JEEEIT TRANSACTIONS, Vol.2,No.1,December 2025

Design and Development of a Multi-Authentication Smart Door Lock System

Abdulkarem M. A. Mohamed[1], and Akram Muntaser[2]

[1]Mecatronics Department, Higher Institute of Science and Technology, Tarhuna, Libya

[2]Control Engineering Department, College of Electronic Technology, Bani Walid, Libya

*Corresponding author: akrm3266@gmail.com

ABSTRACT This project presents the design and implementation of a smart electronic door lock system based on the Arduino Mega microcontroller. The proposed system enhances security by integrating multiple authentication methods, including fingerprint recognition, RFID card identification, facial recognition, and password verification, providing users with flexible and reliable access control. The integration of several security techniques significantly improves system reliability, minimizes unauthorized access, and provides greater flexibility than conventional mechanical locking systems. This project demonstrates the practical application of embedded systems and smart technologies in access control and home security. The proposed design offers a low-cost, scalable, and user-friendly solution that can be further enhanced through integration with Internet of Things (IoT) technologies, mobile applications, and cloud-based monitoring systems for future smart home and smart building applications.

KEYWORDS IOT, Smart Door, Lock System, RFID card, Matrix keypad, facial recognition camera.

I. INTRODUCTION

The rapid advancement of smart home technologies, embedded systems, and the Internet of Things (IoT) has significantly transformed modern residential and commercial security systems. Among these technologies, intelligent electronic access control has become an essential component of smart buildings by providing enhanced security, user convenience, and remote management capabilities. Unlike conventional mechanical locks, smart door lock systems utilize embedded controllers, sensors, wireless communication, and biometric authentication technologies to improve protection against unauthorized access while offering flexible and user-friendly operation [1], [6], [7].

Conventional lock-and-key mechanisms have several inherent limitations. Physical keys can be lost, duplicated, or stolen, making them vulnerable to unauthorized access. In addition, mechanical locking systems provide little or no capability for user identification, access monitoring, or remote management. These limitations have motivated researchers to develop electronic access control systems that employ various authentication techniques, including passwords, RFID cards, biometric identification, Bluetooth, Wi-Fi, and smartphone-based applications [2], [5], [6].

Recent advances in microcontrollers, low-cost sensors, and embedded computing platforms have enabled the development of affordable smart door lock systems suitable for residential, commercial, educational, and industrial applications. The Arduino Mega microcontroller has become one of the most widely adopted platforms for embedded system development because of its low cost, ease of programming, extensive input/output capabilities, and large open-source software ecosystem [3], [11]. Combined with biometric sensors and wireless communication technologies, Arduino-based systems provide an effective platform for implementing intelligent access control solutions.

Several smart door lock systems have been reported in the literature using individual authentication techniques such as password verification, RFID card identification, fingerprint recognition, or facial recognition [4 -10]. While these approaches improve security compared with traditional mechanical locks, most existing systems rely on a single authentication method. Consequently, system performance may be compromised when the selected authentication technology becomes unavailable or performs poorly under certain operating conditions. Multi-factor authentication systems can overcome these limitations by integrating multiple independent authentication techniques within a unified embedded platform, thereby improving system flexibility, reliability, and security.

Motivated by these challenges, this paper presents the design and implementation of a low-cost multi-authentication smart door lock system based on the Arduino Mega microcontroller. The proposed system integrates four complementary authentication methods, namely fingerprint recognition, RFID card identification, password verification, and facial recognition, to provide flexible and reliable access control. The modular hardware and software architecture allows users to select the preferred authentication method while facilitating future integration with IoT connectivity, cloud-based

monitoring, and mobile applications. Experimental evaluation demonstrates the successful implementation and reliable operation of the proposed system, highlighting its suitability for smart homes [12], educational laboratories, and small commercial access control applications.
The remainder of this paper is organized as follows. Section II presents the research objectives and significance of the proposed system. Section III reviews related work on smart door lock technologies. Section IV describes the proposed hardware and software architecture. Section V presents the experimental results and discussion, and Section VI concludes the paper with recommendations for future work.

