Research Article

Mobile App for IoT-Based Home Security System with Fingerprint Access Control

Abdul Wahid[1*], Rahmat Hidayat[2], Muhammad Riska[3]

[1,2,3] Department of Informatics and Computer Engineering, Makassar State University, Indonesia
* Corresponding Author: wahid@unm.ac.id

Abstract: This study investigates the development and evaluation of an Android-based security system for residential areas, focusing on entrance and exit gate control. Recognizing the limitations of existing systems, we propose an "IoT-based Fingerprint Security Village" application. The system utilizes a prototype development model informed by data collected through interviews, questionnaires, and observations. The application allows residents to monitor and access gates using fingerprint scanners, enhancing security and convenience. To ensure quality, the system underwent rigorous testing based on the ISO 25010 software testing standard. Testing encompassed five key aspects, Functional Suitability: The application achieved a perfect score, indicating it flawlessly performs its intended functions. Portability: The application successfully functioned on all 14 tested Android devices. Performance Efficiency: CPU usage remained exceptionally low (average 0.1%, max 5.5%), and memory usage (average 58.2 MB, max 86.5 MB) demonstrated efficient resource utilization. Security: Testing revealed a low-medium security risk, highlighting areas for potential improvement. Usability: The user-friendliness test yielded a very high score (92%), placing it in the "Very Feasible" category. These results confirm that the "IoT-based Fingerprint Security Village" application effectively meets all evaluated aspects of the chosen software testing standard.

Keywords: IoT based System; Security Village; Android; Fingerprint; ISO 25010

Citation: A.Wahid, R.Hidayat, M.Riska, "Mobile App for IoT-Based Home Security System with Fingerprint Access Control", *Iota*, **2024**, ISSN 2774-4353, Vol.04, 02. https://doi.org/10.31763/iota.v4i2.732

Academic Editor : Adi, P.D.P
Received : March, 20 2024
Accepted : April, 18 2024
Published : May, 8 2024

1. Introduction

The relentless march of technology constantly introduces new tools and methods, often by combining existing ones to create more advanced solutions. These advancements have a profound impact on our daily lives, influencing everything from communication to the way we conduct business. In the realm of security, this progress brings forth innovative solutions to safeguard individuals and their belongings.

Several technological tools have been developed to streamline human activities, including automated equipment that assists with various tasks. As research and development deepen [1], existing knowledge expands, leading to the creation of entirely new products or substantial improvements to existing ones. This process, with its long-term focus [1], [2], drives innovation in the security sector as well.

Security, particularly in the context of home protection, remains a top priority for everyone. Conventional security systems often incorporate biometrics, a technology identified by [3], [4] as a method for readily identifying individuals based on unique physical (e.g., fingerprints, facial features, retinas) or behavioral characteristics. Biometric systems have evolved into robust security solutions capable of fulfilling both identification and verification needs. Fingerprint technology, with its high level of security, exemplifies a widely used system. It relies on hardware sensors that read an individual's fingerprint for identification and verification purposes. Notably, fingerprints were the first security system, pioneered by E. Henry in America back in 1902.

The Security Village system, also known as environmental or regional security, provides a valuable tool for security personnel and residents. It allows them to monitor their surroundings and identify potential security threats, both internally and externally. This system often utilizes Android, an open-source, Linux-based operating system for smartphones and mobile devices. As defined by [5], a sensor is a device that detects external stimuli and translates them into an electrical signal. This allows the system to react to environmental changes. Fingerprints, as described by [6], are a well-established biometric tool with over 100 years of use in forensic investigations. Their unique, unchanging nature and relative ease of acquisition make them a reliable method for user identification.

Existing security systems for residential areas often lack efficiency, particularly at entry and exit points. While fingerprint scanners offer a reliable security solution, their integration into a comprehensive system remains an area for exploration [7]. This research addresses this gap by proposing an Android-based "IoT-based Fingerprint Security Village" application. This application leverages fingerprint scanners and mobile technology to enhance security and convenience for residents in gated communities.

2. Theory

2.1 Development

According to Law No. 11 of 2019 concerning the National System of Science and Technology, development is an activity to increase the benefits and support of science and technology that has been proven to be true and safe to improve the function and benefits of science and technology. The development can be in the form of processes, products, and designs.

