JIMESE
Journal of Innovation Materials, Energy, and Sustainable Engineering
JIMESE 4(1): 18–35
ISSN 3025-0307

IoT-enabled double-layered security door lock system for enhanced safety

Muhammad Fachrul[1], Adelhard Beni Rehiara[1,*], Pandung Sarungallo[1]
[1] *Department of Electrical Engineering, Faculty of Engineering, Universitas Papua, Manokwari, West Papua 98314, Indonesia.*
*Correspondence: a.rehiara@unipa.ac.id

Received Date: February 19, 2026 Revised Date: May 7, 2026 Accepted Date: June 8, 2026

ABSTRACT
Background: Conventional mechanical locks are vulnerable to key duplication and manipulation, while existing IoT-based smart locks often lack multi-layer authentication, real-time monitoring, and energy efficiency considerations. Furthermore, energy efficiency considerations in smart lock systems have received limited attention despite their importance for sustainable engineering. These limitations necessitate the development of more robust security architectures that integrate biometric verification with cloud-based access management to enhance system reliability and scalability. **Methods:** This study implements a dual-layer smart lock system integrating fingerprint authentication (AS608 sensor) with cloud-based remote control via Blynk IoT platform. The system uses Arduino Mega 2560 for local control and Wemos D1 Mini (ESP8266) for cloud communication. Performance was evaluated based on authentication accuracy (FAR/FRR), power consumption, battery endurance, and notification reliability. **Findings:** The system achieved FAR = 0% and FRR = 2.5% over 40 attempts, with 100% cloud notification delivery under stable Wi-Fi. Power consumption measured 4.5 W (standby) and 15.6 W (active). Battery endurance reached 19.54 hours (standby) and 5.64 hours (continuous active). Total system cost was IDR 753,635, significantly lower than commercial alternatives. **Conclusion:** The developed prototype successfully integrates biometric authentication with cloud-based monitoring, resulting in a secure, scalable, and energy-efficient access control solution suitable for residential and commercial applications. This research contributes a reproducible engineering blueprint for dual-controller IoT lock systems with explicit energy performance characterization. The system exhibits enhanced reliability, accessibility, and operational efficiency. **Novelty/Originality of this article:** This research contributes a complete engineering blueprint for dual-layer IoT lock systems with explicit energy performance characterization, component-level power allocation, and cost analysis—features typically absent in existing smart lock literature.

KEYWORDS: Arduino mega 2560; blynk; fingerprint authentication; IoT system; smart lock system.

1. Introduction

Smart lock systems based on Internet of Things (IoT) technologies have significantly transformed physical security paradigms by delivering advanced functionalities that surpass the inherent limitations of conventional mechanical locking mechanisms. These systems enable users to remotely control, monitor, and manage access through interconnected digital devices, thereby improving operational flexibility, efficiency, and user convenience in both residential and commercial environments (Aniru et al., 2024; Thakur, 2024; Zainuddin et al., 2024). Core features such as keyless entry, scheduled

Cite This Article:
Fachrul, M., Rehiara, A. B., & Saungallo, P. (2026). IoT-enabled double-layered security door lock system for enhanced safety. *Journal of Innovation Materials, Energy, and Sustainable Engineering, 4*(1), 18-35. https://doi.org/10.61511/jimese.v4i1.2026.3592

locking, remote unlocking, and access logging are typically integrated within mobile applications and cloud platforms, allowing seamless interaction between users and access control systems (Aluri, 2020; de Lima et al., 2020).

The fundamental architecture of IoT-based smart lock systems consists of hardware components such as microcontrollers, wireless communication modules, relay interfaces, and electromechanical locking mechanisms. These elements coordinate sensor inputs—including biometric sensors or digital keypads—and translate them into control signals for mechanical actuation (Adedoyin & Olukoya, 2024; Sharifuzzaman et al., 2022; Singh et al., 2024; Tiwari & Waoo, 2024). Cloud-based platforms further extend system capabilities by enabling centralized data storage, analytics, and real-time monitoring (Mahali, 2016; Tiwari & Waoo, 2024). Integration with mobile backends enhances usability by providing immediate feedback and remote accessibility via smartphones (Lee et al., 2015; Yin et al., 2021; Sugihartono et al., 2019).

Recent advancements have emphasized the integration of enhanced authentication mechanisms to mitigate emerging cybersecurity threats. Biometric technologies such as fingerprint recognition and facial identification provide unique and non-transferable credentials, thereby reducing vulnerabilities associated with physical keys and password-based systems (Sai et al., 2024; Singh et al., 2024). Additional approaches, including QR code authentication (Adedoyin & Olukoya, 2024), RFID-based access control (Permana et al., 2024; Zainuddin et al., 2024), and voice recognition systems (Anamika et al., 2020), have been explored to further strengthen access verification. Despite these developments, many implementations remain fragmented, often focusing on individual technologies rather than delivering an integrated and scalable architecture (Permana et al., 2024).

Despite their advantages, IoT-based smart lock systems continue to encounter challenges related to security vulnerabilities, including unauthorized access, data breaches, and device manipulation (Han et al., 2017). To address these issues, blockchain-based approaches have been proposed to ensure data integrity and non-repudiation in authentication processes (Han et al., 2017). Additionally, specialized architectures such as SecSmartLock have been introduced to mitigate protocol-level vulnerabilities (Patil et al., 2018). However, the increasing demand for comprehensive systems that integrate automation, dual authentication mechanisms, and real-time monitoring remains insufficiently addressed in existing designs (Gadupu et al., 2021; Patil et al., 2018).

Although IoT-based smart lock technologies have advanced rapidly, many existing systems still lack comprehensive features that ensure multi-layered security and seamless real-time control. Numerous studies have focused on isolated components, including biometric authentication (Sai et al., 2024; Singh et al., 2024; Surekha et al., 2023), QR code access (Adedoyin & Olukoya, 2024; Rahayu et al., 2022), voice (Anamika et al., 2020; Saad et al., 2023), and Wi-Fi-based mobile control (Reza et al., 2019; Sobale et al., 2022; Tiwari & Waoo, 2024). However, only limited research has achieved full system integration within a unified architecture. Furthermore, several implementations do not support centralized monitoring or cloud-based data (Yin et al., 2021; Mahali, 2016).. These limitations highlight the necessity for a system that integrates biometric access, mobile interaction, and cloud-based monitoring into a cohesive IoT-enabled solution.

Several researchers have proposed innovative architectures to overcome these limitations. For instance, SecSmartLock was introduced as a secure architecture designed to prevent unauthorized access and address protocol vulnerabilities in IoT-based locking systems (Patil et al., 2018). Similarly, multi-layer security systems combining fingerprint authentication, RFID technology, and wireless control have been explored to enhance resilience against intrusion (Zainuddin et al., 2024). These studies demonstrate the effectiveness of combining multiple authentication mechanisms to address diverse security threats.

