Journal of Information Systems and Informatics
Vol. 6, No. 3, September 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i3.844 Published By DRPM-UBD

IoT-Based Smart Door Lock System with Fingerprint and Keypad Access

Ketut Ananta Kevin Permana[1], I Nyoman Piarsa[2], Anak Agung Ketut Agung Cahyawan Wiranatha[3]

[123]Departement of Information Technology, Udayana University, Bali, Indonesia
Email: [1]kevinprmn25@gmail.com, [2]manpits@unud.ac.id, [3]agung.cahyawan@unud.ac.id

Abstract

Doors are important components in a home, serving as entry points, room dividers, and security barriers. Door locks have evolved from manual mechanisms to automatic systems using technologies such as passwords, face sensors, and fingerprint sensors. To enhance practicality and efficiency, an Internet of Things (IoT)-based Smart Door Lock system using keypads and fingerprint sensors was developed in this research. The system was built using the Waterfall model Software Development Life Cycle (SDLC) and utilizes Firebase for real-time data communication and control through an Android application. Black box testing was conducted to verify the system's functionality, achieving a 100% success rate across 20 trials. The system offers enhanced security and remote access control, with potential applications in both residential and commercial settings.

Keywords: Internet of Things, ESP-32, Keypad, Fingerprint, Android

1. INTRODUCTION

The Internet of Things (IoT) is a technology that connects computing devices and everyday objects through networks without requiring direct human interaction. IoT involves smart devices with processors, sensors, and communication devices that collect, send, and process data from their environment. The collected data is shared through IoT gateways or edge devices, then sent to the cloud or analyzed locally [1]. As a technology that supports Industry 4.0, IoT integrates the physical world with the digital, enabling broad and flexible connectivity. Although still in the early stages of development, IoT offers a wide range of modern solutions and services with a global network of interconnected devices, using standardized and interoperable communication protocols [2].

Doors play an important role in a home, as they are not only the main access for residents to enter and exit, but also serve as the main element that provides security and privacy. As an integral part of a home's structure, the door is often the first point of interaction for anyone who enters, making it an essential element in

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

creating a first impression of the home [3]. Currently, mechanical locks that are still manual in nature are commonly used to secure doors [4]. However, along with the development of technology, door security systems have also progressed. Various digital door security systems have been developed, offering more sophisticated and efficient solutions to improve the safety and comfort of home residents [5]. Nowadays, automatic door locks are available that can be accessed using various methods, such as passwords, facial recognition sensors, fingerprint sensors, or even E-KTPs that have been recorded during automatic key generation. This technology offers a higher level of security and convenience for room owners, allowing them to manage access more easily and safely [6].

Related research was conducted aimed at designing and implementing a door security system using a fingerprint sensor based on Arduino Uno R3 microcontroller and DY-50 fingerprint sensor module. The prototype is tested using a fingerprint sensor which then activates the door lock solenoid to unlock the door [7]. Similar research was also conducted at BMT NU Jangkar. focused on developing a smart door lock system using a fingerprint sensor and Arduino Uno microcontroller. This system uses Arduino Uno as a microcontroller, fingerprint sensor, and 12V adapter as a power source. Testing is done by registering the fingerprint first, then trying the registered fingerprint to open the door lock solenoid [8]. Another study conducted aims to design and develop a dual-mode home security system that uses fingerprints and is integrated with IoT technology that is directly connected to an Android smartphone. This system utilizes the ESP-32 Wroom microcontroller, fingerprint sensor, and solenoid door lock as output. Testing is done by simulating the installed hardware and testing the performance of the camera and fingerprint sensor [9]. Another research on door lock discusses the design and implementation of a digital door lock system using an Arduino microcontroller and keypad. This system is designed to increase security by using a PIN entered through a keypad. Testing is done by trying several combinations of PINs that have been stored or not stored [10-12].

The main advantage of using door lock technology is its ability to precisely manage who can access a room. This technology solves problems related to lost keys, duplication of manual keys, as well as the difficulty in managing multiple keys for different rooms. The more rooms there are, the more keys there are to store, which can be a time-consuming and cumbersome process to find the right key [13]. Despite the advancements in door lock technology, many existing systems lack flexibility, remote control features, or integration with modern IoT infrastructures. This creates a gap for systems that are both secure and practical while providing seamless remote monitoring and control. Therefore, the need arises to develop a door security system that is safe, practical, and efficient by combining PIN and fingerprint sensors based on the ESP-32 microcontroller and utilizing Android applications as the remote access control and monitoring. This research combines

several door lock access methods in previous studies that have been mentioned to further advance usability and enhancement of door lock technology both used in residential or commercial environments.