II. Research Objectives and Significance

i. Problem Statement

Conventional mechanical door locking systems continue to be widely used in residential, commercial, and institutional buildings due to their simplicity and low cost. However, these systems suffer from several limitations, including key loss, unauthorized duplication, lock tampering, and the inability to monitor or record user access. Although electronic door lock systems have addressed some of these shortcomings, many existing solutions rely on a single authentication method, such as passwords, RFID cards, or biometric identification. The dependence on a single authentication mechanism may reduce system reliability when credentials are lost, compromised, or affected by environmental conditions. Therefore, there is a growing need for smart access control systems that integrate multiple authentication technologies to provide improved security, flexibility, and reliability [2], [5], [6].

ii. Research Objectives

The primary objective of this research is to design, implement, and experimentally validate a low-cost smart electronic door lock system based on the Arduino Mega microcontroller. The proposed system integrates four independent authentication methods, namely fingerprint recognition, RFID card identification, password verification, and facial recognition, within a unified embedded platform. The specific objectives of this work are to:

- Design a modular hardware architecture for multi-factor authentication.
- Develop software for authentication, access control, and user interaction.
- Integrate multiple authentication modules into a single embedded system.
- Evaluate the functionality and reliability of the proposed prototype through experimental testing.
- Demonstrate a scalable platform that can be expanded with additional authentication methods and smart technologies.

iii. Significance of the Research

The proposed smart door lock system contributes to the development of secure and intelligent access control solutions by combining multiple authentication technologies within a single embedded architecture. Unlike conventional smart locks that rely on a single authentication mechanism, the proposed design provides users with greater flexibility by allowing them to select the most appropriate authentication method according to their operating environment. The modular hardware and software architecture also simplifies maintenance and facilitates future integration with Internet of Things (IoT) connectivity, cloud-based services, and mobile applications.
In addition to its practical applications in smart homes and intelligent buildings, the proposed system serves as an effective educational platform for embedded systems, mechatronics, and Internet of Things (IoT) laboratories. The use of commercially available hardware and open-source development tools makes the system cost-effective, easily reproducible, and suitable for engineering education, prototype development, and small-scale commercial access control applications.

III. Literature Review

The rapid growth of smart homes, Internet of Things (IoT), and embedded systems has accelerated the development of intelligent access control technologies. Unlike conventional mechanical locks, smart electronic locks employ programmable controllers, sensors, wireless communication, and biometric authentication to improve both security and user convenience. Various authentication methods have been proposed in the literature, including password-based systems, RFID cards, fingerprint recognition, facial recognition, Bluetooth, Wi-Fi, and mobile applications. Each technology offers unique advantages and limitations regarding security, cost, reliability, and ease of implementation. Figure 1 presents the most common authentication technologies employed in modern smart door lock systems, including fingerprint recognition, password entry, RFID cards, facial recognition, and Internet-connected smart locks. These technologies form the foundation of current access control solutions and are widely adopted in residential, commercial, and institutional environments [4], [7], [15].

FIGURE 1. Representative smart door lock authentication technologies: (a) fingerprint recognition, (b) password keypad, (c) RFID card access, (d) facial recognition, and (e) IoT-enabled smart lock.

Password-based authentication remains one of the simplest and most economical approaches for electronic door security [2]. It requires only a keypad and a microcontroller, making implementation straightforward and inexpensive. However, password systems are vulnerable to password sharing, guessing attacks, and shoulder surfing, which may reduce overall system security.

RFID-based authentication has become one of the most widely used technologies for access control because of its fast response, contactless operation, and ease of use [5], [10]. RFID systems utilize uniquely encoded tags that communicate with an RFID reader to grant or deny access. Although RFID technology provides greater convenience than mechanical keys, unauthorized card duplication and tag loss remain potential security concerns.

Biometric authentication has significantly improved the reliability of access control systems by using unique physiological characteristics for user identification [4], [8]. Fingerprint recognition is among the most mature biometric technologies due to its high accuracy, relatively low cost, and rapid verification time. Nevertheless, fingerprint sensors may experience degraded performance under unfavorable environmental conditions or when fingerprints are damaged or contaminated [13].

Face recognition has emerged as an effective contactless biometric authentication technology for modern access control systems [6], [7]. By analyzing unique facial features, it enables fast and convenient user identification without requiring physical interaction with the system. This technology enhances user convenience and hygiene, particularly in shared environments. However, its performance can be affected by variations in lighting conditions, facial occlusions, camera quality, and changes in appearance such as masks, glasses, or facial hair [14], [18], [19].