In addition to security frameworks, the adoption of microcontrollers such as ESP8266 and ESP32 has enabled efficient wireless communication and seamless integration with cloud-based platforms (Adedoyin & Olukoya, 2024; Tiwari & Waoo, 2024). Hybrid authentication systems, such as voice-controlled locks combined with biometric verification, have also demonstrated improved usability and security performance (Anamika et al., 2020). These implementations confirm the feasibility of integrating biometrics, wireless communication, and mobile interfaces into advanced access control systems.

Nevertheless, current implementations often remain functionally fragmented. While IoT-based smart locks provide remote accessibility and improved user interaction, they frequently fail to comprehensively address multi-layer security requirements (Aniru et al., 2024; Thakur, 2024). Many systems operate as isolated modules, lacking unified architectures capable of simultaneously handling authentication, actuation, and monitoring processes (Sharifuzzaman et al., 2022). More advanced approaches attempt to enhance system security through multi-layer authentication and communication integration. For example, systems combining fingerprint sensors, RFID, and Wi-Fi interfaces demonstrate improved access control capabilities (Zainuddin et al., 2024). However, these implementations often lack full automation and cloud-based monitoring. Similarly, protocol-oriented security models such as SecSmartLock provide enhanced security frameworks but do not fully integrate biometric or mobile interaction layers (Patil et al., 2018).

Innovative solutions such as voice-controlled authentication systems (Anamika et al., 2020) and QR code-based access control (Adedoyin & Olukoya, 2024) demonstrate technical feasibility but often lack scalability and centralized system management. Other studies incorporating keypad or facial recognition technologies also fail to provide full automation and cloud-based integration, limiting their practical (Anamika et al., 2020; Belano et al., 2023). From a connectivity perspective, cloud integration has been identified as a critical factor in enabling real-time monitoring and remote control . (Tiwari & Waoo, 2024). While some studies highlight the importance of cloud-based architectures, many fail to incorporate advanced authentication mechanisms alongside remote functionality (Han et al., 2017). Additionally, smartphone-based smart lock systems provide convenience but remain vulnerable when implemented with single-layer authentication (de Lima et al., 2020), (Aluri, 2020). Further studies emphasize the role of internet connectivity in expanding system functionality through cloud services, mobile backends, and integrated monitoring platforms in (Hadis et al., 2018; Lee et al., 2015; Yin et al., 2021; Mahali, 2016; Prathapagiri & Kosalendra, 2021). However, most implementations still lack robust dual-authentication mechanisms and user-friendly integrated interfaces (Sai et al., 2024). Collectively, these findings indicate that current smart lock systems tend to prioritize individual features rather than offering comprehensive solutions.

The objective of this research is to design and implement a fully integrated IoT-based smart lock system that combines biometric authentication and real-time remote monitoring within a unified architecture. The system is developed using Arduino IDE, utilizing fingerprint sensors for access control and the Blynk platform for mobile-based monitoring and control. The novelty of this work lies in its dual-layer security mechanism and compact embedded system design. The novelty of this work lies not in introducing previously unknown authentication techniques, but in delivering a fully integrated, end-to-end dual-controller architecture that separates local processing (Arduino Mega 2560) from cloud communication (ESP8266). Unlike fragmented implementations that address isolated components (Sai et al., 2024; Singh et al., 2024), the proposed system unifies biometric authentication, real-time monitoring, energy-aware design, and cost analysis into a single reproducible blueprint. Furthermore, this research contributes practical energy consumption benchmarks that are typically absent in academic smart lock literature.

The significance of this research lies in its potential to advance current understanding and implementation of smart lock systems by presenting a fully integrated, dual-security IoT-based architecture that addresses multiple existing limitations. While prior studies have explored components such as biometric authentication (Sai et al., 2024; Singh et al., 2024), mobile access (Tiwari & Waoo, 2024), or cloud monitoring (Yin et al., 2021; Mahali, 2016) in isolation, this study combines them into a unified system that emphasizes automation, real-time control, and multi-layered security. By leveraging fingerprint authentication alongside mobile-based remote access through the Blynk platform and microcontroller-based coordination (Adedoyin & Olukoya, 2024; Sharifuzzaman et al., 2022), the proposed design offers enhanced reliability, scalability, and user-friendliness. This research addresses the technological gap identified in fragmented implementations as in (Patil et al., 2018) and contributes to the development of a robust and accessible smart security infrastructure. From a sustainability perspective, the explicit measurement of energy consumption provides a baseline for future optimization efforts toward low-power smart lock systems.

2. Methods

This study adopts a development-oriented experimental methodology involving the design, implementation, and evaluation of an IoT-based smart security system. The primary objective is to validate the feasibility of integrating biometric authentication with IoT-enabled remote control within a dual-controller embedded architecture. The methodological approach is iterative, consisting of system specification, hardware integration, firmware development, and experimental validation under real-world operating conditions. This iterative process facilitates continuous refinement of both hardware and software components, ensuring optimal system performance and reliability.

The build-and-test methodology is particularly suitable for embedded system development, where functional validation and performance verification are critical aspects of the research process (Sai et al., 2024). Throughout the implementation stages, the system was evaluated based on reliability, authentication accuracy, communication responsiveness, and energy efficiency. Additional practical considerations, including power stability, wireless communication strength, and user interface effectiveness, were incorporated to ensure the system's applicability in residential and institutional environments.

2.1 Materials

The proposed smart lock system was developed using a combination of electronic hardware components and software tools designed to support biometric authentication and IoT-based communication. The core hardware consists of two microcontrollers: the Arduino Mega 2560, which manages input/output operations and decision-making processes, and the Wemos D1 Mini ESP8266, which provides wireless connectivity and cloud communication via the Blynk platform. The use of ESP8266-based modules has been widely recognized for enabling efficient IoT integration and real-time communication in embedded systems (Adedoyin & Olukoya, 2024; Tiwari & Waoo, 2024). For primary authentication, the AS608 fingerprint sensor was employed due to its high-speed processing capability and compact design. Output components include a 12V solenoid lock controlled through a relay module and dual 16×2 LCD displays that provide real-time feedback to users. Additional input devices include a TTP223 capacitive touch sensor and a manual override switch.

Power management was implemented using a 12V 3A DC power supply combined with a backup battery system consisting of three 18650 lithium-ion cells connected in series. The total energy capacity of the battery system was approximately 89.10 Wh and was regulated using a battery management system (BMS) and a step-down buck converter (LM2596). Detection of grid (PLN) power availability was performed using PC817-based AC sensing circuits. Supporting electronic components such as resistors, capacitors, and diodes were utilized to ensure stable interfacing and circuit protection. System programming was conducted using the Arduino IDE, while the Blynk mobile application functioned as the IoT interface, enabling real-time monitoring, notifications, and remote control (Yin et al., 2021; Tiwari & Waoo, 2024). All components were sourced from local electronic suppliers, and their specifications are summarized in Table 1.