According to [1], development is deepening and expanding existing knowledge. In development, there are stages: planning, implementation, and evaluation, which are accompanied by improvement activities so that a form is produced that is considered appropriate. Research and development also aim to create new products or improve existing products. Development is focused on the long term. Then it is used to prepare employees following the growth and change of the organization.

2.2 System

According to [8], a system is a collection or group of any subsystem/part/component, both physical and non-physical, that are interconnected and can work together harmoniously to achieve a specific goal. According to [8], there are several classifications of systems, namely:

1. Abstract systems and physical systems [9]:
   Abstract systems are systems that cannot be seen directly. These systems are usually thoughts or ideas. An example is philosophy. Physical systems are systems that can be seen with the naked eye and are always used by humans, for example, accounting systems, computer systems, and others.
2. Natural systems and artificial systems [10], [11]:
   Natural systems are systems that exist due to the influence of nature, for example, the earth's rotation system, the gravity system, and others. Artificial systems are systems that are designed and created by humans.
3. Closed systems and open systems [12], [13]:
   Closed systems are systems that have no connection with the outside of the system and are not affected by the outside conditions of the system. Open systems are systems that are connected to the outside of the system.

2.3 Security Village

In general, the elements of society are considered when looking for a house as a place to live for their families, namely the security of the housing environment. Moreover, The Security Village system, or what is often called environmental or territorial security is a system that can be used to help security personnel and residents monitor their surroundings from the possibility of criminal disturbances, both from outside the environment and from within the environment itself [14], [15].

2.4 Android OS

Android is an open-source Linux-based operating system for smartphones/mobile phones. There is an open-source platform on Android that makes it easy for developers to create and create their applications [16], [17]. Two types of Android operating system distributors have been created in the world. One receives support from Google or Google Mail Services (GMS), and the other is which is freely distributed without direct Google support known as Open Handset Distribution (OHD). Based on the above explanation, it can be concluded that Android is a Linux-based mobile device operating system released in 2007, which was first developed by Android.Inc. which was eventually acquired by Google in 2005.

2.5 Fingerprint

According to [5], a sensor is a device that receives a stimulus, usually called a stimulus, as a quantity of a certain property or condition that can be converted into an electrical signal. According to [3], Fingerprint or fingerprint is biometric that has been used systematically for investigation for 100 years that has been measured, duplicated, and then examined extensively, a biometric that does not change and is relatively easy to take. Fingerprint sensors are currently used by various electronic devices, including smartphones, doors, and other devices that have a high level of security and can only be opened by those who are authorized, in this case, the homeowners in the housing complex [18], [19].

3.Method

3.1 Research Type and Data Sources

This type of research uses Research & Development (R&D) research. According to [1], Research and development (R&D) is the process of developing a new product or improving an existing product first. To determine the test results of the development of the Android OS-based security village system using a fingerprint scanner with ISO25010 which uses testing of functional suitability, portability, performance efficiency, security, and usability aspects [20], [21].

3.2 System Architecture

The system architecture in Figure 1 is the security village system that is being designed. This system uses several technologies, including the fingerprint system on smartphones (Fingerprint Reader), ESP32 [22], and servo motors. When residents who live in the housing complex place their finger on the smartphone, then the ESP32 will read and search for fingerprints in the database. If the registered fingerprint matches the previously placed fingerprint, the ESP32 will send a command to open the gate [23], [24], [25].

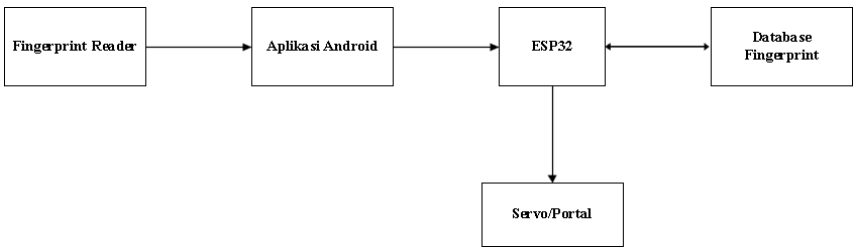

Figure 1. System Architecture

3.3 Development Model

The development model used in this research is the development model from the SDLC (System Development Life Cycle) method [26], [27], [28].