Recent advances in computer vision have enabled facial recognition to become an attractive contactless authentication method. Camera-based identification eliminates the need for physical credentials while improving user convenience. However, facial recognition systems generally require greater computational resources and may be affected by variations in lighting conditions, facial orientation, and image quality.

Several researchers have developed Arduino-based smart locking systems by integrating one or more authentication techniques. Sharma et al. [4] developed a fingerprint-based smart door lock using an Arduino platform and demonstrated reliable biometric authentication for residential security. Afroz [9] presented an Arduino Uno-based smart door lock that successfully implemented electronic access control using embedded hardware. Other studies have implemented RFID-based access control using Arduino and ESP8266 microcontrollers to enable wireless monitoring and remote management [5], [10]. More recent research has investigated IoT-enabled smart locks capable of remote access through smartphones and cloud services [7], further extending system functionality for smart home applications. Although previous studies have demonstrated the effectiveness of individual authentication methods, relatively few systems combine multiple authentication techniques within a single embedded platform. Integrating fingerprint recognition, RFID identification, password verification, and facial recognition provide multiple independent layers of security while improving system flexibility and user accessibility. This multi-factor authentication approach reduces dependence on a single security mechanism and enhances the overall reliability of the access control system.

Motivated by these limitations, the present work proposes a low-cost, Arduino Mega-based smart door lock system that integrates four complementary authentication methods within a unified embedded architecture. The proposed system combines the simplicity of password authentication, the convenience of RFID technology, the accuracy of fingerprint recognition, and the flexibility of facial recognition to provide a practical and scalable solution for modern smart access control applications [16], [17].

IV. Proposed Smart Door Lock System

i. System Overview

The proposed smart door lock system is designed to provide a secure, flexible, and cost-effective access control solution by integrating four independent authentication methods: fingerprint recognition, RFID card identification, password verification, and facial recognition. Unlike conventional electronic door locks that rely on a single authentication mechanism, the proposed system allows users to select the most appropriate authentication method according to their requirements and operating conditions. This multi-authentication architecture enhances system reliability, improves user convenience, and reduces dependence on a single security technology.

The system is built around an Arduino Mega 2560 microcontroller, which serves as the central processing unit and coordinates communication among all hardware modules. The Arduino interfaces with the fingerprint sensor, RFID reader, matrix keypad, and facial recognition module to acquire user credentials and execute the authentication process. Additional peripheral devices, including an LCD display, LEDs, buzzer, and servo motor, provide user feedback and control the physical door locking mechanism. The modular architecture simplifies hardware integration, facilitates future system expansion, and enables straightforward maintenance.

Figure 2 illustrates the overall operational flow of the proposed smart door lock system. After system initialization, the controller continuously monitors all authentication devices while remaining in the idle state. When a user selects one of the available authentication methods, the corresponding input data are acquired and transmitted to the Arduino Mega for processing. The controller compares the received credentials with the database of authorized users stored in memory. If authentication is successful, the Arduino activates the servo motor to unlock the door, displays a confirmation message on the LCD, illuminates the green status LED, and maintains the unlocked state for a predefined period before automatically returning the lock to its secure position. If the authentication credentials are invalid, access is immediately denied and the system activates the red LED and buzzer to provide visual and audible warning signals. An error message is simultaneously displayed on the LCD, after which the controller returns to the idle state and waits for the next authentication attempt.