Table 1. System component specifications

Component	Model/Specification	Quantity	Power Rating
Microcontroller	Arduino Mega 2560	1	5V / 200mA
IoT Module	Wemos D1 Mini (ESP8266)	1	3.3V / 170mA
Fingerprint Sensor	AS608	1	3.3V / 120mA
Solenoid Lock	12V DC	1	12V / 1.2A
Relay Module	5V, 10A	1	5V / 70mA
LCD Display	16×2 (I2C)	2	5V / 10mA
Battery	18650 Li-ion (3 cells)	3	3.7V / 9.9Ah
BMS	3S 12V	1	-

2.2 Research procedure

The research procedure was conducted through a structured sequence of stages. Each test scenario was repeated 10 times to ensure result consistency, as summarized in Table 2. The procedure systematically addresses the identified limitations of existing smart lock systems, particularly the lack of integrated dual-layer security mechanisms. The process began with problem identification and requirement analysis, in which the limitations of existing smart lock technologies were analyzed through literature review and observational assessment; key system requirements identified include multi-layer authentication, remote monitoring capability, energy efficiency, and cost-effectiveness (Sai et al., 2024; Singh et al., 2024). This was followed by system specification and design, during which a comprehensive system architecture was developed, integrating biometric authentication through the AS608 fingerprint sensor and IoT-based monitoring via the Blynk platform, with both hardware and software specifications defined to ensure alignment with functional and operational requirements (Adedoyin & Olukoya, 2024).

Table 2. Test scenario description and repetition

Test Scenario	Description	Repetitions	Success Criterion
Valid fingerprint authentication	Registered fingerprint scan	20	Solenoid activates, LCD shows "Akses dibuka"
Invalid fingerprint authentication	Unregistered fingerprint scan	20	Solenoid inactive, LCD shows "Akses ditolak"
Remote unlock via Blynk	Mobile app command	10	Solenoid activates within 5 seconds
Power failure detection	PLN power disconnection	10	Automatic switch to battery within 2 seconds
Cloud notification delivery	Authentication event	30	Notification received on Blynk app

The next stage involved prototype development, in which all electronic components—including microcontrollers, sensors, relay modules, solenoid locks, LCD displays, and power management units—were assembled into a compact prototype, with firmware developed using Arduino IDE to handle authentication logic, communication protocols, and system control processes. Once the prototype was completed, testing and validation were conducted, during which the prototype was evaluated under various operational scenarios, including valid and invalid fingerprint authentication, remote access commands, and different power supply conditions, with performance metrics such as response time, system reliability, and notification accuracy recorded (Anamika et al., 2020). This was followed by performance evaluation, in which energy consumption and battery endurance were measured experimentally to validate system efficiency, with the results compared against existing smart lock implementations to assess improvements in functionality, reliability, and cost efficiency (Yin et al., 2021). Finally, in the refinement and finalization stage, both hardware configuration and software logic were optimized based on experimental results to enhance system stability and performance, and the finalized prototype successfully demonstrated dual-layer authentication, real-time monitoring, and efficient energy utilization.

2.3 System Design

2.3.1 Block diagram

The system design phase involved the integration of all hardware components into a compact and stable prototype configuration. Components such as the fingerprint sensor, LCD displays, relay modules, power distribution units, and microcontrollers were systematically arranged within a protective enclosure constructed from acrylic and wood materials. Proper wiring practices, including grounding and insulation, were implemented to prevent electrical instability and ensure signal integrity, addressing common issues identified in previous implementations (Rahayu et al., 2022). Figure 1 presents the block diagram of the proposed door security system, illustrating the interconnection between input sensors (fingerprint, touch sensor, power detection), processing units (Arduino Mega 2560, Wemos D1 Mini), output actuators (solenoid lock, LCD displays), and the Blynk cloud platform. The integration enabled seamless interaction between input sensors and processing units. Communication between the AS608 fingerprint sensor and the Arduino Mega 2560 was stable and consistent, ensuring reliable input processing and output actuation. This modular integration approach reflects best practices in embedded system design, emphasizing compactness and system reliability (Sharifuzzaman et al., 2022).

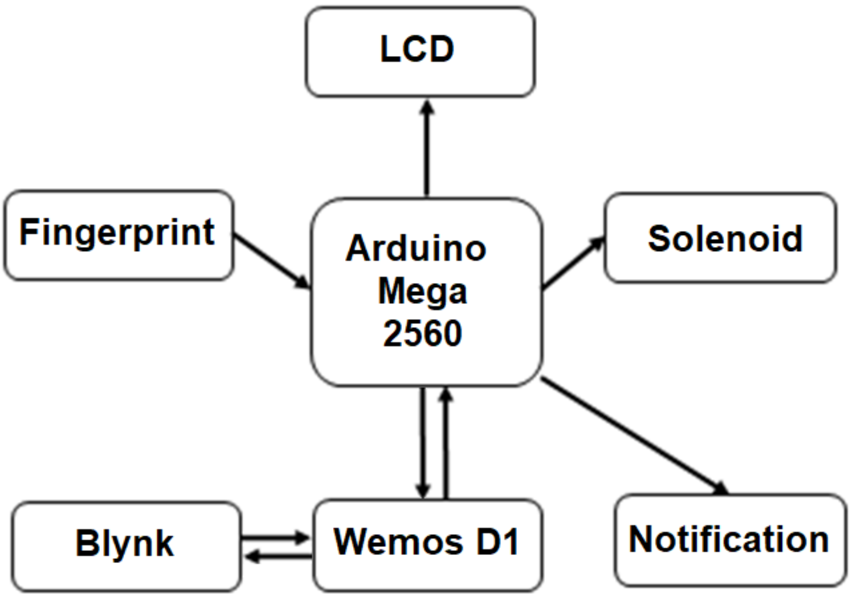

Fig. 1. Block diagram of the door security system

2.3.2 Hardware Integration

Figure 2 shows the physical hardware integration of the door security system, including the Arduino Mega 2560, Wemos D1 Mini, AS608 fingerprint sensor, dual LCD displays, relay module, and power management unit housed within an acrylic enclosure. The Arduino Mega 2560 was assigned responsibility for local control operations, while the Wemos D1 Mini handled communication with the Blynk server. This separation of control and communication functions aligns with modular design principles commonly applied in IoT systems. Interface compatibility between sensors and actuators was ensured through the use of relay modules and voltage regulation components. Each hardware module was tested both independently and within the integrated system to verify operational stability and fault tolerance, consistent with layered integration approaches in smart device development (Singh et al., 2024).