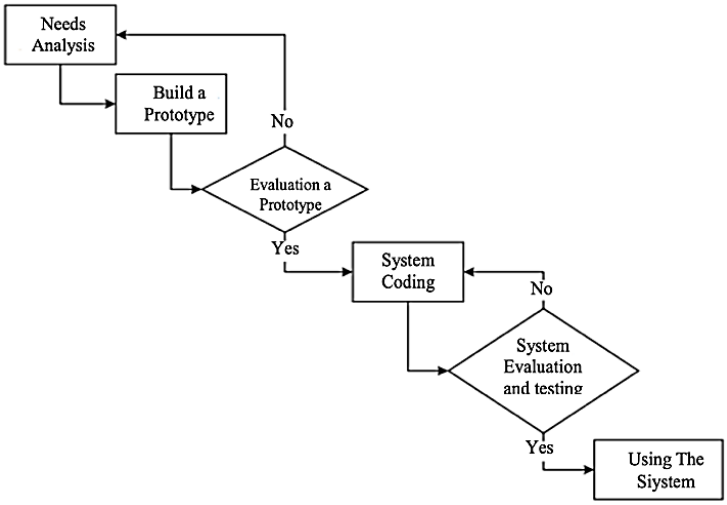

Figure 2. Prototype Development Stages

Based on the prototype stages in Figure 2, development begins with the first system requirements analysis, then builds the prototype by designing the database and storyboard, and then the design is evaluated by the user. If the design follows the user's desires or needs, the process can proceed directly to the system coding stage. However, if the prototype does not yet follow the user's needs or desires, the development process must return to stages 1, 2, and 3. After the system coding stage is complete, the system evaluation and testing stage will be carried out. Evaluation is carried out by the user while system testing uses testing software [29], [30].

4. Result and Discussion

4.1 Building the Application System

This research presents an Android operating system (OS)-based application for secure access control in residential communities, aptly named "Security Village." The application was developed using Android Studio software and leverages the Kotlin programming language for efficient functionality. Firebase serves as the application's database management system, ensuring secure storage of user data. The primary objective of this system is to streamline resident access to entrance and exit gates. Residents can conveniently control gate access through the application installed on their devices. This integration with a security-managed system not only enhances convenience but also bolsters security within the residential area.

4.1.1 Login Screen

Figure 3 is a multi-user login screen that contains columns for filling in email, password, and a login button.

Figure 3. Login Screen

4.1.2 Admin Dashboard Screen

Figure 4. Admin Dashboard

Moreover, Figure 4 is a user dashboard screen that contains a Resident menu, History, Profile, Recent History, Guest List, and a guest entry button.

4.1.3 Resident Menu Screen

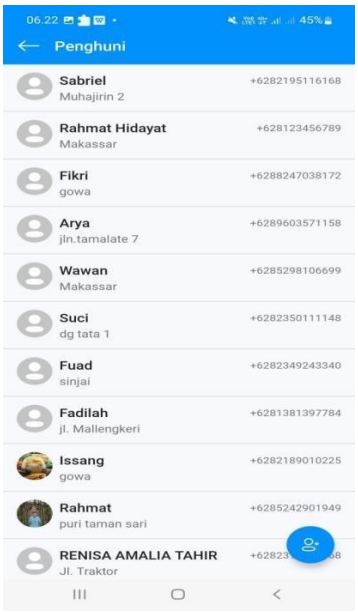

Figure 5. Resident Menu

Figure 5 is a resident menu screen that contains information or resident data and a button to add residents.

4.1.4 Add New Resident Menu Screen

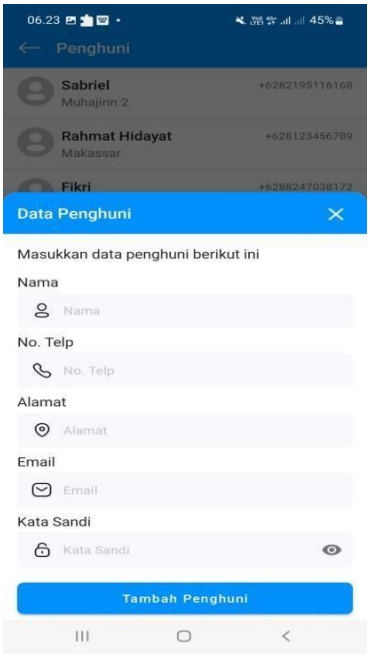

Figure 6. Add New Resident Menu

Figure 6 depicts the resident menu screen, which facilitates account registration. This screen provides designated fields for residents to enter their Name, Phone Number, Address, Email, and Password. Additionally, an "Add Resident" button allows users to complete the registration process.