2. METHODS

The methodology employed to achieve the objectives involves five stages of the system development life cycle, specifically using the waterfall method. Each stage is executed systematically, as depicted in the Figure 1 [14].

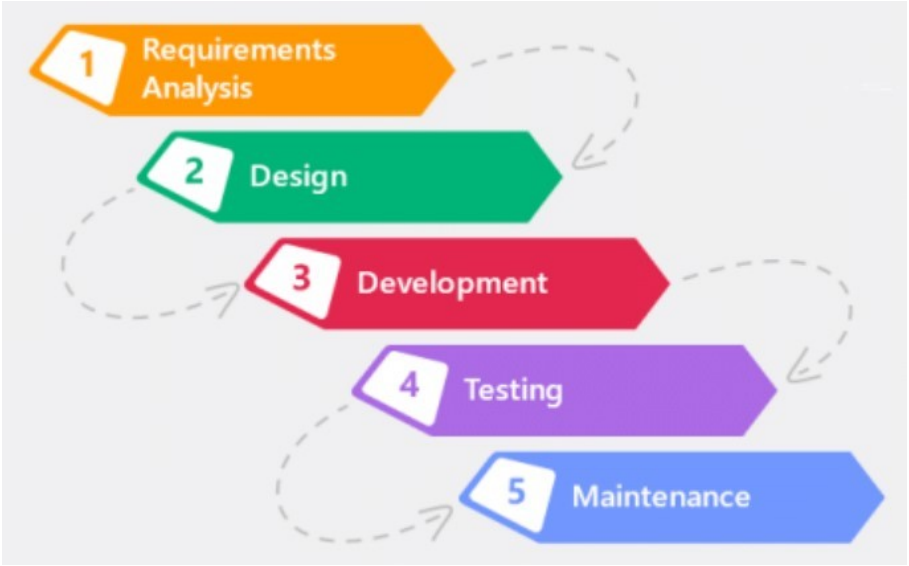


Figure 1. SDLC Method

Figure 1 shows the various stages in the development of the research. These stages include initial requirements analysis, system design, implementation, testing and system maintenance. However, this research only focuses on the testing phase, so the other stages are not discussed in too much detail.

2.1. Requirements Analysis

The initial stage of this process, known as requirements analysis, covers various factors such as the device to be used, desired features, and other software-related aspects. This stage involves collecting relevant literature from various sources such as books, journals, notes, and the internet. Such literature serves as a valuable reference to review the research material and acquire relevant knowledge.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

2.2. Design

The design stage follows the needs analysis and focuses on creating models based on the needs that have been identified during the analysis stage. This modeling process involves the use of various tools, including system overviews, schematic designs, hardware designs, and application or software designs.

Table 1. Softwares or Components for System Design Step

No	Softwares / Components	Amount
1	ESP-32	1
2	Sensor Fingerprint JM-101B	1
3	Keypad 4x4 Matrix 16 Key	1
4	Push Button	1
5	Modul Relay 1 Channel	1
6	Hi-Link HLK-20M12	1
7	Step Down LM2596	1
8	LCD I2C 16x2	1
9	Solenoid Door Lock	1

These tools that can be seen in table 1 serve as essential components in visually representing the structure and relationships within the system. Using these modeling techniques, the design stage aims to create a clear and comprehensive blueprint that will guide the subsequent development and implementation stages of the project.

2.3. Implementation

This stage involves developing a smart door lock system design. The database implementation as well as the data communication between the device and the mobile application used Firebase, while the programming languages used were C/C++ and Java. In addition, some hardware is also used in this research, including ESP32, fingerprint sensor, keypad, relay module, jumper cable, lcd i2c, solenoid door lock, 12V power supply, push button, and stepdown module. The hardware implementation results, and system overview will be provided in section 3.

2.4. Testing

Black box testing is a crucial stage in the software development process that aims to ensure the smoothness and reliability of the program that has been created. This testing stage is very important to identify and correct errors or deficiencies in the program flow[15]. The black box test results, that will be provided in section 3, show that each scenario has been successful and as expected [16].

