

DESIGN AND IMPLEMENTATION OF A SMART DOOR LOCK SYSTEM BASED ON ARDUINO MEGA 2560

Vo Van An ⁽¹⁾

(1) Institute of Engineering and Technology, Thu Dau Mot University
Corresponding author's email: anvv@tdmu.edu.vn

DOI: 10.37550/tdmu.EJS/2026.02.732

Article Info

Volume: 8

Issue: 2

June: 2026

Received: Apr. 15th, 2026

Accepted: May. 25th, 2026

Page No: 279-290

Abstract

This paper proposes the design and implementation of a smart door lock system based on the Arduino Mega 2560 platform, integrating multi-modal authentication including password, fingerprint, and RFID. The system is built on a centralised control architecture to optimise processing flow and enhance operational reliability. Compared to traditional systems using Arduino Uno with a limited number of authentication layers, the proposed solution enhances security and scalability. Experimental results show that the system achieves high accuracy, with 100% success rates for passwords and RFID and 96.7% for fingerprint recognition. At the same time, the system ensures fast response times, meeting real-time requirements. These results affirm the effectiveness and feasibility of the solution in embedded security applications and IoT systems.

Keywords: Arduino, embedded security system, fingerprint, multimodal authentication, smart door lock, password, RFID.

1. Introduction

In recent years, the rapid development of smart homes, embedded security systems, and Internet of Things (IoT)-based surveillance technology has significantly increased the demand for smart access control solutions. Traditional mechanical lock systems are increasingly unable to meet modern security requirements due to their vulnerability to key duplication, unauthorized access, and limitations in monitoring capabilities. Therefore, smart door lock systems based on embedded microcontrollers have become an important research direction in both academic and industrial applications. These systems aim not only to enhance security effectiveness but also to provide flexibility, scalability, and higher real-time operational capabilities for residential, office, and industrial environments.

Among existing embedded platforms, the Arduino-based architecture is widely used due to its low cost, ease of programming, open-source ecosystem, and compatibility with a wide range of sensors and communication modules. Many recent studies have focused on integrating authentication technologies such as passwords, radio frequency identification (RFID), and fingerprint recognition into door lock systems. These authentication mechanisms are considered effective solutions for enhancing the reliability of access

control compared to traditional mechanical lock systems. However, the majority of current systems still utilize relatively simple hardware architectures and have a limited number of authentication layers, reducing scalability and practical applicability in complex security environments.

1.1. Literature review

Some studies have investigated the implementation of smart door lock systems based on Arduino with various authentication mechanisms. In this study (Ricky Reyensen Samosir et al., 2025), the authors propose an automatic door lock system using passwords to enhance security and convenience. The system is built on an ATmega328 microcontroller (Arduino Uno), programmed with the Arduino IDE, and designed using a block diagram to describe its structure and operating principles. An experimental research method is applied to evaluate and refine the system. In (Mohamad Irkam et al., 2024), this study proposes a document security system using Arduino Uno integrated with fingerprint and RFID modules to enhance safety with a two-layer authentication mechanism. The system uses a fingerprint sensor as the access activation mechanism and an RFID tag attached to the file cover for identification via electromagnetic waves through an RFID reader, which consists of two main components: the tag and the reader. The ATmega328 microcontroller serves as the central processing unit, and the system also integrates supporting elements such as a microSD card, a buzzer, a push button, and a servo. This solution helps minimize the risk of document loss and misuse in enterprises. In the context of increasing security risks, study (Harishni L et al., 2024) proposes a smart door lock system based on the Arduino platform, integrating an LCD, servo, and matrix keypad for password authentication. The system automatically locks temporarily and sends alerts via a GSM module when the wrong password is entered too many times. The model is simulated in Tinkercad to verify feasibility, enhance security, and ensure user-friendliness.

