IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

Design and Implementation of Smart Locker System

Borate Suraj Ashok[1], Pawar Omkar Sanjay[2], Virkar Nikita Ramdas[3], Prof. Pathan Farook Firoz[4]
[*1,2,3,]Department of Electronics and Telecommunication Engineering
[*5]Guide, Department of Electronics and Telecommunication Engineering
Rajiv Gandhi College of Engineering, Parner, Maharashtra, India.

Abstract: *Traditional lock systems and single-factor electronic security methods are vulnerable to unauthorized access, key duplication, and password theft. To overcome these limitations, this project presents a secure multi-factor smart locker system using RFID authentication, PIN verification, and fingerprint recognition.*

The system is developed using an Arduino Uno microcontroller integrated with an RC522 RFID reader, 4×4 matrix keypad, R307 fingerprint sensor, LCD display, relay module, buzzer, and solenoid door lock. The authentication process is performed in three stages. First, the user scans an RFID card. If the card is recognized, the system requests a 4-digit PIN through the keypad. After successful PIN verification, fingerprint authentication is performed. Only when all three stages are verified successfully does the relay activate the solenoid lock to open the door.

For additional security, the system triggers a buzzer alarm after three incorrect attempts and temporarily locks the system to prevent unauthorized access. The proposed smart locker system provides higher security, reliability, and faster response compared to traditional locking systems, making it suitable for homes, offices, banks, laboratories, and other restricted areas.

Keywords: *fingerprint sensor*

I. INTRODUCTION

The security of physical spaces has become a major concern in modern residential, commercial, and industrial environments. Traditional mechanical locks, which have been used for decades, are no longer sufficient to provide reliable protection against modern security threats. Physical keys can be lost, stolen, or duplicated easily, while conventional electronic locking systems that rely only on passwords or PINs are vulnerable to password guessing, shoulder-surfing, and unauthorized access. These limitations create the need for a more advanced and reliable security solution capable of protecting sensitive areas and valuable assets.

To overcome these security challenges, this project proposes a Multi-Factor Authentication based Smart Locker System that combines three different layers of authentication for enhanced protection. Multi-factor authentication increases security by requiring users to verify their identity through multiple independent methods, ensuring that failure of one authentication factor does not compromise the entire system. The proposed system integrates RFID technology, PIN verification, and biometric fingerprint recognition to create a highly secure and efficient access control mechanism.

The system designed in this study is based on three distinct categories of authentication:

Something you have: An RFID card or tag is used as the first authentication layer. Only registered RFID cards are allowed to proceed further in the verification process.

Something you know: After successful RFID verification, the user must enter a valid 4-digit PIN using the keypad. This adds an additional security layer against unauthorized access.

Something you are: The final stage involves biometric fingerprint authentication using the fingerprint sensor. Since fingerprints are unique for every individual, this provides strong identity verification and prevents duplication or impersonation.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, May 2026 Impact Factor: 8.2

The proposed system is implemented using an Arduino Uno microcontroller as the central processing unit. The hardware components include an RC522 RFID reader, R307 fingerprint sensor, 4×4 matrix keypad, LCD display, relay module, buzzer, and solenoid door lock. The LCD guides the user during authentication, while the relay controls the electronic lock mechanism. Additionally, a buzzer alarm is activated after multiple failed attempts to enhance security and prevent unauthorized entry.

The working mechanism of the smart locker system follows a sequential process. Initially, the RFID card is scanned and verified. If the card is recognized, the user is prompted to enter the correct PIN. After successful PIN verification, the fingerprint sensor authenticates the user's biometric identity. Once all authentication stages are completed successfully, the relay activates the solenoid lock, allowing access to the locker. If incorrect credentials are entered repeatedly, the buzzer alarm is triggered and the system temporarily restricts access for safety purposes.

This project demonstrates how integrating embedded systems, biometric security, and electronic access control can significantly improve security compared to traditional locking systems. The developed smart locker system provides high accuracy, reliability, and fast response time, making it suitable for homes, offices, banks, laboratories, lockers, and other restricted-access environments.

II. LITERATURE REVIEW

The development of smart access control systems has progressed from traditional mechanical locks to modern electronic and biometric authentication technologies. However, as security threats continue to increase, the limitations of single-authentication systems have become a major concern. This section discusses the existing authentication methods used in smart locker systems and identifies the limitations that motivate the development of the proposed multi-factor security system.

2.1 Existing RFID Lock Systems

Radio Frequency Identification (RFID) technology is widely used in smart lock and access control systems because of its low cost, fast response time, and ease of implementation. In RFID-based systems, a reader detects and verifies a card or tag to grant access. Although these systems are convenient, they provide limited security because RFID cards can be lost, stolen, duplicated, or cloned using unauthorized devices. Since the system only verifies the RFID tag and not the actual identity of the user, unauthorized persons may gain access if they possess a valid card. Therefore, RFID-only systems are not sufficient for highly secure environments.