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

2.5. Maintenance

Maintenance is the final stage of the project that allows assessment of the achievement of the set goals. This stage ensures the continued effectiveness and usability of the smart door lock system. In addition, maintenance provides an opportunity to make necessary updates or upgrades according to evolving needs and requirements. With good maintenance, the system can continuously adapt to changes, ensuring optimal functionality and high security for its users.

3. RESULTS AND DISCUSSION

3.1. System Overview

This system overview aims to provide an in-depth understanding of how the smart door lock system works and facilitate the delivery of information regarding various aspects and features of the system. This description covers the various components and interactions that occur within the system, thus providing a comprehensive view for the user or developer. Figure 1 will clarify and illustrate in detail the overview of the smart door lock system, assisting in the visualization of the structure and workflows involved.

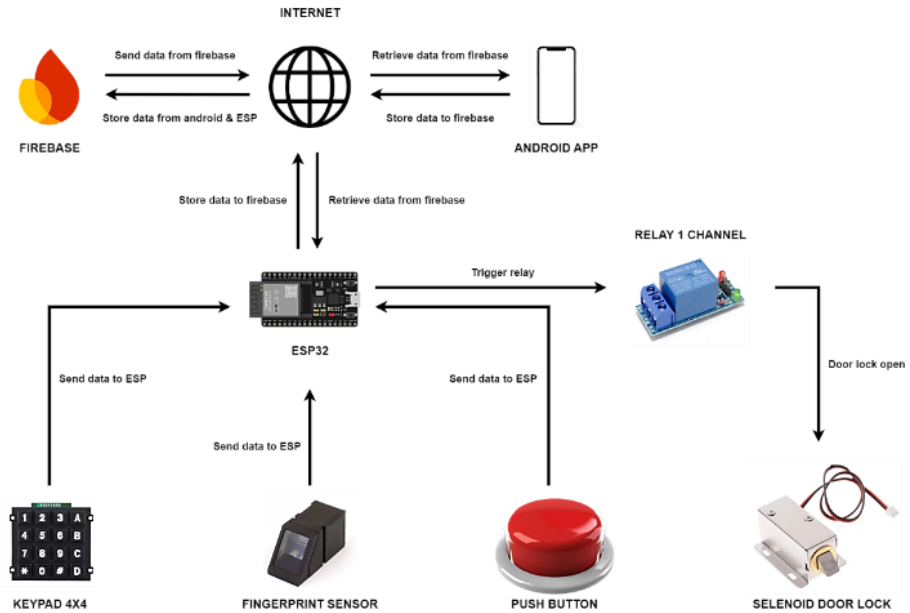


Figure 2. System Overview

Figure 2 is a system overview of the smart door lock system in this study. This figure shows the relationship between each component, starting from the ESP32

which acts as a microcontroller that will process input and output from each sensor. Keypad, fingerprint sensor, and push button act as input from the user which is then processed by ESP32 and gives a trigger to the relay which will activate the door lock solenoid. The mobile application is used as a control and monitoring device that is able to access the door lock and monitor door lock activities through firebase as data communication and database connected to the internet.

3.2. Schematic Designs

Schematic designing is an important step in the development of electronic systems, where detailed diagrams are created to connect the microcontroller with various other supporting modules, such as sensors, actuators, and communication modules. In this schematic, each module is connected to specific pins on the microcontroller, which allows the system to read data from that module and send the necessary commands. This design ensures that all components can interact effectively and efficiently, and function in accordance with the objectives set out in the needs analysis stage. With a good schematic design, the process of implementing and testing the system will run more smoothly and structured.