In study (Kapil Kumar Bhati et al., 2025), the authors present the design of a low-cost door lock system based on an Arduino Uno, featuring a keypad for password entry, an LCD, and a servo to control the locking mechanism. The hardware architecture, password authentication software, and enforcement mechanism are briefly described. Test results show that the system operates stably and has potential applications in basic access control. Limitations regarding security and the locking mechanism are also analyzed, with suggestions for future upgrades. Paper (Chasokela, D et al., 2022) proposes a door control system based on the Arduino Uno microcontroller, integrating a camera and an ultrasonic sensor to enhance security. The system only allows the door to open when the entered password matches the stored data in memory. Upon successful authentication, the microcontroller sends a signal to control the servo motor to unlock. Simultaneously, the system records images of the access attempts for reference in situations such as theft or unauthorized intrusion. In (Sandhyarani Suresh Kamble et al., 2025), this article presents the design and implementation of an electromagnetic door lock system using RFID technology controlled by the Arduino Uno microcontroller. The system integrates an RC522 reader with a solenoid locking mechanism to provide a secure, effective access control solution. Evaluation results show that the proposed solution is low-cost, easy to deploy, scalable, and suitable for civil and office security applications. Study (Sonali Podder et al., 2025) proposes a fingerprint door lock system using Arduino, integrating biometric sensors to authenticate users and control a servo or electromagnetic lock upon successful identification. This solution eliminates physical keys, reducing the risk of unauthorized access, while being low-cost, easy to deploy, and scalable. Experimental

results demonstrate that the system has a fast response time, high accuracy, and good reliability in smart home and IoT applications.

Overall, previous studies have made significant contributions to the development of low-cost smart security systems. However, there are still some limitations. (i) the majority of current systems use only one or two authentication methods rather than a fully integrated multi-factor authentication architecture. (ii) most studies utilize the Arduino Uno platform based on the ATmega328 microcontroller, which has limited hardware resources in terms of memory, communication, and scalability. (iii) many studies primarily focus on implementing functionality without providing a detailed analysis of the centralized control architecture, the real-time signal processing flow, or a comprehensive quantitative assessment under actual operating conditions. Therefore, there remains a need for research on a smart door lock system that integrates multiple authentication methods within a centralized embedded architecture, capable of enhancing operational reliability, security levels, and future system development.

1.2. Research gap

Based on the overview of the surveyed studies, several important research gaps remain inadequately addressed. Current smart door lock systems primarily focus on low-cost solutions or individual authentication mechanisms, without integrating multiple authentication methods into a unified control framework. Most previous studies also utilize microcontrollers with limited hardware resources, making it difficult to integrate additional modules and advanced security functions. Furthermore, the research lacks attention to a centralized address architecture capable of synchronizing multiple authentication modules while reducing control latency and avoiding logical conflicts during operation.

Another significant limitation is the lack of detailed hardware analysis and quantitative experimental evaluation. Many studies only demonstrate functionality without fully assessing criteria such as authentication success rates, response times, processing reliability, or system scalability. Therefore, there are still limitations in understanding how multi-factor authentication systems operate under continuous real-world conditions and how centralized control architecture can improve synchronization and system stability.

1.3. Research objectives

To address the aforementioned limitations, this study proposes the design and implementation of a smart door lock system based on the Arduino Mega 2560 platform, integrating multimodal authentication methods including passwords, fingerprints, and RFID. Unlike previous studies that primarily focused on one or two-layer security mechanisms, the proposed system employs a centralized control architecture to coordinate all authentication modules on a unified embedded platform. The main objectives of the research include: (i) designing a centralized smart door lock architecture that integrates password, fingerprint, and RFID authentication methods on the Arduino Mega 2560 platform; (ii) analyzing the hardware architecture and operational principles of the integrated authentication modules, including the AS608 fingerprint sensor, RC522 RFID module, and matrix keyboard; (iii) experimentally evaluating the operational reliability of the system through quantitative metrics such as success authentication rates and response times; (iv) comparing the proposed system with previous representative studies regarding authentication capability, scalability, hardware resources, control architecture, and experimental evaluation; (v) demonstrating the feasibility of a scalable

multi-factor embedded security system suitable for IoT integration, cloud monitoring, and future smart security applications. The paper's structure consists of four sections: Section 1 - Introduction. Section 2 - Building smart door lock system. Section 3 - Presentation of the hardware model and evaluation of the operation of the smart door lock system. Finally, there is the conclusion and references.