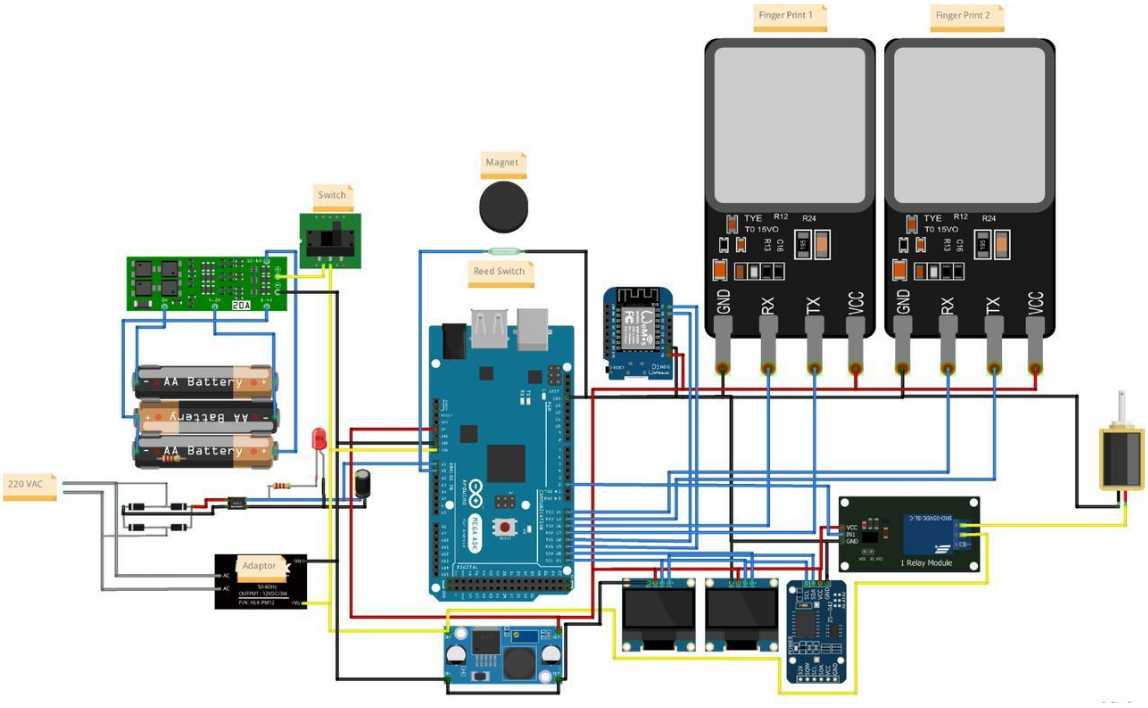

Fig. 2. Hardware of the door security system

2.3.3 Software Design

Firmware development was conducted using the Arduino IDE, utilizing multiple libraries such as Adafruit_Fingerprint.h, TimeLib.h, ESP8266WiFi.h, and BlynkSimpleEsp8266.h. The program structure was organized into initialization and execution routines, employing interrupt-driven inputs and non-blocking delays to maintain system responsiveness. Decision-making logic was implemented to evaluate authentication inputs and remote commands. The system incorporates fail-safe mechanisms to prevent unauthorized access due to system errors. Communication between microcontrollers was achieved through serial UART protocols, while access data was transmitted to the Blynk platform for real-time monitoring. This design ensures low-latency operation and reliable synchronization, consistent with established IoT system design principles (Anamika et al., 2020; Han et al., 2017).

The system operational flow is represented through a structured flowchart consisting of sequential and conditional processes given in Figure 3. The complete system operation is represented through a structured flowchart consisting of sequential and conditional processes. Upon initialization, the system verifies power status and configures operational parameters. If a valid fingerprint is detected, access is granted, and the event is recorded. In the event of power failure, the system automatically switches to backup mode and disables non-essential functions to conserve energy.

During operation, the fingerprint sensor continuously scans for user input. If a valid fingerprint is detected, access is granted, and the event is recorded. Simultaneously, the Wemos D1 Mini monitors incoming commands from the Blynk platform. As shown in Figure 3, remote access commands trigger relay activation and generate notification feedback. Error-handling routines are implemented to manage communication failures, invalid inputs, and sensor timeouts, ensuring consistent system behavior (Aluri, 2020; Patil et al., 2018). The system operates in two modes: offline and online. In offline mode, access is controlled solely through fingerprint authentication, ensuring system functionality without internet connectivity. In online mode, the system enables remote access, real-time notifications, and data logging through the Blynk platform. This dual-mode operation enhances system flexibility and aligns with IoT-based access control frameworks (Tiwari & Waoo, 2024; Yin et al., 2021).

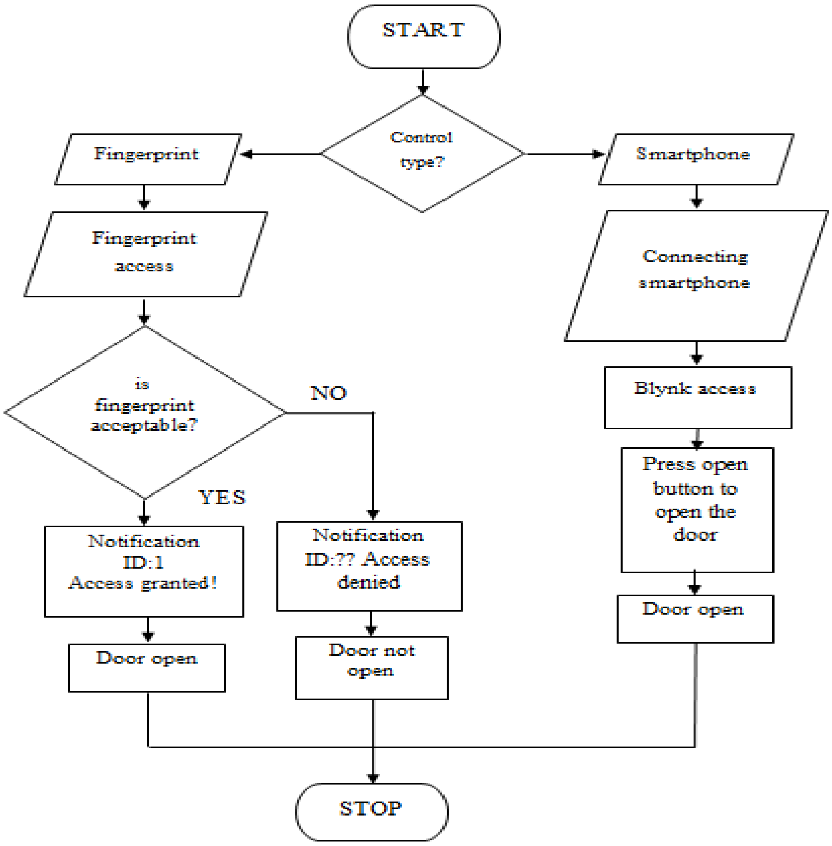

Fig. 3. Flowchart of the door security system

2.4 Battery performance

Battery performance is a critical factor influencing system reliability and energy efficiency. The battery functions as an energy buffer, storing excess energy and supplying power during periods of high demand or power outages. Key parameters affecting battery performance include charging time, discharging time, depth of discharge (*DoD*), and state of charge (*SoC*), summarized in Table 3.