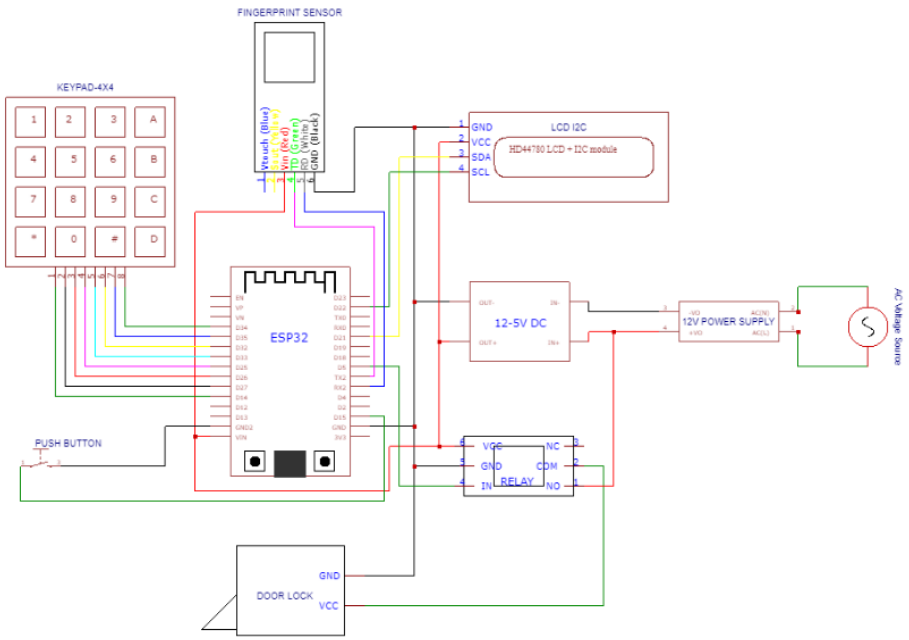


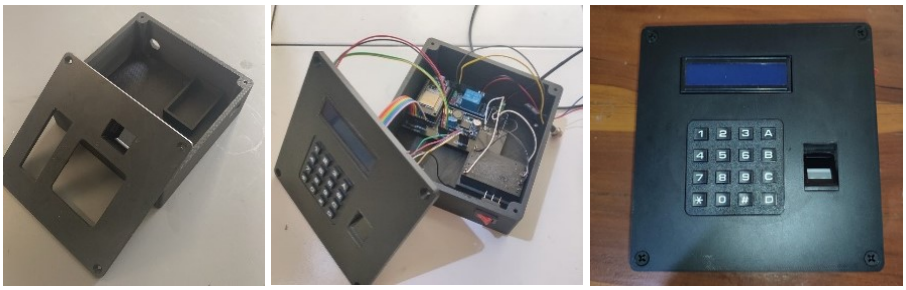
Figure 3. Schematic Designs

Figure 3 is a schematic design of the smart door lock system in this study. Each electronic hardware is connected into a single unit, each PIN on the device is

connected to each PIN on the ESP32 to then function as expected. This circuit uses a 12V AC power source which is used to supply the door lock solenoid and uses a 12V to 5V stepdown module to supply other modules including ESP32.

3.3. Hardware Implementation

At this stage, the electronic components that have been designed in the schematic are implemented into a real device. This process involves mounting and connecting the components on the circuit board, as well as ensuring all modules function properly according to the initial design. As a protector and to add aesthetic value to the device, a container is also designed for the electronic components that have been designed by adjusting the shape and size of the components.



(a) (b) (c)

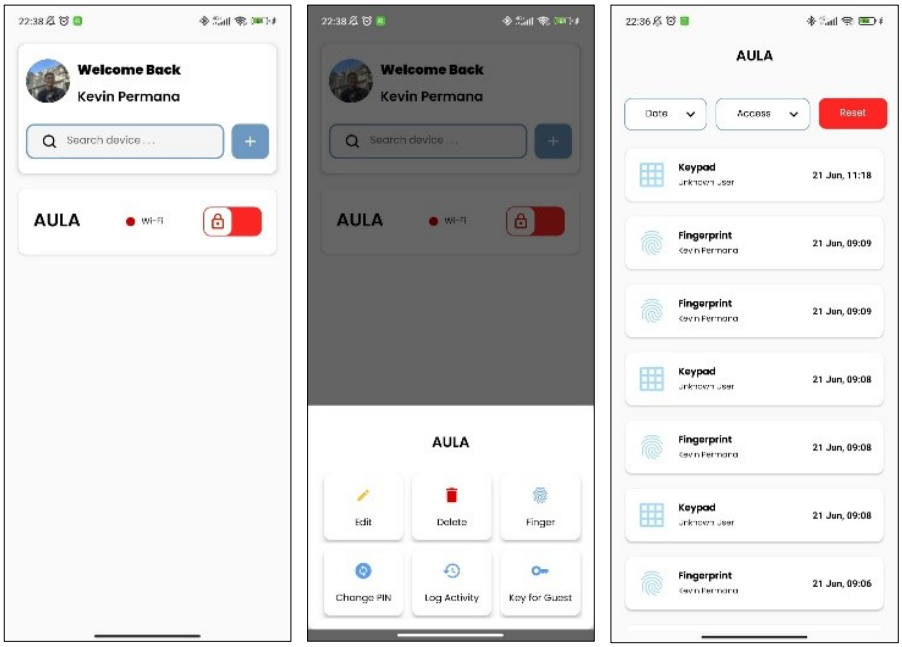
Figure 4. Hardware Implementation

Figure 4 is the result of the hardware implementation of the smart door lock system in this study. Figure (a) shows the device that is the container of each electronic component. Figure (b) shows electronic devices that have been connected using PCB (Printed Circuit Board) and implemented in a customized container. Figure (c) shows the final result of the hardware implementation which is the result of all the components that have been put together.