2. Building a smart door lock system

2.1. Block diagram of the smart door lock system.

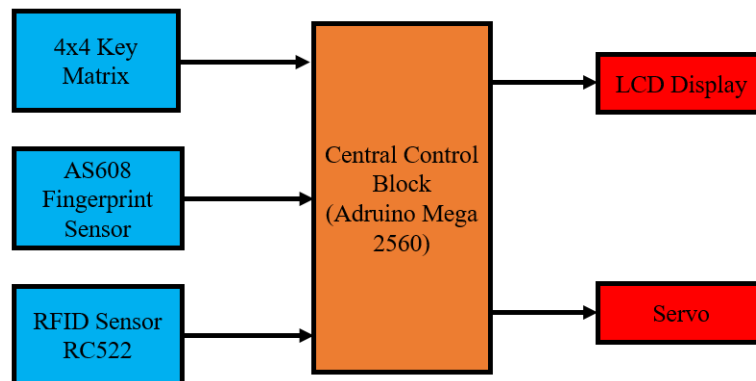


Figure 1. Block diagram of the smart door lock system.

Source: Vo Van An, 2026

Figure 1 presents the overall block diagram of the smart door lock system, which is designed with a centralized control architecture. The system consists of three main functional blocks: the sensor and input block, the central processing block, and the actuation block. The sensor and input block includes a keypad matrix, an AS608 fingerprint sensor, and an RFID sensor that receives authentication signals from the user, converts them to digital data, and sends the data to the central processor (Arduino Mega 2560). The central processing block executes authentication algorithms, compares them with stored data, and makes control decisions. The control signals are then transmitted to the actuation block to activate the electronic locking mechanism (servo). This structure ensures a sequential processing flow, reduces control delays, and enhances system reliability.

2.2. Design of the Smart Door Lock System

2.2.1. Central Control Block (Arduino Mega 2560)

The Arduino Mega 2560 is a microcontroller development board based on the ATmega2560, operating at 5 V with a 16 MHz clock. The board provides 54 digital input/output pins (14 of which support PWM), 16 analog input pins with 10-bit resolution, and four hardware UART ports supporting TTL serial communication. Additionally, the system supports SPI and I2C (TWI) protocols, allowing flexible integration with peripheral devices. The ATmega2560 microcontroller features 256 KB of Flash memory (8 KB reserved for the bootloader), 8 KB of SRAM, and 4 KB of EEPROM, meeting the requirements for deploying complex embedded control algorithms. The board can be powered via a USB port or an external power source in the range of 6–20 V (recommended: 7–12 V) and integrates the ATmega8U2 as a USB-to-serial converter, allowing programs to be uploaded directly via the bootloader without the need for external programming hardware (Arduino et al., 2011).

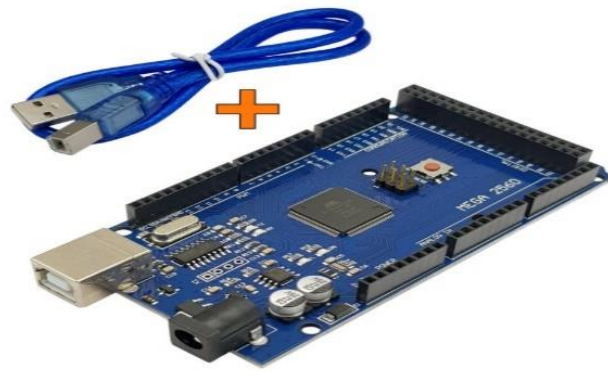


Figure 2. Central controller Arduino Mega 2560.

Source: Arduino, 2011

2.2.2. Sensor and Input Block

The AS608 fingerprint sensor is an integrated optical biometric module capable of on-device fingerprint acquisition, processing, and storage without requiring an external processor (Figure 3). It operates within a 3.3–5 V DC range and communicates via TTL serial with a configurable baud rate of 9600–57600 bps. The module features four primary pins (V+, TXD, RXD, GND), enabling straightforward integration with microcontrollers such as Arduino. Its fully integrated architecture supports real-time performance, stability, and reliability, making it suitable for applications including access control, smart door locks, and embedded security systems (Handson Technology et al., 2019).



Figure 3. AS608 Fingerprint Sensor.

Source: Handson Technology, 2019

Figure 4 depicts the operating principle of the AS608 fingerprint sensor. The sensor employs Total Internal Reflection (TIR) and Frustrated Total Internal Reflection (FTIR) to capture fingerprint patterns. When a finger contacts the prism surface, the ridges disrupt internal reflection while the valleys maintain it, producing intensity variations that form a contrast image. This image is captured by an integrated sensor and processed to generate a digital fingerprint template for storage and authentication (Handson Technology et al., 2019).