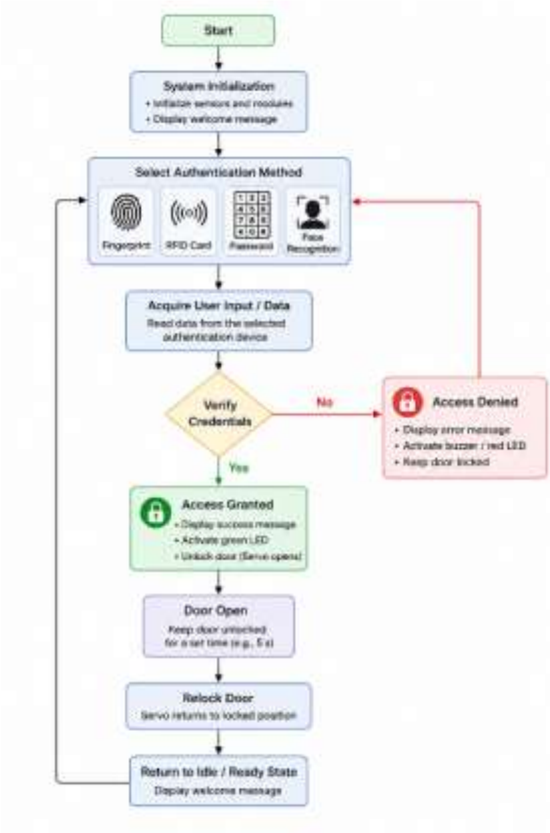

FIGURE 2. **Flowchart of the proposed smart door lock system**

This decision-making process ensures reliable operation while maintaining a consistent user interface across all authentication methods. Furthermore, the modular software design allows additional authentication technologies, communication modules, or cloud-based services to be incorporated in future versions without requiring major modifications to the existing hardware architecture.

ii. Hardware and Software Design

The proposed smart door lock system consists of an integrated hardware and software platform designed to provide reliable, secure, and flexible access control through multiple authentication techniques. The hardware architecture is centered on the Arduino Mega 2560 microcontroller, which serves as the main controller responsible for coordinating data acquisition, authentication processing, actuator control, and communication among all peripheral devices. The Arduino Mega was selected because of its large number of digital and analog input/output pins, sufficient memory capacity, ease of programming, and compatibility with a wide range of sensors and communication modules, making it well suited for embedded security applications.

The authentication subsystem consists of four independent input devices: a fingerprint sensor for biometric identification, an RFID reader for contactless authentication, a matrix keypad for password verification, and a camera module used for facial recognition. These devices provide users with multiple authentication options while improving overall system flexibility and reliability. User interaction is facilitated through a LCD module, which displays operating instructions, authentication status, and system messages. A servo motor functions as the door locking actuator, while green and red LEDs together with a buzzer provide immediate visual and audible feedback indicating successful or unsuccessful authentication attempts. The modular hardware configuration simplifies installation, maintenance, and future system upgrades.

The control software was developed using the Arduino Integrated Development Environment (IDE). The software employs a modular programming approach in which each authentication method operates as an independent software module while sharing a common authentication and access control routine. The Arduino continuously monitors all input devices and processes authentication requests according to predefined decision logic. For fingerprint, RFID, and password authentication, credential verification is performed directly by the controller using stored user information. Facial recognition is performed using an external computer vision application that analyzes facial images and transmits the authentication result to the Arduino through serial communication. Upon successful authentication, the controller activates the servo motor, updates the LCD display, and enables visual confirmation through the green LED. When authentication fails, access is denied, warning messages are displayed, and the buzzer together with the red LED are activated before the system returns to the idle state.

iii. Authentication Strategy and Design Advantages

The proposed smart door lock system adopts a multi-authentication strategy that allows users to access the protected area through any one of four independent authentication methods: fingerprint recognition, RFID card identification, password verification, or facial recognition. Rather than requiring multiple credentials simultaneously, the system provides alternative authentication mechanisms, enabling users to select the most convenient method according to the operating environment and application requirements. This design improves accessibility while maintaining a high level of security.

For every authentication request, the Arduino controller acquires the user credentials from the selected authentication module and compares them with the authorized user database. If the credentials are verified successfully, the controller grants access by unlocking the door through the servo motor, displaying a confirmation message on the LCD, and activating the green status LED. Invalid authentication attempts result in immediate access denial, activation of the buzzer and red LED, and the display of an appropriate warning message. The system then automatically returns to the idle state, ready to process the next authentication request. This unified authentication framework ensures consistent operation regardless of the selected authentication method.

Compared with conventional electronic locking systems, the proposed design offers several important advantages. First, integrating multiple authentication technologies improves system reliability by eliminating dependence on a single security mechanism. Second, the modular hardware and software architecture enables straightforward expansion to incorporate additional authentication technologies, such as smartphone applications, Bluetooth, Near Field Communication (NFC), or voice recognition, without requiring significant modifications to the existing controller. Third, the use of the Arduino Mega platform provides a low-cost, open-source, and easily programmable solution suitable for educational laboratories, residential security systems, and small commercial applications.