4.1.5 History Menu Screen

Figure 7. History Menu

Figure 7 is a history menu screen that contains Exit History information, name, time, and date.

4.1.6 Admin Profile Menu Screen

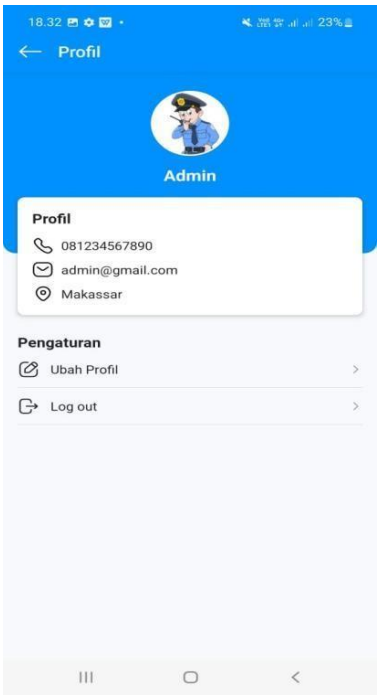

Figure 8. Admin Profile Menu

Figure 8 illustrates the admin profile menu screen. This screen displays the administrator's profile information, including a profile photo, phone number, email address, and address. Additionally, it provides buttons for changing the profile information and logging out.

4.1.7 Change Admin Profile Screen

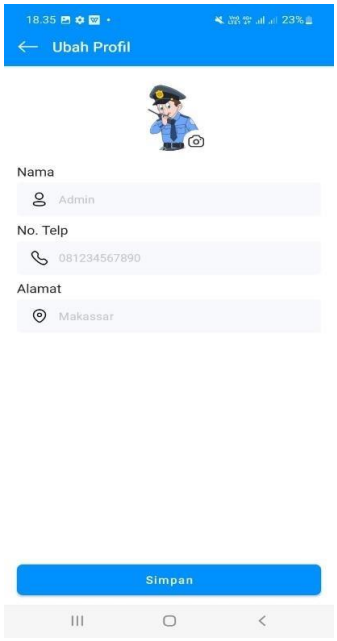

Figure 9. Change Admin Profile Menu

Figure 9 is a change admin profile menu screen that contains columns for filling in a name, phone number, address, photo, and a save button to change the profile.

4.1.8 Add Guest Menu Screen

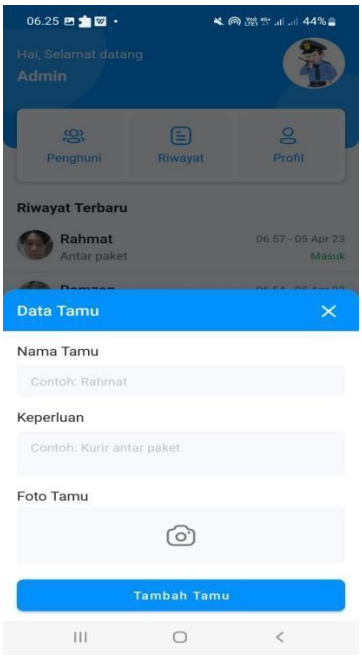

Figure 10. Add Guest Menu

Figure 10 is an add guest screen that contains columns for filling in guest name, purpose, and photo, and an add guest button to open the next portal with fingerprint verification.

4.1.9 Remove Guest Screen

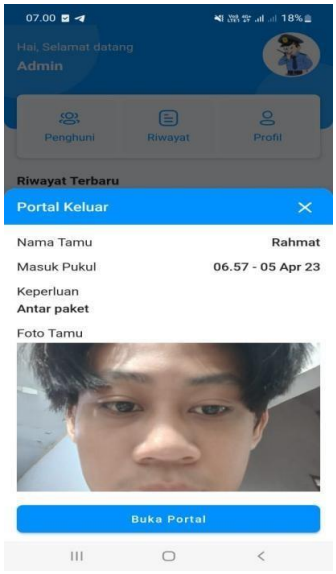

Figure 11. Remove Guest

Figure 11 is a remove guest screen that contains status information in the form of the guest name, check-in time, purpose, photo, and a next portal open button followed by fingerprint verification.