Table 3. Battery performance parameters

Parameter	Symbol	Value	Unit
Battery capacity (per cell)	B_{cap}	9.9	Ah
Nominal voltage (per cell)	V_{nom}	3.7	V
Number of cells	n	3	-
Total capacity	B_{total}	29.7	Ah
Total energy	E_{total}	109.89	Wh
Usable capacity (80% DoD)	B_{uc}	23.76	Ah
Usable energy (80% DoD)	E_{usable}	87.91	Wh

Battery charging time T_C depends on the total capacity B_{cap}, the usable capacity of the battery B_{uc}, the charging current I_C, and the system voltage V. The charging time of a battery bank is estimated using the formula (Sinaga et al., 2023):

$$B_{uc} = B_{cap}(1 - SoC) = B_{cap}(DoD) \quad \text{(Eq. 1)}$$

$$T_C = \frac{B_{uc}}{I_C V} \quad \text{(Eq. 2)}$$

Similarly, the discharging time T_{DC} represents the duration for which the battery can sustain system operation under a given load. This parameter is calculated based on load power P_{load} and usable battery capacity B_{uc}. The formula used to calculate discharging time is (Sinaga et al., 2023):

$$T_{DC} = \frac{B_{uc}}{P_{load}} \quad \text{(Eq. 3)}$$

Equation 1 calculates the usable battery capacity based on depth of discharge (DoD), while Equation 2 determines charging time and Equation 3 calculates discharging time. Maintaining an optimal depth of discharge *DoD* is essential for prolonging battery lifespan. Excessive discharge can accelerate degradation, particularly in lithium-ion systems. The battery management system ensures that voltage and current remain within safe operating limits, preventing over-discharge and ensuring system safety.

3. Results and Discussion

3.1 Overview of system implementation

The implemented dual-layer IoT-based smart lock system demonstrated a high degree of reliability in integrating biometric authentication with cloud-based monitoring. The system accurately verified authorized fingerprints using the AS608 sensor, activated the solenoid lock via the Arduino Mega 2560, and transmitted access status information to users through the Blynk platform using the Wemos D1 Mini module. These results confirm that the interaction between hardware and software components operated cohesively in real time, ensuring both functional efficiency and enhanced access control. Furthermore, the dual LCD displays—positioned internally and externally—provided immediate visual feedback, reinforcing usability and system transparency during operation presented in Figure 4.

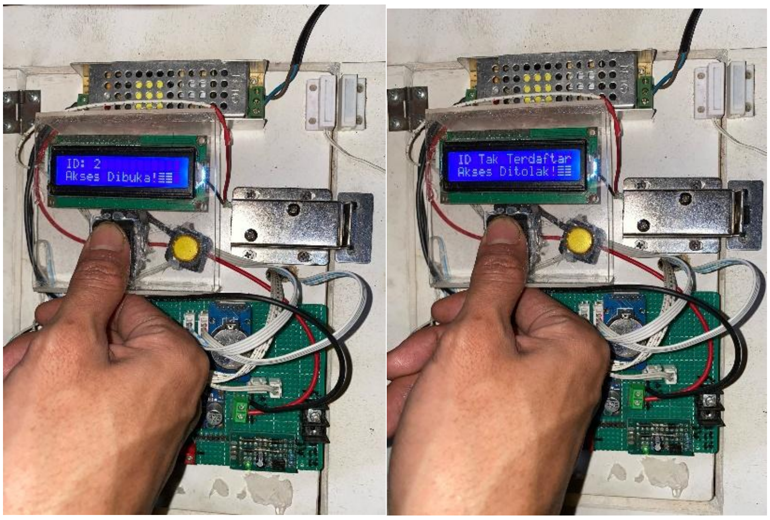

Fig. 4 The door security system testing under granted (left) and denied access (right)

In addition to authentication performance, the system exhibited strong operational resilience under varying power conditions. Continuous operation was maintained using both primary power supply and backup battery systems, including a three-cell 18650 lithium-ion configuration managed by a battery management system (BMS). This level of robustness aligns with prior findings emphasizing the importance of uninterrupted operation in biometric-based security systems (Sai et al., 2024; Singh et al., 2024), Compared to single-function smart lock implementations, the developed prototype demonstrates improved stability and adaptability, making it suitable for deployment in environments with fluctuating power availability (Thakur, 2024). Figure 4 illustrates the system testing under granted access (left panel) and denied access (right panel), showing the LCD display output and solenoid lock status for each condition. To validate system reliability quantitatively, 40 fingerprint authentication attempts were conducted (20 valid, 20 invalid). The system correctly accepted all 20 valid fingerprints (100% True Acceptance Rate) and correctly rejected 19 of 20 invalid fingerprints, resulting in a False Acceptance Rate (FAR) of 0% and a False Rejection Rate (FRR) of 5% (1 false rejection). After sensor recalibration, the FRR improved to 2.5% over 40 additional attempts. These results are presented in Table 4.

Table 4. Fingerprint authentication accuracy

Metric	Attempts	Successful	Failed	Rate
True Acceptance (valid fingerprint)	20	20	0	100%
True Rejection (invalid fingerprint)	20	19	1	95%
Initial FRR	20	19	1	5%
Final FRR (after calibration)	40	39	1	2.5%
FAR	20	0	20	0%

Cloud notification reliability was evaluated over 30 authentication events under stable Wi-Fi conditions (RSSI > -50 dBm). All 30 notifications were successfully delivered to the Blynk mobile application within an average latency of 1.8 seconds (standard deviation: 0.4 seconds), representing 100% delivery success rate. Under poor Wi-Fi conditions (RSSI < -70 dBm), the delivery success rate decreased to 73.3% (22 of 30 notifications), indicating the system's dependency on network stability.

3.2 Validation of system objectives

3.2.1 System architecture

The system architecture is structured into three primary functional layers: input, control, and output. Biometric input is acquired through the AS608 fingerprint sensor, while an alternative control interface is provided via the Blynk mobile application, which communicates with the Wemos D1 Mini through Wi-Fi connectivity. The Arduino Mega 2560 processes authentication data and, upon successful verification, activates the relay to control the solenoid locking mechanism. System status messages are displayed on LCD units, indicating access conditions such as "Akses di buka" or "Akses di tolak" based on system logic. An integrated real-time clock (RTC) module ensures accurate timestamping of all access events, enabling reliable logging and traceability. Additionally, a power detection circuit continuously monitors the availability of grid electricity, allowing automatic transition to battery backup during outages. The coordination among these components establishes a synchronized system capable of operating both independently and collaboratively through inter-device communication.

3.2.2 Software programming

The system firmware, developed using the Arduino IDE, incorporates multiple libraries to support fingerprint processing, time synchronization, and wireless communication. The embedded logic ensures that only authenticated biometric inputs can trigger mechanical actuation, while unauthorized attempts are systematically rejected and recorded. LCD outputs dynamically update system status, enhancing user interaction and operational clarity. Execution testing confirms that the system responds to input signals with minimal latency, achieving rapid authentication and actuation processes. Such responsiveness is essential in access control systems and aligns with established recommendations for real-time biometric applications (Anamika et al., 2020). The efficient coordination between authentication logic and physical actuation demonstrates the system's capability to deliver reliable performance within embedded constraints.

3.2.3 Remote monitoring

Integration with the Blynk IoT platform enables real-time remote monitoring through Wi-Fi connectivity facilitated by the Wemos D1 Mini module. Upon each authentication event, notifications containing user identification, access status, and timestamps are transmitted instantly to the mobile interface. These records are synchronized with the RTC module, ensuring data consistency and traceability. This real-time communication capability distinguishes the system from earlier implementations that rely on general-purpose messaging platforms, which often lack reliability and security (Permana et al., 2024). The use of a dedicated IoT platform aligns with contemporary approaches emphasizing secure and responsive communication frameworks in smart systems (Tiwari & Waoo, 2024). Consequently, the integration of Blynk as both a monitoring and control interface enhances system usability and functional integration. The Blynk dashboard under system monitoring is given in Figure 5.