Finally, the proposed architecture provides a practical foundation for future smart building applications. The modular design facilitates integration with Internet of Things (IoT) platforms, cloud-based databases, mobile applications, encrypted wireless communication, and artificial intelligence algorithms for enhanced biometric recognition and intelligent access management. These capabilities make the proposed system scalable, adaptable, and suitable for next-generation smart access control systems

V. Experimental Results and Discussion

i. Experimental Setup

The proposed smart door lock system was implemented and experimentally evaluated to verify the functionality and reliability of the integrated multi-authentication platform. The Arduino Mega 2560 microcontroller coordinates communication among all hardware modules while executing the authentication and access control algorithms. To evaluate the effectiveness of the proposed design, a prototype was assembled using commercially available hardware components, including an Arduino Mega 2560, fingerprint sensor, RFID reader, 4×4 matrix keypad, camera module for facial recognition, LCD display, servo motor, LEDs, and a buzzer. Figure 3 shows the assembled experimental prototype used for system implementation and performance evaluation. The prototype integrates all authentication modules into a single embedded platform, enabling users to access the system through fingerprint recognition, RFID card identification, password verification, or facial recognition. The system was tested under normal indoor laboratory conditions to evaluate the functionality of each authentication method individually as well as the complete integrated system. Performance evaluation focused on authentication reliability, response time, communication among hardware modules, and overall system stability during repeated authentication attempts.

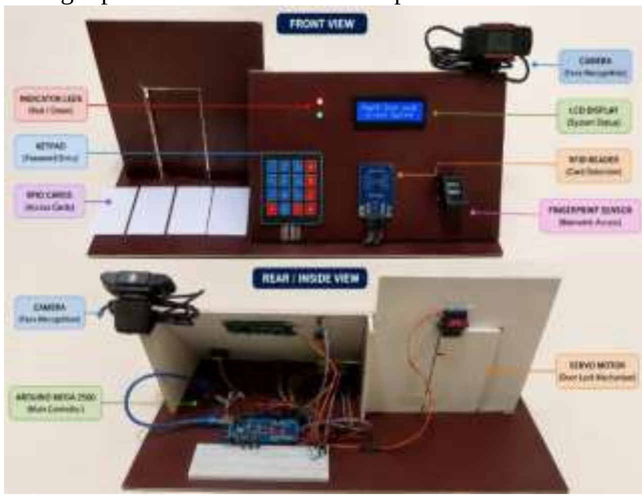

FIGURE 3. **Experimental prototype of the proposed multi-authentication smart door lock system, integrating the Arduino Mega controller, fingerprint sensor, RFID reader, matrix keypad, facial recognition camera, LCD display, servo motor, LEDs, and buzzer.**

ii. Face Recognition Implementation

The facial recognition module was implemented using a Python application developed with the OpenCV computer vision library [20]. The application captures real-time images from the camera, detects human faces, extracts facial features, and compares the detected face with previously registered users stored in the facial recognition database. Prior to authentication, authorized users are enrolled by capturing multiple facial images under different viewing conditions to improve recognition accuracy. During system operation, the camera continuously acquires image frames, and the Python program performs face detection and recognition in real time. Once a valid match is identified, the application transmits a successful authentication signal to the Arduino Mega through serial communication. The Arduino then activates the door unlocking mechanism, updates the LCD display, and enables the green status indicator. If no authorized face is detected, an authentication failure signal is transmitted, causing the controller to deny access and activate the warning indicators. This architecture separates computationally intensive image processing from the embedded controller, allowing the Arduino to focus on real-time access control while the external computer performs facial recognition efficiently.

iii. Authentication Performance

The proposed smart door lock system successfully implemented four independent authentication mechanisms, allowing users to select the most appropriate access method according to their requirements. Each authentication module was evaluated repeatedly using both authorized and unauthorized credentials to verify correct system operation. Successful authentication consistently resulted in door unlocking through servo motor actuation, while invalid authentication attempts maintained the door in the locked state and generated audible and visual alarm indications. Table I summarizes the overall performance of the implemented authentication methods.

Among the evaluated authentication techniques, the fingerprint sensor demonstrated reliable user identification with rapid response and high repeatability, making it suitable for routine access control applications. RFID authentication provided the shortest verification time because authentication required only contactless detection of a registered RFID tag. Password authentication offered a simple and inexpensive solution that required minimal hardware resources; however, its effectiveness depended on correct user input. The facial recognition module provided convenient contactless authentication and eliminated the need for physical credentials, although its performance was influenced by ambient lighting conditions, camera positioning, and facial orientation.