3.4. Software Implementation

The software design was developed and implemented in the form of an Android-based application. The application was designed specifically for the mobile platform, allowing users to access and control the smart door lock system through their Android device. This process involved the creation of an intuitive interface as well as the integration of features that support the main functionality of the application, ensuring an efficient and effective user experience. As such, users can utilize the full capabilities of the system directly from their smartphone or tablet.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**



(a) (b) (c)

Figure 5. Software Implementation

Figure 5 is the result of the software or android application for the smart door lock system in this study. Figure (a) shows the home page of the application, where the home page displays the smart door lock devices that have been added, each device has a switch button that acts as access to open and close the door lock device. Figure (b) shows when the device on the home page is selected, it will display several additional menus or features such as edit device, delete device, add fingerprint, change device PIN, activity log to monitor door lock activity, and key for guest to create a temporary key. Figure (c) is a monitoring display in the application, where every door lock access is done, it will be recorded and displayed on the activity log page.

3.5. System Testing

Testing is an important stage to ensure that the developed system is as expected. Black Box Testing is done to test software based on functional specifications, without examining the design and program code, aiming to ensure that the functions, inputs, and outputs of the software match the required specifications. The following table shows the results of the system performance testing.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 1. Test Results of Door Lock Access Through the Application

No	Test Scenarios	Test Cases	Expected Results	Result
1	Access the door lock via the app by entering a wrong PIN	PIN (incorrect)	The system denies door lock access and displays a message: Invalid PIN	Succeed
2	Access the door lock via the app by entering the correct PIN	PIN (correct)	System receives door lock access then activates door lock solenoid	Succeed

Table 1 is the scenario and results of testing the door lock access feature through the application. Testing was carried out with 2 test scenarios and got the results fulfilled or appropriate.

Table 2. Testing Results of Door Lock Access Through Keypad

No	Test Scenarios	Test Cases	Expected Results	Result
1	Access the door lock with an incorrect PIN	PIN (incorrect)	The system denies door lock access and LCD displays a message: PIN is incorrect	Succeed
2	Accessing the door lock with the correct PIN	PIN (correct)	System receives door lock access then activates door lock solenoid	Succeed

Table 2 is the scenario and results of testing the door lock access feature through via keypad. Testing was carried out with 2 test scenarios and got the results fulfilled or appropriate.

Table 3. Testing Results of Door Lock Access Through Fingerprint Sensor

No	Test Scenarios	Test Cases	Expected Results	Result
1	Access the door lock with unregistered fingerprint	fingerprint (unregistered)	The system denies door lock access and LCD displays a message: access denied	Succeed
2	Access door locks with registered fingerprint	fingerprint (registered)	System receives door lock access then activates door lock solenoid	Succeed

Table 3 is the scenario and results of testing the door lock access feature via fingerprint sensor. Testing was carried out with 2 test scenarios and got the results fulfilled or appropriate.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 4. Testing Results of Door Lock Access Through Push Button

No	Test Scenarios	Test Cases	Expected Results	Result
1	Access the door lock with push button module	push button (pressed)	System receives door lock access then activates door lock solenoid	Succeed

Table 4 is the scenario and results of testing the door lock access feature via push button. Testing was carried out with 1 test scenario and got the results fulfilled or appropriate.

Table 5. Door Lock Monitoring Test Results

No	Test Scenarios	Test Cases	Expected Results	Result
1	View the device activity	press the log activity button	System displays the device's access history	Succeed

Table 5 is the scenario and results of testing the door lock monitoring activity. Testing was carried out with 1 test scenarios and got the results fulfilled or appropriate.

3.6. Discussion

The results from the smart door lock system's development and testing reveal a robust and functional solution that integrates both hardware and software components effectively. The system successfully incorporated key inputs such as a keypad, fingerprint sensor, and push button, with an Android-based application providing an interface for remote control and monitoring. The system's performance met the expectations outlined in the test scenarios, and all components, both hardware and software, worked cohesively to achieve the desired functionality.