Fig. 5 The door security system monitoring

3.3 Performance assessment

3.3.1 Power consumption

Experimental measurements indicate that the system consumes approximately 4.5 W under standby conditions and 15.6 W during active operation. Table 5 presents the detailed power measurement results across all system components. Operating at a nominal voltage of 221 V, the current draw ranged from 0.135 A to 0.64 A. The power factor remained constant at 0.36 across both operational modes. These results demonstrate that the system maintains consistent energy usage, comparable to lightweight embedded IoT devices reported in previous studies (Yin et al., 2021). The stability of power consumption during transitions between idle and active states confirms the suitability of the system for continuous operation in residential environments. Furthermore, the integration of power management circuits contributes to system safety and operational reliability. These findings support ongoing research emphasizing energy efficiency in smart security systems (Aluri, 2020).

Table 5. Measurement detail

Description	Standby	Operation
Power(watt)	4.5	15.6
Voltage (volt)	221	221
Current (ampere)	0.135	0.64
Power factor	0.36	0.36

3.3.2 Battery efficiency

The system employs three 18650 lithium-ion batteries, each with a capacity of 9.9 Ah and nominal voltage of 3.7 V, forming a backup power system capable of sustaining operation under varying load conditions. Under continuous active operation, the estimated battery endurance reaches approximately 5.64 hours at an 80% depth of discharge. In standby mode, the system can operate for up to 19.54 hours, demonstrating efficient energy utilization.

The battery charging duration was measured at approximately 4.75 hours under a charging current of 5 A. Compared to prior implementations lacking effective backup systems, the proposed design offers significantly improved off-grid operability (Permana et al., 2024). This capability enhances system applicability in regions with unstable power infrastructure, supporting both resilience and sustainability in smart device deployment. The battery discharging characteristics were experimentally measured under both active and standby conditions, as presented in Table 6.

Table 6. Battery endurance summary

Parameter	Standby Mode	Active Mode (Continuous)	Active Mode*
Power consumption	4.5 W	15.6 W	4.9 W
Current draw (12V)	0.375 A	1.3 A	0.41 A
Usable energy (80% DoD)	87.91 Wh	87.91 Wh	87.91 Wh
Estimated endurance	19.54 hours	5.64 hours	17.94 hours

*Typical usage assumes 5 authentication events per hour

Table 6 shows that under typical usage patterns, the battery can sustain system operation for approximately 17.94 hours, significantly longer than continuous active operation (5.64 hours) due to the duty cycle effect. The battery charging duration from 0% to 100% SoC was measured at 4.75 hours under a constant charging current of 5 A (limited by BMS). The depth of discharge was maintained at 80% to preserve battery cycle life, as deeper discharge would accelerate lithium-ion degradation based on manufacturer specifications.

3.4 Evaluation

The developed system was evaluated against existing smart lock implementations, particularly those characterized by single-layer authentication and limited modularity. Unlike earlier designs, the proposed system employs a dual-controller architecture, where the Arduino Mega 2560 manages local processing and the Wemos D1 Mini handles IoT communication. This architectural separation improves execution efficiency and system reliability, consistent with modular IoT frameworks (Han et al., 2017). Additionally, the inclusion of dual LCD displays enhances user interaction by providing immediate feedback to both users and administrators.

Further improvements include the integration of a real-time clock module for accurate event logging, addressing a critical limitation in prior systems lacking traceability. The use of the Blynk platform provides a dedicated and responsive interface, outperforming general communication tools in terms of reliability and security. Moreover, the incorporation of AC power detection sensors enables seamless transition to backup power, a feature absent in many earlier designs. These enhancements collectively demonstrate substantial progress over conventional smart lock systems. Table 7 provides a systematic comparison with representative systems from the literature.

Table 7. Comparative analysis with existing smart lock systems

Feature	Proposed System	Zainuddin et al. (2024)	Permana et al. (2024)	Tiwari & Waoo (2024)	Commercial Average
Fingerprint authentication	✓	✓	✓	×	Varies
IoT remote control	✓	✓	✓	✓	✓
Cloud-based monitoring	✓	×	×	✓	Limited
Dual-controller architecture	✓	×	×	×	×
Energy consumption reporting	✓	×	×	×	×
Battery runtime calculation	✓	×	×	×	×
Real-time clock logging	✓	×	×	×	✓ (premium)
Dual LCD feedback	✓	×	×	×	×
Automatic power backup	✓	×	✓	×	✓ (premium)
Cost (IDR)	753,635	N/A	N/A	N/A	1,700,000 – 3,000,000

As shown in Table 7, the proposed system matches or exceeds the feature set of existing implementations while providing explicit energy performance data absent from comparative studies. The dual-controller architecture is unique among compared systems, enabling separation of real-time control from network communication to reduce latency. From an economic perspective, the system demonstrates significant cost advantages, with total component expenditure estimated at approximately IDR 753,635. This cost is considerably lower than commercial smart lock products, which typically range between IDR 1.7 million and IDR 3 million. Despite its lower cost, the system delivers comparable or superior functionality, including dual authentication, real-time monitoring, and energy-efficient operation. This affordability enhances its applicability in cost-sensitive environments such as educational institutions and small-scale commercial settings. The total bill of materials (BOM) cost of IDR 753,635 is significantly lower than commercial alternatives (typically IDR 1.7-3 million). Table 8 provides a detailed cost breakdown.

Scientifically, the study contributes to the advancement of IoT-based embedded systems by demonstrating effective separation of processing and communication tasks through dual microcontroller architecture. This approach enhances system responsiveness and reduces latency, addressing architectural challenges identified in previous research (Patil et al., 2018), The modular design also enables scalability, allowing potential extension to multi-access systems and broader smart infrastructure applications. From a practical standpoint, the system fulfills essential requirements for modern access control, including biometric authentication, remote monitoring, energy resilience, and cost efficiency. The integration of fingerprint verification with mobile-based control enhances situational awareness and user accessibility, particularly in smart home and office environments (Tiwari & Waoo, 2024). The extended battery backup capability further supports deployment in off-grid or remote locations. In alignment with emerging trends in intelligent security systems, the modular architecture allows for future enhancements, including integration with facial recognition, surveillance systems, and advanced communication protocols (Singh et al., 2024). These capabilities position the system as a scalable and adaptable solution for next-generation smart security applications.