Overall, the experimental results demonstrate that integrating multiple authentication techniques within a single embedded platform significantly improves system flexibility and enhances operational reliability. When one authentication method is unavailable or unsuitable under specific operating conditions, users may select an alternative authentication mechanism without affecting overall system functionality.

TABLE I
PERFORMANCE COMPARISON OF THE IMPLEMENTED AUTHENTICATION METHODS.

Authentication Method	Success Rate (%)	Average Response Time (s)	Remarks
Fingerprint	92	1.3	High accuracy; slight variations due to finger placement.
RFID Card	100	0.5	Fastest authentication with contactless operation.
Password	100	1.0	Depends primarily on user input speed.
Face Recognition	95	3	Performance affected by lighting and camera positioning.

The experimental evaluation indicates that RFID authentication achieved the shortest average response time because authentication required only contactless identification of a registered tag. Fingerprint authentication provided high recognition accuracy with a moderate response time, making it suitable for routine access control applications. Password verification demonstrated reliable operation while maintaining a simple and low-cost implementation. Face recognition required the longest processing time due to image acquisition and feature extraction performed by the Python-based OpenCV application; however, it offered the advantage of completely contactless authentication. Overall, the experimental results demonstrate that all four authentication methods operated reliably and provided flexible access control under normal laboratory conditions.

iv. System Operation

Figure 4 illustrates the operational sequence of the proposed authentication algorithm. After system initialization, users select one of the four available authentication methods. The selected credentials are acquired and verified against the authorized database stored within the system. Successful authentication activates the servo motor, unlocks the door, displays a confirmation message on the LCD, and illuminates the green status LED. When authentication fails, the controller denies access, activates the buzzer and red LED, displays an error message, and returns to the idle state for another authentication attempt.

The modular implementation enables each authentication method to operate independently while sharing the same decision-making algorithm. Consequently, additional authentication technologies may be incorporated in future versions without significant modifications to the controller architecture.

FIGURE 4. Operational flowchart of the proposed smart door lock authentication algorithm.

v. Experimental Validation

Figure 5 presents representative photographs demonstrating successful operation of authentication methods. Successful authentication resulted in immediate activation of the servo motor, unlocking of the door, display of a confirmation message on the LCD, and illumination of the green LED indicator.

Repeated experimental testing confirmed stable communication among the Arduino Mega controller and all peripheral devices. No communication interruptions or hardware synchronization errors were observed during repeated authentication cycles. Furthermore, the modular architecture enabled all authentication modules to operate independently while sharing the same access control logic, thereby simplifying system integration and improving overall reliability.

FIGURE 5. **Experimental validation of the proposed smart door lock system using (a) fingerprint authentication, (b) RFID authentication, (c) password authentication, and (d) facial recognition.**

vi. Comparative Discussion

Compared with previously reported Arduino-based smart door lock systems, the proposed design provides a more comprehensive authentication framework by integrating four independent authentication methods within a unified embedded platform. Most existing systems employ only one or two authentication mechanisms, limiting system flexibility when users encounter operational constraints such as forgotten passwords, lost RFID cards, or poor biometric acquisition conditions. The proposed architecture overcomes these limitations by providing multiple alternative authentication options while maintaining a consistent control algorithm and hardware architecture.

Another important advantage of the proposed system is its modular design. Additional authentication technologies, including Bluetooth, Near Field Communication (NFC), smartphone applications, cloud databases, or voice recognition, can be incorporated with minimal modifications to the existing hardware and software architecture. Consequently, the proposed platform provides a practical foundation for future Internet of Things (IoT)-enabled smart home and intelligent building applications. To demonstrate the advantages of the proposed system, Table II presents a comparison with representative smart door lock systems previously reported in the literature.

TABLE II
COMPARISON OF THE PROPOSED SYSTEM WITH REPRESENTATIVE SMART DOOR LOCK SYSTEMS REFERENCED [4], [6], [7].

Study	RFID	Fingerprint	Password	Face Recognition
Sharma et al.	✓	✓	✗	✗
Thakur et al.	✓	✗	✓	✗
Almheiri et al.	✗	✓	✗	✓
Proposed System	✓	✓	✓	✓

Compared with previously reported systems, the proposed design offers a more comprehensive authentication strategy while maintaining a low-cost hardware platform based on the Arduino Mega microcontroller. The modular architecture also facilitates future integration with IoT connectivity, cloud-based monitoring, and mobile applications, making the system suitable for next-generation smart home and intelligent building applications.

