Points are assigned based on the answers provided. These questions in M 2 focus on how the system is implemented. Assuming that both systems are implemented optimally, they would both receive a score of 5 out of 5.

Metric M 3 determines the robustness of the logging-on procedures. It consists of five questions regarding these procedures and assigns a point if a procedure is implemented correctly or zero otherwise. Each question is analysed below for both systems.

Question 1: If an error condition occurs, does the system indicate which part of the data is correct or incorrect?

Analysis: This question pertains to how both systems are implemented. If the system relies on a password, it is possible to inform the user that the password was incorrect. Similarly, in the proposed

system, it is also feasible to let the user know if their fingerprint authentication process was accepted or not (see Fig. 9). Both systems follow these procedures, so a point can be assigned to each system.

Question 2: To enhance security, is it possible to limit the number of log-on attempts, with consequences such as introducing a time delay before the next authentication attempt, keeping a record of unsuccessful attempts, disconnecting the connection, or triggering an alarm trap?

Analysis: This question focuses on evaluating how effectively each system is implemented. In the case of the proposed system, it is easier to implement a delay before allowing subsequent attempts since it is more challenging to use brute force techniques with fingerprints compared to passwords [18]. Based on this reasoning, it can be argued that the proposed system has an advantage over one that uses passwords. We assign 1 point to the proposed system and 0.5 points to the other. All the other factors mentioned in this procedure can be implemented for both systems [19].

Question 3: Additionally, can you limit the time allowed to log on, as an additional security measure?

Analysis: This question concerns the implementation aspect, assuming that this can be controlled by the client side for any system that requires authentication. Both systems receive points for this procedure, assuming proper record-keeping is performed on the server side.

Question 4: Following an authentication attempt, does the system show the date and time of the successful authentication and provide details of any unsuccessful attempts?

Analysis: This question focuses on implementation, assuming that both systems maintain proper records on the server side. Both systems receive points for this procedure.

Question 5: All users have their own distinctive identifier, which is for individual use only?

Analysis: Essentially, a fingerprint represents "who you are", while a password represents "what you know". It is reasonable to argue that fingerprints are more unique to an individual compared to a password. Based on this reasoning, we assign a score of 1 to the proposed system and 0.5 points to the other one. All other factors mentioned in the procedure can be implemented for both systems, except for the time delay. Therefore, according to M 3, the proposed system receives a score of 5 out of 5 while the textual password system receives a score of 4 out of 5.

2) Discussion

As discussed above, the proposed system received a score of 15 points, while the one utilizing passwords scored 10 points, according to the metrics introduced above. The main goal of the proposed system is to address some of the limitations of the legacy system that relies on passwords and provides extra security advantages using the proposed system. It aims to enhance the legacy system by implementing improvements based on various criteria.

B. The Method Employed for Software Development

It is necessary to build a reliable, robust system that offers users a range of services to learn, as mentioned above. This means that for developing the app, passing through many stages is essential.

The decision to use the Waterfall approach for the implementation was based on its importance as one of the most widely accepted models in the field of Software Engineering. Its primary goal is to ensure research success [20].

The "Waterfall" technique (see Fig. 3) involves dividing the software development process into phases. In this model, it is customary for the output of each phase to serve as the input for the next phase [20].

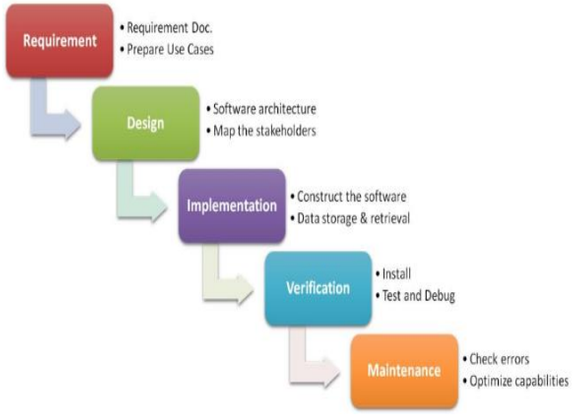

Fig. 3. Different Phases Of The Waterfall Model [20].

C. Sequential Phases of the Waterfall Model

Throughout the Requirement Gathering and Analysis stage, all prospective system requirements are gathered and logged in a requirement specification document.