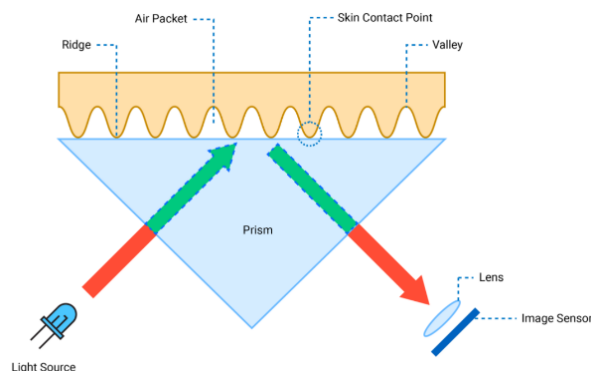


Figure 4. Operating Principle of the AS608 Fingerprint Sensor.

Source: Handson Technology, 2019

Figure 5 illustrates the cross-sectional structure of the fingerprint sensor, which integrates a glass prism, an LED lighting array, and a CMOS image sensor, all arranged perpendicular to two PCB boards soldered together. Light from the LED enters the prism and undergoes total internal reflection (TIR). When a finger contacts the prism, the intensity of reflection changes between the ridge and valley areas, creating a high-contrast fingerprint image. The horizontal PCB integrates the LED array and touch-sensing electrodes, while the vertical PCB integrates the image sensor, microcontroller, and a TTL communication interface. A black epoxy layer covering the prism's bottom enhances background contrast, while an internal optical barrier reduces optical noise and improves recognition accuracy (Handson Technology et al., 2019).

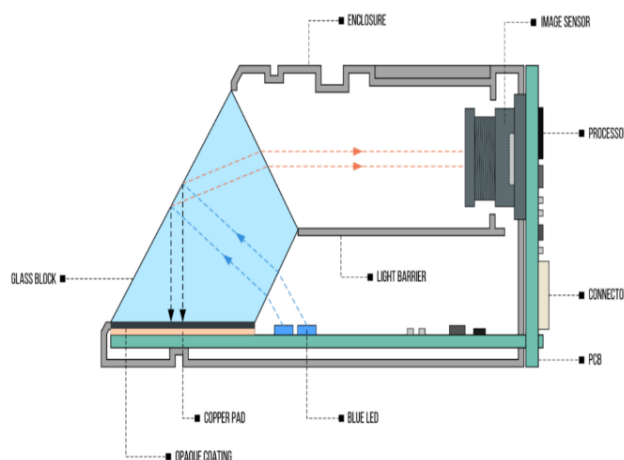


Figure 5. Cross-section of the Fingerprint Sensor

Source: Handson Technology, 2019

The RC522 RFID module is based on the MFRC522 chip from NXP, operating at 13.56 MHz and supporting the ISO/IEC 14443A standard (MIFARE, NTAG). The device integrates an RF transmitter and receiver, enabling contactless communication with cards at a typical range of up to 50 mm, depending on the card size and antenna adjustment. The module operates at 2.5–3.3 V, consumes 13–26 mA, and supports multiple communication interfaces, including SPI (up to 10 Mbit/s), I2C, and UART. Data transmission rates can reach up to 848 kbd according to the ISO14443A standard. The MIFARE S50 card memory provides 1024 bytes, divided into 16 sectors with a two-key

security mechanism (Key A/Key B). The RC522 only supports 13.56 MHz cards and is not compatible with the 125 kHz system (Figure 6) (Handson Technology et al., 2019).



Figure 6. RFID Sensor RC522

Source: Handson Technology, 2019

The 4×4 soft matrix keypad is a membrane input module with 16 keys arranged in a row-column structure, using an 8-pin connector for matrix scanning (Figure 7). The device operates within a temperature range of 0–70 °C, making it suitable for embedded systems and basic control applications. Its overall dimensions are 77 × 69 mm, with an 88 mm connection cable, facilitating mechanical integration. The back features an adhesive layer, enabling flexible installation in various practical applications (Vo Van An et al., 2022).