4.1.10 Remove Guest Screen User Dashboard Screen

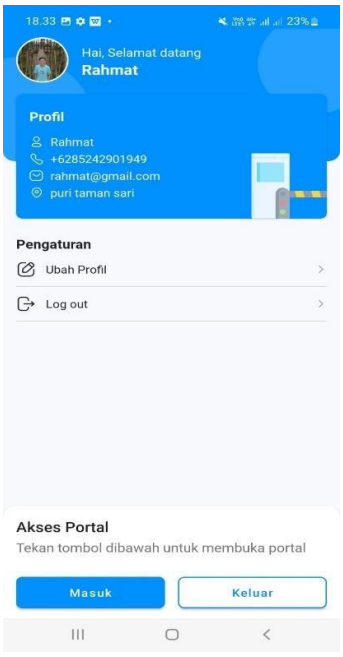

Figure 12. User Dashboard

Figure 12 depicts the user dashboard screen of the Security Village application. This screen provides a comprehensive overview of a user's profile, including their photo, name, phone number, email address, and residential address. Additionally, the dashboard offers convenient buttons for managing user profiles, logging out of the application, and accessing the entrance and exit gate control portal.

4.1.11 Change User Profile

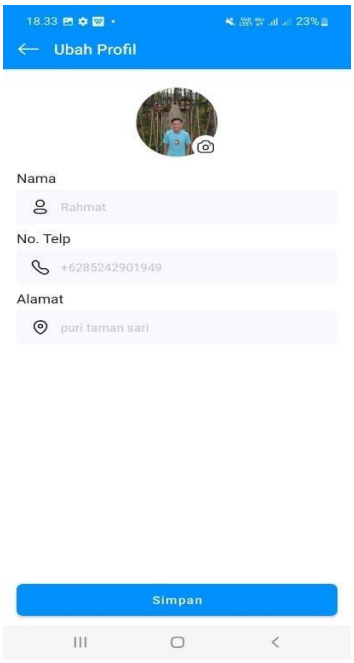

Figure 13. Change User Profile

Figure 13 depicts the user profile editing screen. This screen provides several fields for updating user information, including Name, Phone Number, Address, and a "Change Photo" option. Additionally, a "Save" button allows users to confirm the changes to their profile.

4.1.12 Prototype System

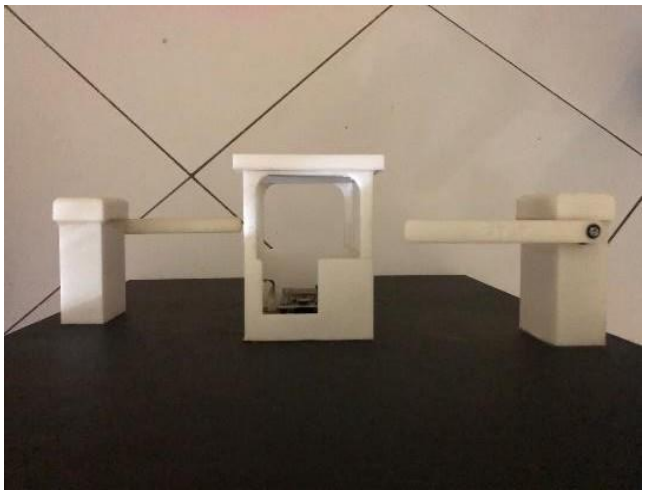

Figure 14. Prototype System

Figure 14 depicts the system prototype designed to resemble a general portal. This prototype incorporates an Internet of Things (IoT) microcontroller capable of connecting to the security system application on a smartphone.

4.2 System Testing

4.2.1 Testing of Functional Suitability Aspect

System testing was carried out by involving 2 (two) experienced experts. The experts tested the system directly by trying all the functions in the system, then filling in the test values in the questionnaire table by checking the options that were considered correct and providing input regarding the development of the tested system. There are 25 points, these points are based on the features that have been developed from the previously approved design. The results of the test questionnaire from the 2 (two) experts are listed in Table 1.

Table 1. Results of testing the functional suitability aspect

Validator	Designed Features (P)	Successfully Tested Features (I)	Feature Completeness
	25	25	1
	25	25	1
Average (∑)	25	25	1

Moreover, to assess the functional suitability of the Security Village information system, we employed a formula derived from the feature completeness matrix. This formula calculates the score by dividing the number of successfully implemented features by the total number of designed features. As shown in Table 1, the application achieved a score of 1 using the aforementioned formula. This score signifies that the software meets the functional suitability criteria. A score approaching 1 aligns with the principles of the feature completeness matrix, indicating a high degree of successful feature implementation.