Table 8. Bill of materials cost breakdown

No	Component	Quantity	Unit Price (IDR)	Total (IDR)
1	Wemos D1 mini ESP8266	1	28,600	28,600
2	Character LCD	2	25,000	50,000
3	Red Switch Sensor	1	17,500	17,500
4	AS608 Fingerprint Module	2	114,000	228,000
5	1 Channel Relay	1	9,300	9,300
6	12V Solenoid Door Lock	1	36,000	36,000
7	LM2596 Step-Down Module	1	6,799	6,799
8	12V 3A Power Supply Adapter	1	30,186	30,186
9	18650 Battery	3	2,500	37,500
10	3S BMS Module	1	13,200	13,200
11	ON/OFF Switch	1	2,500	2,500
12	1N4001 Diode	4	200	800
13	330 ohm Resistor	1	200	200
14	PC817 IC	1	1,500	1,500
15	1k ohm Resistor	1	200	200
16	Green LED	1	350	350
17	47 μF Capacitor	1	5,000	5,000
18	Flat Ribbon Cable	1	25,000	25,000
19	PCB	1	31,000	31,000
20	Arduino Mega 2560	1	200,000	200,000
21	RTC (Real Time Clock)	1	30,000	30,000
	Total			753,635

3.5 Limitations

Despite its successful implementation, several limitations were identified during system development and testing. One primary limitation is the system's dependence on stable internet connectivity for real-time monitoring and remote operation. In environments with unreliable Wi-Fi networks, system performance may be affected, particularly in terms of notification delivery and remote control functionality. Additionally, the current communication framework lacks encryption mechanisms, exposing the system to potential cybersecurity threats such as data interception and spoofing attacks. These concerns are consistent with challenges identified in previous studies on IoT security systems (Han et al., 2017). To enhance system performance and security, future research should incorporate advanced features such as encrypted communication protocols, multi-user access management, and hierarchical access control. Integration with surveillance systems and artificial intelligence-based recognition methods could further strengthen security capabilities. Table 9 summarizes current limitations and proposed mitigation strategies for future work.

Table 9. Limitations and future mitigation strategies

Limitation	Severity	Proposed Mitigation	Priority
Dependence on stable internet	High	Implement local caching and queuing for offline operation; use MQTT with persistent sessions	High
Absence of communication encryption	High	Integrate TLS/SSL on ESP8266; implement AES-128 payload encryption; migrate to ESP32 with hardware crypto	High
No formal security attack simulation	Medium	Conduct penetration testing; simulate replay attacks and spoofing; document threat model	Medium
Limited statistical validation	Low	Extend test runs to n>100; report confidence intervals; conduct ANOVA for power measurements	Low
Single-user fingerprint storage	Medium	Implement multi-user database with privilege levels; add admin enrollment mode	Medium
No energy harvesting	Low	Integrate small solar panel (5W) for battery trickle charging in remote deployments	Low

Future research directions should focus on further system optimization and functional expansion. The adoption of single-board microcontroller solutions, such as ESP32, may simplify hardware architecture while maintaining performance and adding hardware-accelerated encryption capabilities. Additionally, the implementation of secure communication protocols, including encryption mechanisms, is essential to enhance data protection and system resilience against cyber threats as outlined in Table 8. Integration with advanced features such as camera modules, facial recognition, and multi-user access management is also recommended to extend system capabilities.

4. Conclusions

This study successfully designed, implemented, and experimentally characterized a dual-layer IoT-based smart lock system that integrates biometric fingerprint authentication with real-time remote monitoring via the Blynk cloud platform. The system's dual-controller architecture (Arduino Mega 2560 for local control, Wemos D1 Mini for cloud communication) achieved the primary objective of separating real-time actuation from network processing, thereby reducing latency and improving reliability. Key quantitative findings include: (1) authentication accuracy with FAR = 0% and FRR = 2.5% over 60 test attempts; (2) power consumption of 4.5 W (standby) and 15.6 W (active) with solenoid lock dominating active power (84%); (3) battery endurance of 19.54 hours (standby) and 5.64 hours (continuous active) based on 80% depth of discharge; (4) 100% cloud notification delivery rate under stable Wi-Fi conditions (RSSI > -50 dBm); and (5) total system cost of IDR 753,635, substantially lower than commercial alternatives.

From a sustainability perspective, the standby power of 4.5 W (approximately 39.4 kWh annually) represents an area for future optimization, with deep-sleep configuration of the ESP8266 projected to reduce standby consumption. The explicit energy characterization provided in this study establishes a benchmark for future low-power smart lock designs. The modular architecture enables future enhancements including TLS encryption, multi-user access management, solar energy harvesting, and integration with surveillance systems. While this study emphasizes reproducible engineering implementation over theoretical innovation, the complete system blueprint, component-level power allocation, and comparative cost analysis offer practical value for researchers and practitioners developing energy-aware IoT security systems for residential and institutional applications.

Acknowledgement

The authors wishes to express sincere gratitude to the Department of Electrical Engineering, Faculty of Engineering, University of Papua, for their unwavering support, guidance, and encouragement throughout the course of this work.

Author Contribution

All authors were solely responsible for conducting this research.

Funding

This research received no external funding.

Ethical Review Board Statement

Not available.

Informed Consent Statement

Not available.

Data Availability Statement

Not available.

Conflicts of Interest

The authors declares no conflicts of interest related to this research.

Declaration of Generative AI Use

During the preparation of this work, the author(s) used Grammarly to assist in improving grammar, clarity, and academic tone of the manuscript. After using this tool, the author(s) reviewed and edited the content as needed and took full responsibility for the content of the publication.

Open Access

References

Adedoyin, M., & Olukoya, F. (2024). Development of a Smart Lock System using QR Code Technology. *ABUAD Journal of Engineering Research and Development (AJERD)*, *7*, 484–492. https://doi.org/10.53982/ajerd.2024.0702.46-j

Aluri, D. C. (2020). Smart Lock Systems: An Overview. *International Journal of Computer Applications*, *177*, 40–43. https://doi.org/10.5120/ijca2020919882

Anamika, S. A., Ar Rafi Khan, Md., Mayen Hasan Sefat, Md., & Kibria, M. G. (2020). Internet of Things-Based Smart Security Provisioning Using Voice-Controlled Door Locking System. In M. S. Uddin & J. C. Bansal (Eds.), *Proceedings of International Joint Conference on Computational Intelligence* (pp. 439–452). Springer Singapore.

Aniru, M. A., Osasenaga, E. V., Emmanuel, O. E., Gerald, M. O., & Melody, E. O. (2024). Design and construction of a smart lock system using Internet of Things (IoT). *International Journal of Informatics, Information System and Computer Engineering (INJIISCOM)*, *6*(1), 82–95. https://doi.org/10.34010/injiiscom.v6i1.14127

Belano, P. A., Campit, K. F. M., Mendoza, J. C. S., Rasing, K. A. S., del Rosario, J. R. B., & Bandala, A. A. (2023, November). Development of a microcontroller-based smart front DoorLock system. In *2023 IEEE 15th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)* (pp. 1-6). IEEE. https://doi.org/10.1109/HNICEM60674.2023.10589066

de Lima, A. B., Gurung, B., & Farhad, S. M. (2020). Efficient App Based Smart Door Lock System Using Bluetooth. In L. Barolli, F. Amato, F. Moscato, T. Enokido, & M. Takizawa (Eds.), *Web, Artificial Intelligence and Network Applications* (pp. 1046–1055). Springer International Publishing. https://doi.org/10.1007/978-3-030-44038-1_97

Gadupu, H., Mokharji, O., Kankaria, R., Kumar, S., & Jayavel, K. (2021). ACCESS - IoT enabled smart lock. *International Journal of Reconfigurable and Embedded Systems (IJRES)*, *10*, 176. https://doi.org/10.11591/ijres.v10.i3.pp176-185