One of the key strengths of this project is the seamless interaction between hardware and software components. The use of the ESP32 microcontroller as the central processing unit enabled the smart door lock system to handle multiple inputs (keypad, fingerprint sensor, and push button) efficiently. The ESP32's ability to process data and communicate with a mobile application through the internet (via Firebase) ensures real-time monitoring and control, which enhances the system's utility in both domestic and commercial settings.

The hardware implementation, including the integration of a 12V AC power source and the use of a step-down module to regulate power for the ESP32 and other components, ensures stability in operation. The custom-built PCB, housed in a container for protection and aesthetics, indicates thoughtful consideration of design and practicality.

On the software side, the Android application offers an intuitive user interface, allowing users to control and monitor the system remotely. The integration of features like activity logs, guest key creation, and device management adds to the system's robustness and user-friendliness. The successful execution of these features in testing demonstrates the reliability of the system.

The system's performance was validated through comprehensive testing, as demonstrated by the results presented in Tables 1 through 5. All scenarios, whether through app access, keypad input, fingerprint recognition, or push button activation, showed consistent and successful results. This confirms that the system reliably responds to both correct and incorrect inputs, providing a secure locking mechanism while also ensuring ease of access for authorized users.
The testing scenarios showed no failures, suggesting that the design and implementation were thorough and capable of handling real-world usage. The black-box testing methodology used was effective in ensuring that the system meets functional requirements without needing to evaluate internal code structures. This approach was particularly useful in validating the user interface and input/output interactions, confirming the system's functionality from a user's perspective.

Despite the system's success, there are areas that could benefit from further development. For example, while the ESP32 provides adequate functionality, the system could potentially be enhanced by incorporating more advanced microcontrollers or additional communication protocols such as Zigbee or Z-Wave to improve scalability and integration with other smart home systems.
Another area for improvement is the fingerprint sensor, which currently works based on binary (registered/unregistered) identification. Implementing a more advanced biometric authentication system with support for multiple user profiles or higher security features could increase the system's appeal for use in more sensitive or high-security environments. Finally, while the Android application functions well in this initial implementation, expanding its compatibility to iOS platforms would make the system more accessible to a wider audience. Additionally, incorporating more real-time data analytics or integration with cloud-based services could further enhance the monitoring capabilities.

The results from this study demonstrate the effectiveness of the smart door lock system in providing a reliable and user-friendly access control solution. The hardware and software components were successfully integrated, and the system performed well in all test scenarios. The system's functionality can be further extended by making improvements in biometric security, platform compatibility, and scalability. Nonetheless, this project provides a solid foundation for further development and presents a practical solution for secure access management.

4. CONCLUSION

The research on the Smart Door Lock system has been successful, meeting expectations for door lock access through Android applications, keypads, fingerprints, and push buttons. The design and development process involved the seamless integration of hardware and software components, ensuring that each feature functions optimally and addresses user needs. The Android application includes essential features such as door lock access, device management (CRUD), fingerprint addition, PIN changes, activity logs, and temporary PINs, optimally utilizing Internet of Things (IoT) technology, enabling remote monitoring and control with Firebase RTDB for efficient, real-time data storage to communication. The system was tested 20 times with a 100% success rate across various scenarios, proving its reliability. For practical applications in both residential and commercial environments, this system will be able to provide enhanced security and ease of access. Future research should focus on testing the system under different environmental conditions and integrating additional security features, such as RFID and facial recognition, to further enhance flexibility and security. Expanding the system's capability into a broader Smart Home ecosystem and ensuring system operability during power outages through the integration of UPS are also potential areas for improvement.

REFERENCES

[1] A. N. Mas Erwan, M. N. H. Muzaffar Alfian, and M. S. Mohamad Adenan, "Smart Door Lock," *Int. J. Recent Technol. Appl. Sci.*, vol. 3, no. 1, pp. 1–15, Mar. 2021, doi: 10.36079/lamintang.ijortas-0301.194.

[2] A. S. Ariffin and N. Harum, "Smart Door Lock System by Using Face Recognition," in *Conf. Bus. Soc. Sci. Technol. (CoNeScINTech)*, vol. 3, no. 1, pp. 46–55, Aug. 2023.