Next, during the System Design stage, the requirement specifications identified during the preliminary stage are investigated in depth to initiate a system design. This design helps detail the hardware and system requirements and construct the whole system formation [20].

During the Implementation stage, the system is structured based on the insights delivered by the system design. This construction happens through the creation of small programs, known as components, which are combined in the following stage. Every component is individually built and evaluated for its operational abilities; a process known as Unit Testing [20].

In the Integration and Testing phase, all the components constructed during the execution stage are combined into an integrated system after each unit's functionality has been validated. Following the incorporation of the complete system, comprehensive testing is undertaken to identify and report any defects or faults.

System Deployment: After implementing both functional and non-functional testing, the product is introduced into the customer's environment or can be made available in the market.

System Maintenance: In the client's environment, specific problems may occur, which are addressed by releasing patches. Furthermore, to enhance the product, updated versions may be issued. Maintenance implies serving these updates to the customer's environment.

In this way, the stages follow each other and flow progressively downwards (like a waterfall) [20].

D. Functional & Non-Functional Requirements

1) Functional Requirements

- Mobile Owner User can add their fingerprint to the system (Registration).
- The owner can add/remove the fingerprint of any user to indicate their granting of permission or otherwise.
- The user can lock/unlock any installed application with their fingerprint.
- The app system will communicate with the Android System as a 3rd party application.

2) Non-Functional Requirements

Security: The most generally utilized password is the word “password.” As a result, data are kept secure by some algorithms used for encrypting passwords are similarly secure like the password. It is simple to guess easy passwords, that leads to security being compromised. However, a complex password may not be usable by users [21]. Adding a biometric trait will make the system stronger, as it is difficult to steal or guess these characteristics.

Privacy: This is the capability to control access to one’s personal information, to remain autonomous, and to keep one’s life free of intrusions. Since identity fraud is increasing, fingerprints, that are considered a strong biometric trait, are becoming an increasingly attractive method for user authentication [21].

Performance: The application should have minimal delay when administering fingerprint authentication orders.

Compatibility: The application should be compatible with Android smartphones Version 7.0 or higher.

E. System Design

1) Use Case Diagram

Among many forms of UML artifacts, use case diagrams have proven to be highly effective for the verification and validation of requirements, particularly in the context of app requirements [22]. The use case diagram is illustrated in this subsection (see Fig. 4).

2) Data Flow Diagram

The data flow diagram is considered one of the most important diagrams utilized in the structural methods used to represent a wider view of the system. The DFD is drawn (see Fig. 5).

3) Sequence Diagram

Due to the significant role of analysis sequence diagrams in object-oriented systems analysis and design, it is necessary to have an efficient sequence diagram modelling technique that can assist beginners in creating these diagrams [23]. The sequence diagram is presented (see Fig 6).

4) Prototyping (Application Screens)

In the prototype, the initial screen asks the user to provide the fingerprint to be able to perform the authentication process (see Fig 7).

If the fingerprint provided is incorrect, the user will be prompted with this screen (see Fig 8).

If the fingerprint provided is correct, the user will be prompted with this screen (see Fig 9).

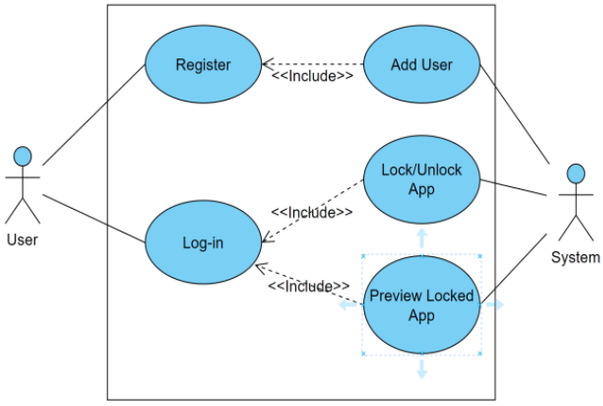

Fig. 4. Use Case Diagram.