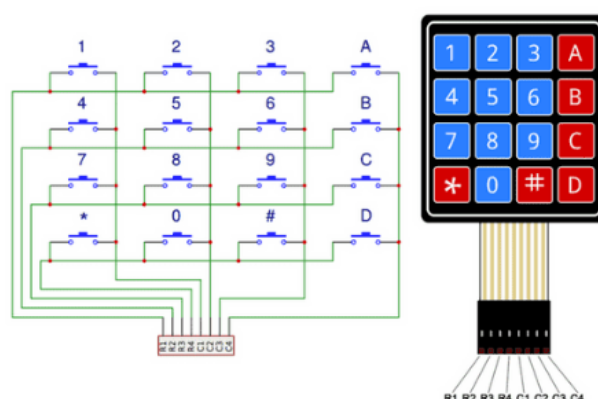


Figure 7. 4x4 Key Matrix.

Source: Vo Van An, 2022

In this study, the focus is not on the optical mechanism but on integrating the sensor into a centralised control architecture, where fingerprint data is processed and synchronised with other authentication methods (passwords and RFID) to ensure the system operates reliably and stably.

3. Completing the model and evaluating system performance

3.1. Completing the Model of the Smart Door Lock System.

Figure 8 presents the functional diagram of the smart door system, which includes the sensor and input block, the central control block, and the actuator block, all linked via a centralized control architecture. Signals from the input devices are transmitted to the

processor for authentication and logical control processing, which then issues activation commands to the corresponding locking mechanism. Based on this functional diagram, the actual hardware system has been assembled and deployed, as illustrated in Figure 9. The experimental model demonstrates synchronized integration between the hardware modules, ensuring stable operation and meeting the control requirements of the smart door lock system.

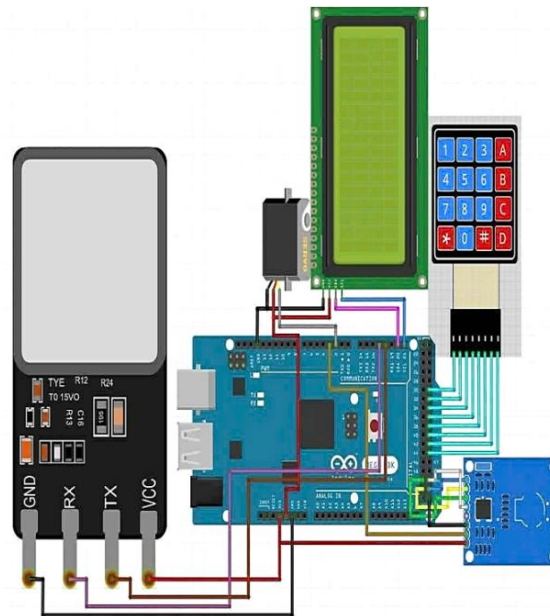


Figure 8. Schematic diagram of the Smart Door Lock

Source: Vo Van An, 2026

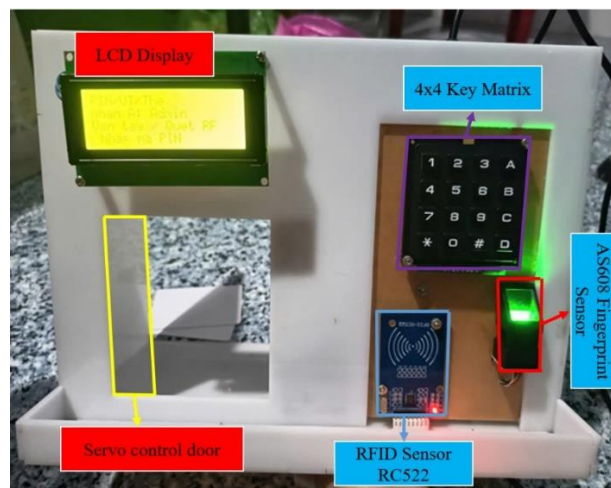


Figure 9. Hardware Model of the Smart Door System.