4.2.2 Testing of Portability Aspect

Similar to the functional suitability assessment, we evaluated the portability of the Security Village information system using a formula derived from the feature completeness matrix. This formula calculates the portability score by dividing the number of features successfully implemented across various devices by the total number of designed features. As demonstrated in Table 2, the application achieved a perfect score of 1 using this formula. This score indicates that the application functions flawlessly across a wide range of devices, fulfilling the portability aspect. As with the functional suitability evaluation, a score approaching 1 aligns with the principles of the feature completeness matrix, signifying successful portability across diverse devices.

Table 2. Results of Testing the Portability Aspect

No.	Devices	Android Version	Successful
1.	Oppo A92	Android 11	1
2.	Real Me 5	Android 10	1
3.	Poco X3 GT	Android 13	1
4.	Realme C21	Android 11	1
5.	Xiaomi Redmi Note 10S	Android 12	1
6.	Vivo V21	Android 12	1
7.	Oppo Reno 4F	Android 12	1
8.	Vivo 1802	Android 8	1
9.	Oppo A35S	Android 8	1
10.	Realme 7i	Android 10	1
11.	Samsung A51	Android 12	1
12.	Xiaomi Redmi A1	Android 12	1
13.	Oppo A77S	Android 12	1
14.	Samsung A14	Android 13	1
	Total		**14**

The formula derived from the feature completeness matrix is again employed to assess the portability of the Security Village information system. This formula calculates a portability score by dividing the number of features that function successfully across various devices by the total number of designed features. As shown in Table 2, the application achieves a perfect score of 1 using this formula. This score indicates that the application can be used flawlessly on a wide range of devices, fulfilling the portability aspect. Consistent with the functional suitability evaluation, a score approaching 1 aligns with the principles of the feature completeness matrix, demonstrating successful portability across diverse devices.

4.2.3 Testing of Performance Efficiency Aspect

A more detailed breakdown of the testing results is presented in Table 3.

Table 3. Results of testing the performance efficiency aspect

No	Category	Average	Rate Maximum	Results
1	CPU Usage	0.1%	5.5%	Limit Low
2	Usage Memory	58.2 MB	86.5 MB	Limit Low

Table 3 presents the results of testing the Security Village application's performance efficiency using Apptim software. The average CPU usage is remarkably low at 0.1%, with a maximum reaching only 5.5% (considered a low limit). Similarly, the average memory usage sits at a comfortable 58.2 MB, with a maximum of 86.5 MB (also considered a low limit).

Throughout the testing process, the application exhibited no memory leaks or crashes that could lead to forced closures or launch failures. Notably, all test results fell within the lower limit range, with none reaching the medium or exceeding the maximum usage limits. This indicates that the developed Security Village application effectively meets the performance efficiency criteria established by the ISO 25010 software quality testing standards.

4.2.4 Security Testing Aspect

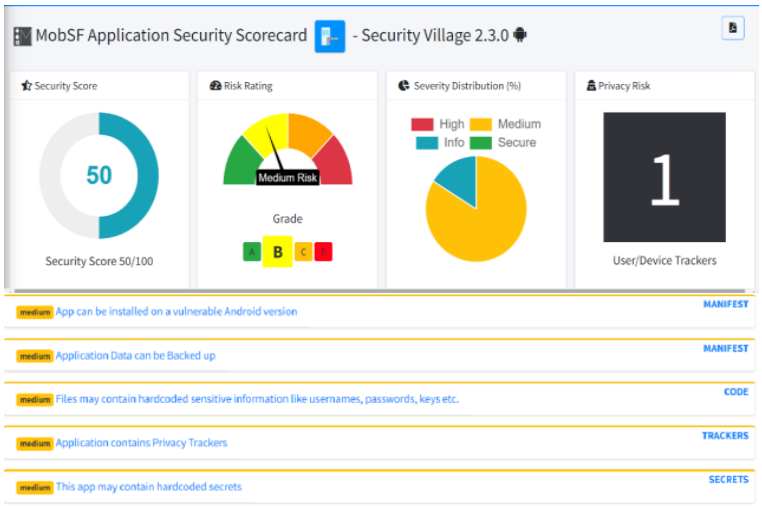

Figure 15. Result of Security Aspect Testing

For the security aspect of the Security Village application, testing was conducted using MobSF software, a tool specifically designed to evaluate security vulnerabilities within Android applications. As illustrated in Figure 15, MobSF software was employed to assess the security of the Security Village application. The test results indicate that the application falls within the "Low-Medium Risk" category. This implies that while there might be some potential security vulnerabilities, they are not considered severe. It's important to note that the application still adheres to the ISO 25010 software quality testing standards, demonstrating an overall good security posture.