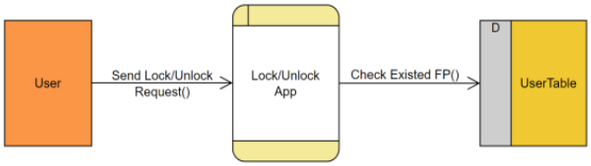

Fig. 5 Data Flow Diagram.

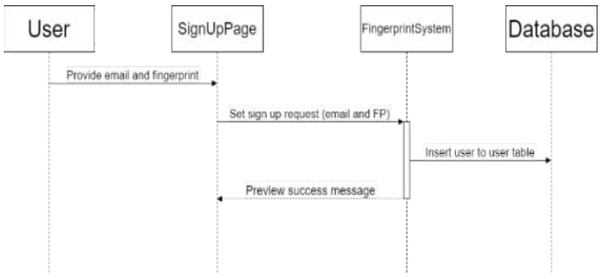

Fig. 6. Sequence Diagram.

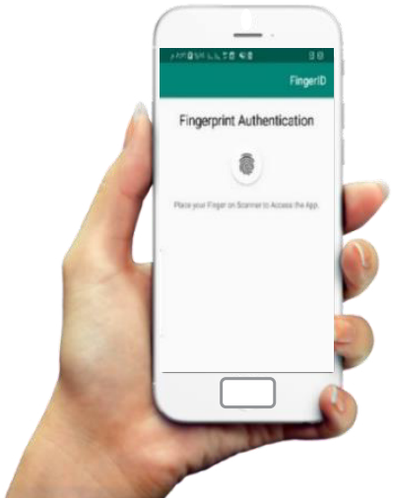

Fig. 7. Initial Screen.

Fig. 8. print Rejection Screen.

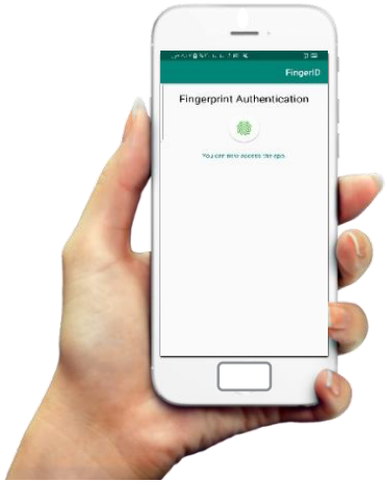

Fig. 9. Fingerprint Approval Screen.

IV. Future Work

A. Limitations

While the concept underlying the suggested system is promising, it is essential to acknowledge the existence of limitations and potential obstacles that require further thought. The dependability of fingerprint recognition technology is a significant difficulty that must be addressed. While fingerprints are commonly acknowledged as a reliable means of identification, there may be situations in which the recognition system has difficulties precisely identifying a user's fingerprint. Authentication failure can occur as a result of various factors, such as the presence of dirt, moisture, or a minor finger injury.

Moreover, conditions that some individuals' fingerprints have may potentially lead to complications in the process of authentication. Furthermore, it is important to acknowledge that the efficacy of the proposed approach might be impacted by the calibre and functionalities of the fingerprint sensor integrated within Android smartphones. Lower-quality sensors could be decreasing the accuracy rate, thereby impacting the overall performance of the proposed authentication process.

Additionally, one of the main vulnerabilities in Android operating systems is root access, which grants users access to the operating system. As a result, it allows users to manipulate or bypass the security measures applied to the system. If any breach occurs in the root access, fingerprints stored on the device are compromised.

B. Future Work

The methodology proposes enhancing the security of Android applications using the integration of fingerprint authentication. The main objective of the proposed system is to provide a reliable approach for users' identity authentication. The proposed authentication mechanism can possibly be improved in the future. Therefore, research should endeavor to delve into different modalities integration, namely, but not limited to facial recognition and voice authentication techniques, in conjunction with the fingerprint data so as to improve the overall security measures. It is of utmost importance to explore how these methods can effectively complement each other. No effort should be spared towards improving usability as well as user experience. This will ensure a friendly system for the user. Usability studies should involve the collection of user input, interface improvement, and optimizing system enrolment. Checking the system tolerance towards scalability and compatibility is recommended to ensure optimal performance of the proposed system across a wide set of Android devices.