Source: Vo Van An, 2026

4. Experimental Results

The smart door lock system has been implemented and experimentally verified to assess its feasibility and reliability in real-world operation. Figure 10 illustrates the overall model execution process, showing the synchronized integration among the central controller, authentication modules, and actuators, with stable feedback and no logic errors

during repeated open/close cycles. Figure 11 shows the password-setting and authentication functions using the 4×4 key matrix, where the row-column scanning mechanism ensures accurate recognition of entered characters and only unlocks when the data matches. Figure 12 demonstrates the fingerprint registration and identification mode, showing that the acquisition, feature extraction, and matching processes are performed quickly and reliably. Figure 13 illustrates the RFID authentication method, where the card identification code is read and verified before issuing the control command to the locking mechanism. Experimental results show that the system operates stably under repeatable testing conditions, with high authentication accuracy and consistent response times. The addition of quantitative metrics, such as success rate and response time, provides objective evidence of the system's reliability. The centralised control architecture ensures synchronisation among authentication modules, minimising latency and avoiding logical conflicts during multi-modal operation.



Figure 10. Experimental Run of the Smart Door Lock System Model.

Source: Vo Van An, 2026



Figure 11. Experimental Run of the Model with Password Setting Function Using the Key Matrix.

Source: Vo Van An, 2026



Figure 12. Experimental Run of the Model with Fingerprint Recognition Setting Function.

Source: Vo Van An, 2026



Figure 13. Experimental Run of the Model with RFID Card Recognition Function.

Source: Vo Van An, 2026

To evaluate the proposed system's performance in more detail, quantitative experiments were conducted for each authentication method. The results, including the success rate and average response time, are summarised in Table 1.

Table 1. Quantitative evaluation of the performance of authentication methods.

Authentication Method	Number of Trials	Successful Attempts	Success Rate (%)	Average Response Time (ms)
Password (Keypad)	30	30	100%	320
Fingerprint (AS608)	30	29	96.7%	850
RFID (RC522)	30	30	100%	210

To quantitatively evaluate the system's performance, experiments were conducted for each authentication method. As shown in Table 1, the system achieved high success rates across all methods: password and RFID authentication reached 100%, while fingerprint recognition achieved 96.7% due to minor discrepancies in finger placement. In terms of response time, the RFID method was the fastest (approximately 210 ms), followed by password entry (320 ms). In comparison, fingerprint recognition required a longer processing time (around 850 ms) due to image acquisition and processing. These results indicate that the system ensures high reliability and good real-time responsiveness.

Proceed to analyze and compare the current study with representative studies (Ricky Reyensen Samosir et al., 2025; Mohamad Irkam et al., 2024; Harishni L et al., 2024; Kapil Kumar Bhati et al., 2025; Chasokela, D et al., 2022; Sandhyarani Suresh Kamble et al., 2025; Sonali Podder et al., 2025) based on the criteria of: microcontroller platform, authentication method, number of security layers, control architecture, level of hardware analysis, experimental evaluation, and system scalability. Table 2 summarizes this comparative analysis, highlighting the limitations of existing solutions and emphasizing the improvements of the proposed multimodal smart door lock system.

Table 2. Comparison of the Proposed Smart Door Lock System with Related Studies

References	Evaluation criteria							
	Microcontroller platform	Authentication methods	Number of security layers	Control architecture	Hardware analysis	Experimental evaluation	Scalability	Multimodal integration level
(Ricky Reyensen Samosir et al., 2025)	Arduino Uno	Password	1	Basic	Restrictions	Basic	Restrictions (low resources)	Low
(Mohamad Irkam et al., 2024)	Arduino Uno	Fingerprint + RFID	2	Simple integration	Medium	Basic	Restrictions	Medium
(Harishni L et al., 2024)	Arduino	Password + GSM	1	Simulation + GSM	Restrictions	Simulation	Restrictions	Low
(Kapil Kumar Bhati et al., 2025)	Arduino Uno	Password	1	Basic	Restrictions	Simple Experimental	Restrictions	Low
(Chasokela, D et al., 2022)	Arduino Uno	Password + Camera	1	Camera supplement	Medium	Simple experimental	Restrictions	Medium
(Sandhyarani Suresh Kamble et al., 2025)	Arduino Uno	RFID	1	Single RFID	Restrictions	Functional experimental	Restrictions	Low
(Sonali Podder et al., 2025)	Arduino	Fingerprint	1	Single fingerprint	Restrictions	Functional experimental	Restrictions	Low
Proposed research	Arduino Mega 2560	Password + Fingerprint + RFID (multimodal)	3 independent layers	Centralized control architecture, fully integrated	Detailed analysis of each module and processing flow	Evaluation of multi-mode operation, system stability verification	High (multiple UARTs, large memory, SPI/I2C)	High