4.2.5 Usability Aspect Testing

Furthermore, to assess the usability of the Security Village application, a questionnaire containing 28 questions was distributed to 14 student users. The questionnaire employed a Likert scale to gather feedback. Once all responses were collected, the scores were converted into percentages using the following equation 1.

$$P = (\text{Score obtained} / \text{Maximum score}) \times 100\% \quad [1]$$

Where P is Percentage, the Score obtained is the score obtained from the questionnaire, Maximum score is the maximum possible score for the questionnaire The usability testing yielded a highly positive outcome, with a score of 92% placing the system within the "Very Feasible" category. This score signifies that the Security Village system is user-friendly and effectively caters to the needs of its users.

4 Conclusions

This study successfully developed an Android OS-based security village application featuring multi-user login, resident data management, access history, guest management tools, and a logout function.

Rigorous testing based on the ISO 25010 software testing standards confirmed the application's quality across five key aspects. They are Functional Suitability: The application achieved a perfect score, indicating it flawlessly performs all intended functions. Portability: The application functioned successfully on all tested devices, demonstrating its adaptability. Performance Efficiency: CPU and memory usage remained exceptionally low, signifying efficient resource utilization. Security: While testing revealed a low-medium security risk, highlighting areas for potential improvement, the application meets the standard's requirements. Usability: With a user-friendliness score of 92% ("Very Feasible"), the application is easy to learn and navigate.

These exceptional results demonstrate that the developed "Security Village" application effectively addresses security concerns in residential communities while offering a convenient user experience.

Acknowledgments: Thanks to the entire research team, lecturers, and colleagues at the Department of Informatics and Computer Engineering, Makassar State University, thank you for all your cooperation, hopefully, this research can be a good reference for the same discipline, in the future.

Author contributions: All authors are responsible for building Conceptualization, Methodology, analysis, investigation, data curation, writing—original draft preparation, writing—review and editing, visualization, supervision of project administration, funding acquisition, and have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sugiyono, Metode penelitian kuantitatif, kualitatif, R&D. Bandung, Indonesia: CV. Alfabeta, 2016.
2. A. Rachman, E. Yochanan, A. Samanlangi, and H. Purnomo, Metode Penelitian Kuantitatif, Kualitatif dan R&D. 2024.
3. D. Maltoni, D. Maio, A. K. Jain, and J. Feng, Handbook of Fingerprint Recognition. Cham: Springer International Publishing, 2022. doi: 10.1007/978-3-030-83624-5.
4. A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4–20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349.
5. J. Fraden, Handbook of modern sensors: Physics, Designs, and Applications, 5th ed. San Diego, USA: Springer Cham, 2016. [Online]. Available: https://doi.org/10.1007/978-3-319-19303-8
6. H. Oktianatasari, W. F. Mahmudy, and B. Rahayudi, "Automated Fingerprint Identified System dengan Teknik Minutiae-Based," vol. 4, no. 2, 2008.
7. Universitas Gadjah Mada Yogyakarta et al., "Integration of Indoor Localization System using Wi-Fi Fingerprint, Bluetooth Low Energy Beacon and Pedometer Based on Android Application Platform," IJIES, vol. 13, no. 4, pp. 171–181, Aug. 2020, doi: 10.22266/ijies2020.0831.15.
8. P. Ein-Dor and E. Segev, "A Classification of Information Systems: Analysis and Interpretation," Information Systems Research, vol. 4, no. 2, pp. 166–204, Jun. 1993, doi: 10.1287/isre.4.2.166.
9. T. Gabor, L. Belzner, M. Kiermeier, M. Beck, and A. Neitz, A Simulation-Based Architecture for Smart Cyber-Physical Systems. 2016, p. 379. doi: 10.1109/ICAC.2016.29.
10. A. Moreno and A. Etxeberria, "Agency in Natural and Artificial Systems," Artificial Life, vol. 11, no. 1–2, pp. 161–175, Jan. 2005, doi: 10.1162/1064546053278919.
11. A. Sloman, "Varieties of Meta-cognition in Natural and Artificial Systems".
12. C. Cellucci, "From Closed to Open Systems," in Philosophy of mathematics: Proceedings of the 15th International Wittgenstein Symposium, Wien: Hölder-Pichler-Tempky, 1993, pp. 206–220.
13. R. Anderson, "Open and Closed Systems Are Equivalent (That Is, in an Ideal World)," in Perspectives on Free and Open Source Software, J. Feller, B. Fitzgerald, S. A. Hissam, and K. R. Lakhani, Eds., The MIT Press, 2005, pp. 127–142. doi: 10.7551/mitpress/5326.003.0013.
14. J. Hendrawan, I. D. Perwitasari, and R. S. Ritonga, "The Village Security Information System (Siskamling) to Support Digital Village Development".
15. X. Zhu, L. Yang, and J. Han, "Research on SysML-Based Urban-village Security Administration System," in Proceedings of the 2016 International Conference on Public Management (ICPM 2016), Kunming, China: Atlantis Press, 2016. doi: 10.2991/icpm-16.2016.96.
16. L. Ma, L. Gu, and J. Wang, "Research and Development of Mobile Application for Android Platform," IJMUE, vol. 9, no. 4, pp. 187–198, Apr. 2014, doi: 10.14257/ijmue.2014.9.4.20.
17. F. Sposaro and G. Tyson, "iFall: An Android Application for Fall Monitoring and Response".
18. M. Muniruzzaman, "A Survey of Biometrics Security System," vol. 11, Nov. 2011.
19. D. Bhattacharyya and R. Ranjan, "Biometric Authentication: A Review," Science and Technology, vol. 2, no. 3, 2009.
20. A. A. Rahman, "Quality Consideration for e-Learning System Based on ISO/IEC 25000 Quality Standard".
21. A. Acharya and D. Sinha, "Assessing the Quality of M-Learning Systems using ISO/IEC 25010," International Journal of Advanced Computer Research, vol. 3, no. 3.
22. A. Wahid, D. Syahbani, and F. Adiba, "Implementation of Smart Farming for Oyster Mushroom Cultivation Based on Wireless Sensor Network Using ESP8266," IOTA, vol. 3, no. 2, pp. 148–160, May 2023, doi: 10.31763/iota.v3i2.610.