[3] R. Saputra and N. Surantha, "Smart and real-time door lock system for an elderly user based on face recognition," *Bull. Electr. Eng. Inform.*, vol. 10, no. 3, pp. 1345–1355, Jun. 2021, doi: 10.11591/eei.v10i3.2955.

[4] A. C. Frobenius, J. Kuswanto, R. Ardiansyah, and F. W. Y. Untoro, "Perancangan Prototipe Kunci Pintu Digital Berbasis IoT Menggunakan Metode HDLC," *Jambura J. Electr. Electron. Eng.*, vol. 5, no. 2, pp. 148–156, 2023.

[5] R. Rizky et al., "Penerapan Metode Fuzzy Sugeno Untuk Pengukuran Keakuratan Jarak Pada Pintu Otomatis di CV Bejo Perkasa," *J. Tek. Inform. Unika St. Thomas (JTIUST)*, vol. 5, no. 1, 2020.

[6] N. U. Putri et al., "Pelatihan Doorlock Bagi Siswa/Siswi Mas Baitussalam Miftahul Jannah Lampung Tengah," *J. Technol. Soc. Community Serv. (JTSCS)*, vol. 3, no. 2, pp. 198–203, 2022.

[7] P. E. S. Dita, A. A. Fahrezi, P. Prasetyawan, L. Ratu, and B. Lampung, "Sistem Keamanan Pintu Menggunakan Sensor Sidik Jari Berbasis Mikrokontroller Arduino UNO R3," *J. Tek. Sist. Komput. (JTIKOM)*, vol. 2, no. 1, 2021.

[8] A. Z. Rohman, Sunardi, and A. Munazilin, "Rancang Bangun Smart Door Lock Menggunakan Fingerprint dan Mikrokontroler Arduino Uno di BMT NU Jangkar," *G-Tech: J. Technol. Appl.*, vol. 7, no. 4, pp. 1245–1253, Oct. 2023, doi: 10.33379/gtech.v7i4.3029.

[9] A. H. Bachtiar, P. P. Surya, and R. P. Astutik, "Rancang Bangun Dual Keamanan Sistem Pintu Rumah Menggunakan Pengenalan Wajah dan Sidik Jari Berbasis IoT (Internet of Things)," *J. POLEKTRO: J. Power Electron.*, vol. 11, no. 1, 2022.

[10] E. Z. Orji, U. I. Nduanya, and C. V. Oleka, "Microcontroller Based Digital Door Lock Security System Using Keypad," *Int. J. Latest Technol. Eng. Manag. Appl. Sci. (IJLTEMAS)*, vol. 8, no. 1, pp. 92–97, 2019.

[11] R. Wahyuni, Y. Irawan, and Z. P. Noviardi, "Alat Pengaman Pintu Dengan Password Menggunakan Arduino Uno at Mega 328p dan Selenoid Door Lock," *J. Inform. Manaj. Komput.*, vol. 12, no. 1, 2020.

[12] R. Suwartika and G. Sembada, "Perancangan Sistem Keamanan Menggunakan Solenoid Door Lock Berbasis Arduino Uno pada Pintu Laboratorium di PT. XYZ," *J. E-Komtek (Electro-Comput. Technol.)*, vol. 4, no. 1, pp. 62–74, Jun. 2020, doi: 10.37339/e-komtek.v4i1.217.

[13] A. Salam and S. B. Bhaskoro, "Sistem Keamanan Cerdas pada Kunci Pintu Otomatis menggunakan Kode QR," *Cybern.*, vol. 5, no. 1, pp. 1–11, 2021.

[14] I. T. Maulana, "Penerapan Metode SDLC (System Development Life Cycle) Waterfall Pada E-Commerce Smartphone," *J. Ilm. Sist. Inform. Ilmu Komput.*, vol. 2, no. 2, pp. 1–6, 2022.

[15] F. Asrin and G. V. Utami, "Implementing Website-Based School Information Systems in Public Elementary Schools Using Waterfall Model," *J. Inf. Syst. Inform.*, vol. 5, no. 2, pp. 590–614, May 2023, doi: 10.51519/journalisi.v5i2.495.

[16] B. M. Sidhunata et al., "Point of Sales (POS) System Design using Design Thinking Framework for Motorcycle Workshop," *J. Inf. Syst. Inform.*, vol. 5, no. 3, pp. 874–886, Aug. 2023, doi: 10.51519/journalisi.v5i3.515.