V. Conclusion

This paper presents a methodology for enhancing the security of Android applications through the implementation of fingerprint authentication. It provides a comprehensive approach to user verification, thereby promoting the security of data and applications. Integrating this authentication technique within the Android ecosystem guarantees streamlined user functionality. Nevertheless, it is imperative to realize the inherent limitations associated with the dependability of fingerprint identification technology, specifically related to factors such as environmental conditions and device quality, which have the potential to impact the accuracy of recognition. Further studies ought to prioritize the enhancement of this technology through thorough improvement and the exploration of modalities integration to add an extra layer to existing security measures. In the future, it is necessary to maintain a level of readiness while observing advancements in technology and integrating them into the suggested system to enhance security protocols. By adopting this approach, we remain at the forefront of safeguarding user data and privacy by advocating enhanced security measures in mobile applications within the dynamic landscape of the present time. This study represents a significant advancement in establishing a secure ecosystem for Android applications, making a valuable contribution to protecting user information in an increasingly digital world.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Author declare that he has no conflict of interest.

References

[1] W. Yang, J. Li, Y. Zhang, and D. Gu, "Security analysis of third-party in-app payment in mobile applications," Journal of Information Security and Applications, vol. 48, pp. 102358, 2019.

[2] A.K. Jain, P. Flynn, and A.A. Ross, Eds., Handbook of Biometrics, Springer Science & Business Media, 2007.

[3] C. Le and R. Jain, "A survey of biometrics security systems," Washington University in St. Louis, EEUU, 2009.

[4] S. Liu and M. Silverman, "A practical guide to biometric security technology," IT Professional, vol. 3, no. 1, pp. 27-32, 2001.

[5] A.I. Khan, "Comparing and Improving Existing Fingerprint Recognition Algorithms," Research Gate, 2015.

[6] Fingerprint, available online: https://academic-accelerator.com/encyclopedia/fingerprint (accessed August 9, 2023).

[7] Chaos Computing Club, Project Blinkenlights, available online: http://blinkenlights.net/project.

[8] S. Adebisi, "Fingerprint studies—the recent challenges and advancements: a literary view," Internet J. Biol. Anthropol, vol. 2, no. 2, pp. 1-9, 2009.

[9] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, 2004.

[10] A. Jain, R. Bolle, and S. Pankanti, Eds., Biometrics: Personal Identification in Networked Society, vol. 479, Springer Science & Business Media, 1999.

[11] S. Prabhakar, S. Pankanti, and A.K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security & Privacy, no. 2, pp. 33-42, 2003.

[12] A. Babich, "Biometric Authentication. Types of biometric identifiers," 2012.

[13] R. Saini and N. Rana, "Comparison of various biometric methods," International Journal of Advances in Science and Technology, vol. 2, no. 1, pp. 24-30, 2014.

[14] N. Yıldırım and A. Varol, "Android based mobile application development for web login authentication using fingerprint recognition feature," in Proc. 2015 23nd Signal Processing and Communications Applications Conference (SIU), 2015, pp. 2662-2665.

[15] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats, and trends," Computer Networks, vol. 170, 107118, 2020.

[16] Y. Zhang, Z. Chen, H. Xue, and T. Wei, "Fingerprints on mobile devices: Abusing and leaking," in Proc. Black Hat Conference, 2015.

[17] M. Sporild, "Method for evaluating authentication system quality," Master's thesis, 2007.

[18] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proceedings of the IEEE, vol. 91, no. 12, pp. 2021-2040, 2003.

[19] L. Talley, "User Login (Authentication) Failures and Lockout Mechanism," available online: https://elandings.atlassian.net/wiki/spaces/es/pages/40370191/User+Login+Authentication+Failures+and+Lockout+Mechanism (accessed November 9, 2023).

[20] Y. Bassil, "A simulation model for the waterfall software development life cycle," arXiv preprint arXiv:1205.6904, 2012.

[21] A.K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125-143, 2006.

[22] G. Costain and B. McKenna, "Experiencing the elicitation of user requirements and recording them in use case diagrams through role-play," Journal of Information Systems Education, vol. 22, no. 4, pp. 367-380, 2011.

[23] T. Sin, "Usability of analysis sequence diagram," retrieved June 1, 2007.