23. R. Pasic, I. Kuzmanov, and K. Atanasovski, "ESP-NOW communication protocol with ESP32," IP, vol. 6, no. 1, Mar. 2021, doi: 10.37886/ip.2021.019.
24. A. Maier, A. Sharp, and Y. Vagapov, "Comparative analysis and practical implementation of the ESP32 microcontroller module for the Internet of things," in 2017 Internet Technologies and Applications (ITA), Wrexham: IEEE, Sep. 2017, pp. 143–148. doi: 10.1109/ITECHA.2017.8101926.
25. M. Babiuch, P. Foltynek, and P. Smutný, Using the ESP32 Microcontroller for Data Processing. 2019, p. 6. doi: 10.1109/CarpathianCC.2019.8765944.
26. A. Faqihuddin, I. Wahyuddin, and N. D. Nathasia, "Mysql Database Processing Information System Using The System Development Life Cycle (SDLC) Method At Quality Guarantee Agency Working Unit At National University," vol. 4, no. 36, 2020.
27. Ilham Tri Maulana, "Penerapan Metode SDLC (System Development Life Cycle) Waterfall Pada E-Commerce Smartphone," JUISIK, vol. 2, no. 2, pp. 1–6, Jun. 2022, doi: 10.55606/juisik.v2i2.162.
28. S. Seema, S. Kute, D. Surabhi, and A. Thorat, "A Review on Various Software Development Life Cycle (SDLC) Models," vol. 3, pp. 2320–5156, Aug. 2014.
29. B. A. Camburn et al., "Methods for Prototyping Strategies in Conceptual Phases of Design: Framework and Experimental Assessment," in Volume 5: 25th International Conference on Design Theory and Methodology; ASME 2013 Power Transmission and Gearing Conference, Portland, Oregon, USA: American Society of Mechanical Engineers, Aug. 2013, p. V005T06A033. doi: 10.1115/DETC2013-13072.
30. B. Camburn et al., "Design prototyping methods: state of the art in strategies, techniques, and guidelines," Des. Sci., vol. 3, p. e13, 2017, doi: 10.1017/dsj.2017.10.