VI. Conclusion

This paper presented the design, implementation, and experimental evaluation of a low-cost multi-authentication smart door lock system based on the Arduino Mega 2560 microcontroller. The proposed system successfully integrates four complementary authentication methods, namely fingerprint recognition, RFID card identification, password verification, and Python-based facial recognition using the OpenCV computer vision library, within a unified embedded platform. The modular hardware and software architecture provides a flexible and scalable solution capable of supporting multiple independent authentication mechanisms while maintaining a simple and cost-effective implementation.

Experimental evaluation confirmed reliable operation of all authentication modules under repeated laboratory testing. The proposed system demonstrated stable communication among all hardware components, accurate authentication, and consistent operation of the door locking mechanism. The integration of multiple authentication techniques improves system flexibility, enhances operational reliability, and provides users with alternative access methods under different operating conditions, making the proposed design more versatile than conventional single-factor electronic locking systems.

The proposed platform is well suited for smart homes, educational laboratories, and small commercial access control applications. Furthermore, its modular architecture facilitates future integration with Internet of Things (IoT) connectivity, cloud-based databases, mobile applications, encrypted communication protocols, and advanced artificial intelligence algorithms for improved biometric recognition and intelligent access management.

REFERENCES

[1] *Smart Lock Market – Emerging Research Report*, Emerging Research, 2024.

[2] O. Berglöf and J. Brunzell, "User Perceptions of Convenience Versus Security in Smart Locks," *Smart Locks*, 2023.

[3] Arduino, "Arduino Mega 2560 Rev3," Arduino Documentation. Available: https://docs.arduino.cc/hardware/mega-2560/

[4] A. Sharma, R. Verma, and P. Singh, "Fingerprint Based Smart Door Lock System Using Arduino," *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)*, vol. 10, no. 4, pp. 5123–5128, 2021.

[5] M. Lahmar, "Design of an RFID-Based Smart Door Lock Using ESP8266," 2022.

[6] S. Almheiri, *Exploring the Efficiencies and Vulnerabilities of Smart Door Lock Systems*. Cham, Switzerland: Springer, 2023.
[7] E. Thakur, M. Aljaidi, A. Gupta, M. Alshammari, M. Singla, S. Hussni, S. Anbarkhan, and N. Albalawi, "IoT-Enabled Smart Lock System," *Journal of Electrical Systems*, vol. 20, no. 3, 2024.
[8] M. Mansour, A. S. Omar, A. I. Omran, and M. S. Belaid, "Design and Implementation of a Fingerprint-Based Smart Door Lock Using Arduino Uno," 2024.
[9] A. Afroz, "Digital Smart Door Lock Security System Using Arduino Uno," Gurukul Kangri University, Haridwar, India, 2021.
[10] "Performance Analysis of RFID-Based Smart Door Lock Controlled by Arduino," 2022.
[11] N. K. Prabowo and I. Irwanto, "Implementation of Arduino Microcontroller Boards in Science: A Bibliometric Analysis from 2008 to 2022," 2023.
[12] H. Hamidi, "Smart Home Technologies Based on Internet of Things: A Review," *Journal of Network and Computer Applications*, vol. 153, 2020.
[13] A. K. Jain, K. Nandakumar, and A. Ross, "50 Years of Biometric Research: Accomplishments and Challenges," *Pattern Recognition Letters*, vol. 79, pp. 80–105, 2021.
[14] S. Marcel and S. Z. Li, *Handbook of Biometric Anti-Spoofing*, 2nd ed. Springer, 2023.
[15] Y. Liu, X. Chen, and J. Zhang, "Design of an IoT-Based Intelligent Door Access Control System," *IEEE Access*, vol. 10, pp. 45120–45131, 2022.
[16] M. K. Hasan, A. Almogren, M. M. Hassan, and A. Alamri, "Smart Authentication Systems for IoT Applications: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 452–490, 2022.
[17] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," *Journal of Computer and Communications*, vol. 3, no. 5, pp. 164–173, 2021.
[18] P. Viola and M. Jones, "Rapid Object Detection Using a Boosted Cascade of Simple Features," *International Journal of Computer Vision*, 2004.
[19] G. Bradski, "The OpenCV Library," *Dr. Dobb's Journal of Software Tools*, 2000.
[20] OpenCV Development Team, "OpenCV: Open Source Computer Vision Library," Available: https://opencv.org/