The comparison table shows that studies have made significant contributions to the development of smart door lock systems based on the Arduino platform with the goals of low cost and ease of deployment. However, most works focus on single or dual-layer authentication mechanisms, primarily using the ATmega328 microcontroller with limited hardware resources, resulting in low scalability and integration capabilities. Furthermore, the system architecture in many studies remains discrete, lacking in depth analysis of

signal processing flow and comprehensive evaluation of stability during multi-authentication mode operation. Compared to previous works, the proposed study stands out by building a centralized control architecture on the Arduino Mega 2560 platform with expandable resources, while integrating three independent authentication methods (password, fingerprint, and RFID). This approach not only enhances security levels but also improves scalability, operational reliability, and completeness in the experimental evaluation of the system.

5. Conclusion

The proposed smart door lock system has successfully integrated multi-layer authentication methods within a centralized control architecture using the Arduino Mega 2560 platform. The system demonstrates high reliability and accuracy, validated through both qualitative and quantitative assessments. The inclusion of performance metrics, such as success rate and response time, enhances the scientific value of the research. Compared to existing solutions, the proposed system offers greater scalability, flexibility, and higher security. In future studies, the system could be expanded with IoT connectivity, remote monitoring, data encryption, and cloud-based access management.

References

- Ricky Reyensen Samosir, Jimmie, Meilyana Winda Perdana. (2025). System Design on Door Locks Using Arduino Based Passwords. *Jurnal Teknologi Dan Open Source*, 8, 1179–1185. <https://doi.org/10.36378/jtos.v8i2.5172>.
- Mohamad Irkam, Toni Wijanarko Adi Putra. (2024). Document Security System Using Arduino-Based Fingerprint And Rfid Module. *Journal of Technology Informatics and Engineering*, 2, 32-42. <https://doi.org/10.51903/jtie.v2i1.174>.
- Harishni L, Srisha M, Sandhya S. (2024). Design and Simulation of an Arduino-Based Password-Protected Door Locking System. *International Journal of Engineering and Advanced Technology (IJEAT)*, 14, 25-30. <https://doi.org/10.35940/ijeat.B4550.14021224>.
- Kapil Kumar Bhati, Mohit Kumar, Pankaj Maurya, Mohammad Shahzad, Vishnu Kumar Singh. (2025). Microcontroller-Based Door Locking System. *International Journal of Innovative Science and Research Technology*, 136-144. <https://doi.org/10.38124/ijisrt/25jun180>.
- Chasokela, D., Tshuma, L. S., Mastshe, K., & Sibanda, M. (2022). Password Based Door Locking System. *Indiana Journal of Multidisciplinary Research*, 2, 1-5. <https://doi.org/10.5281/zenodo.7044141>.
- Miss. Sandhyarani Suresh Kamble, Dr. Manisha Vikas Bhanuse. (2025). RFID Based Solenoid Door Lock Using Arduino. *International Journal of Research Publication and Reviews*, 6, 7939-7940.
- Sonali Podder, Sougata Dey, Soumyadeep Mahapatra, Soumyasis Das, Souramita Banik, Sourin Biswas, Nabaneeta Banerjee. (2025). Fingerprint Door Lock System by Arduino. *International Journal of Sciences and Innovation Engineering*, 2(6), 936-942. <https://doi.org/10.70849/ijsci>
- Arduino. (2011). *Arduino Mega 2560 technical specifications and reference manual*. Arduino.cc.
- Handson Technology. (2019). *AS608 optical fingerprint sensor module user guide*. Handsontec.
- Handson Technology. (2019). *RC522 RFID development kit data specifications*. Handsontec.
- Vo Van An, Nguyen Thi Ngoc thao, Dinh the Manh. (2022). Thiet Ke Va Hoan Thien Mo Hinh Cua Thong Minh Su Dung Bluetooth Va Ung Dung Android. *Hoi Nghi Quoc Gia Lan Thu 25 Ve Dien Tu, Truyen Thong Va Cong Nghe Thong Tin (REV-ECIT2022)*, 382-387.