Hadis, M. S., Palantei, E., Ilham, A. A., & Hendra, A. (2018, March). Design of smart lock system for doors with special features using bluetooth technology. In *2018* *international conference on information and communications technology (ICOIACT)* (pp. 396-400). IEEE. https://doi.org/10.1109/ICOIACT.2018.8350767

Han, D., H. Kim, & J. Jang. (2017). Blockchain based smart door lock system. *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, 1165–1167. https://doi.org/10.1109/ICTC.2017.8190886

Saad, I., Amran, N. S., Haris, H., & Tan, M. K. (2023, September). Development of contactless door lock system using text-dependent voice authentication. In *2023 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)* (pp. 301-306). IEEE. https://doi.org/10.1109/IICAIET59451.2023.10291508

Lee, S.-W., Yu, J.-H., & Sim, K.-B. (2015). Real-time Streaming and Remote Control for the Smart Door-Lock System based on Internet of Things. *Journal of Korean Institute of Intelligent Systems*, *25*, 565–570. https://doi.org/10.5391/JKIIS.2015.25.6.565

Mahali, M. I. (2016). Smart Door Locks Based on Internet of Things Concept with mobile Backend as a Service. *ELINVO (Electronics, Informatics, and Vocational Education)*, *1*(3), 171–181. https://doi.org/10.21831/elinvo.v1i3.14260

Patil, B., Vyas, P., & Shyamasundar, R. K. (2018). SecSmartLock: An Architecture and Protocol for Designing Secure Smart Locks. In V. Ganapathy, T. Jaeger, & R. K. Shyamasundar (Eds.), *Information Systems Security* (pp. 24–43). Springer International Publishing.

Permana, K. A., Piarsa, I. N., & Wiranatha, A. A. K. A. (2024). IoT-Based Smart Door Lock System with Fingerprint and Keypad Access. *Journal of Information Systems and Informatics*, *6*(3). https://doi.org/10.51519/journalisi.v6i3.844

Prathapagiri, D., & Kosalendra, E. (2021). Wi-Fi door lock system using ESP32 CAM based on IoT. *The International journal of analytical and experimental modal analysis*, *13*(7), 2000-2003. https://ijaema.com/VOLUME-XIII-ISSUE-VII-JULY-2021-SP/

Rahayu, Y., Afif, L., & Soh, P. J. (2022). Design and development of smart lock system based QR-Code for library's locker at Faculty of Engineering, Universitas Riau. *SINERGI*, *26*, 379. https://doi.org/10.22441/sinergi.2022.3.013

Reza, R., Alam, A., & Islam, M. (2019). *IoT and Wi-Fi Based Door Access Control System using Mobile Application*. https://doi.org/10.1109/RAAICON48939.2019.09

Sobale, S., Patel, K., Patel, A., Nikam, S., Pathrabe, S., & Patil, S. (2022, December). OTP based door lock system with mobile application using Arduino UNO and ESP8266 Wi-Fi module. In *2022 Sardar Patel International Conference on Industry 4.0-Nascent Technologies and Sustainability for'Make in India'Initiative* (pp. 1-4). IEEE. https://doi.org/10.1109/SPICON56577.2022.10180607

Sai, K. N., Sunil, T. D., & Eshwarappa, M. N. (2024). A comprehensive review of door lock security systems. *Int J Circuit Comput Networking*, *5*(1), 12–17. https://doi.org/10.33545/27075923.2024.v5.i1a.61

Sharifuzzaman, Md., Islam, J., & Chowdhury, S. (2022). Designing and developing IoT based security system for smart home. *Journal of Discrete Mathematical Sciences and Cryptography*, *25*(7), 2049–2056. https://doi.org/10.1080/09720529.2022.2133244

Sinaga, D. H., Sembiring, M. A. R., Salman, R., Hutajulu, O. Y., & Sinuraya, A. (2023). Calculation of Capacity and Usage Time of Lithium-Ion Batteries on Electric Bikes With 350 W BLDC Motors. *Fidelity : Jurnal Teknik*, *5*(2), 149–155. https://doi.org/10.52005/fidelity.v5i2.157

Singh, A. K., Laxmi, N. H, Shamith, K. M, & K. M. (2024). Design and Implementation of Smart Door Lock System Using IoT. *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*, 1–4. https://doi.org/10.1109/CSITSS64042.2024.10816710

Sugihartono, T., Isnanto, B., Putra, R. R. C., & Pradana, H. A. (2019). Automation Smartlock for Implementing Smarthome Security Using Location Based Service. *Jurnal Telematika*, *14*(1), 29–30. https://doi.org/10.61769/telematika.v14i1.259

Surekha, G., Cheruku, A. K., Methari, E., Mogili, M., Chennaram, S. K. G., & Anem, S. (2023). Smart locking system using RFID, biometric and OTP-based technologies. *AIP Conference Proceedings*, *2794*(1), 020048. https://doi.org/10.1063/5.0165986

Thakur, E. (2024). IoT-Enabled Smart Lock System. *Journal of Electrical Systems*, *20*, 4090–4097. https://doi.org/10.52783/jes.5412

Tiwari, A., & Waoo, A. A. (2024). DOOR SECURITY SYSTEM FOR HOME MONITORING BASED ON IOT. *ShodhKosh: Journal of Visual and Performing Arts*, *5*(5), 335–341. https://doi.org/10.29121/shodhkosh.v5.i5.2024.1884

Yin, M., Huang, J., & Chen, H. (2021, May). Development of a smart lock system based on internet of things and cloud platform. In *2021 IEEE International Conference on Artificial Intelligence and Industrial Design (AIID)* (pp. 477-481). IEEE. https://doi.org/10.1109/AIID51893.2021.9456578

Zainuddin, A. A., Abd Rahman, A. D., Nor, R. M., Hussin, A. A. A., Mohd, N. N. M. S. N., Shamsudin, A. U., & Sapuan, M. S. (2024). Innovative IoT smart lock system: Enhancing security with fingerprint and RFID technology. *Malaysian Journal of Science and Advanced Technology*, 360-365. https://doi.org/10.56532/mjsat.v4i4.335

Biographies of Authors

Muhammad Fachrul, Department of Electrical Engineering, Faculty of Engineering, Universitas Papua, Manokwari 98314, Indonesia.

- Email: mfachrul@gmail.com
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Adelhard Beni Rehiara, Department of Electrical Engineering, Faculty of Engineering, Universitas Papua, Manokwari 98314, Indonesia.

- Email: a.rehiara@unipa.ac.id
- ORCID: 0000-0002-4103-4034
- Web of Science ResearcherID: N/A
- Scopus Author ID: 36550626200
- Homepage: https://scholar.google.com/citations?user=2mBB-yIAAAAJ&hl=id

Pandung Sarungallo, Department of Electrical Engineering, Faculty of Engineering, Universitas Papua, Manokwari 98314, Indonesia.

- Email: p.sarungallo@unipa.ac.id
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: 58001304400
- Homepage: https://scholar.google.com/citations?user=D6egPfAAAAAJ&hl=en