2.2 Biometric-only Systems

Biometric authentication systems, especially fingerprint-based systems, provide stronger security because fingerprints are unique for every individual and difficult to duplicate. These systems eliminate the need for physical keys or cards and improve user convenience. However, biometric systems also have certain limitations. Fingerprint sensors may fail to recognize authorized users due to dirty fingers, cuts, moisture, or incorrect finger placement. In some cases, low-quality sensors may also be vulnerable to spoofing attacks using artificial fingerprint replicas. Additionally, if the biometric system is used alone without additional verification methods, system security can still be compromised through hardware tampering or sensor bypassing.

2.3 PIN-based Systems

PIN or password-based authentication systems are commonly used in electronic locks because they are simple and cost-effective. In these systems, users enter a predefined numeric password using a keypad to gain access. Although PIN systems are easy to implement, they suffer from several security issues. Passwords can be guessed, shared, forgotten, or observed through shoulder-surfing attacks. If weak passwords are used, unauthorized users may easily break the system through repeated attempts. Therefore, PIN-only authentication does not provide sufficient security for sensitive applications.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

2.4 The Research Gap

A review of existing smart security systems shows that most systems rely on a single authentication technique such as RFID, PIN, or fingerprint recognition. While some advanced systems combine two methods, there are very few affordable and efficient solutions that integrate three authentication layers into a single embedded security system. Many existing systems also focus mainly on convenience rather than maximum protection. The proposed project addresses this gap by developing a triple-layer smart locker system that combines RFID authentication, PIN verification, and fingerprint recognition in a sequential process. By integrating multiple authentication methods, the weaknesses of one technique are compensated by the strengths of the others, resulting in improved security, reliability, and protection against unauthorized access.

III. METHODOLOGY

The methodology of this project focuses on the integration of multiple hardware components and a sequential authentication process to create a highly secure smart locker system. The system combines RFID verification, PIN authentication, and fingerprint recognition to provide multi-layer protection against unauthorized access. The complete methodology is divided into hardware architecture and authentication logic.

System Architecture and Hardware Integration

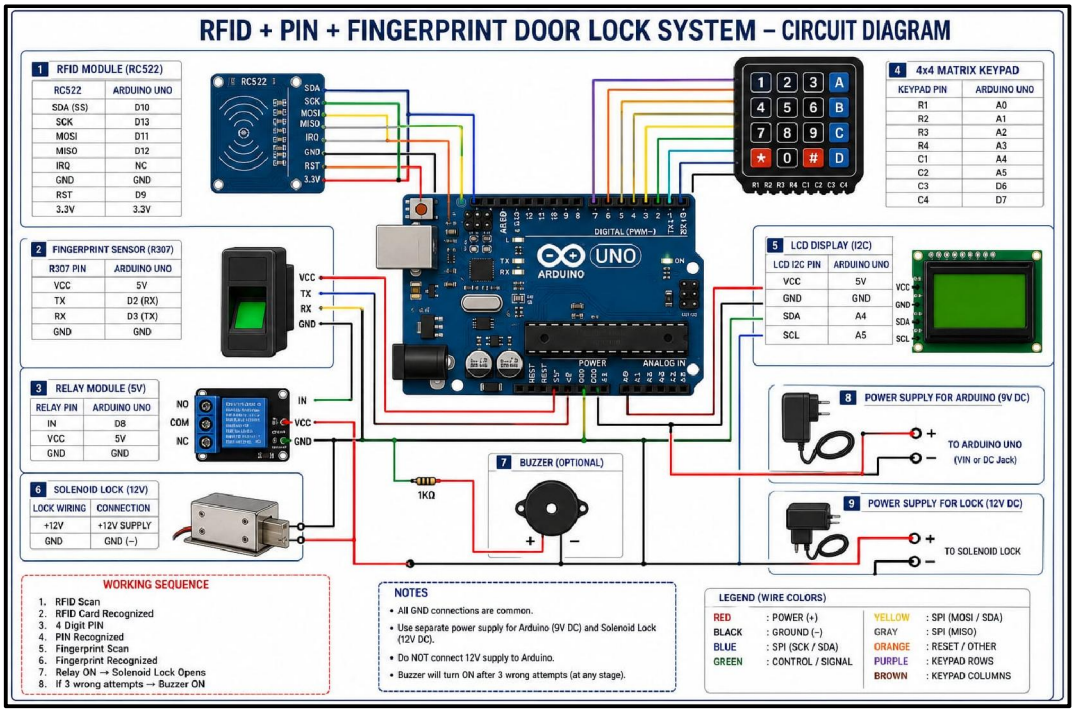
The core of the system is a central processing unit—typically an Arduino Uno or an ESP32 microcontroller which acts as the gateway controller [1]. The hardware is integrated through a series of peripheral modules:

- **RFID Module (RC522):** Used for the first-level authentication by scanning RFID cards or tags.
- **Fingerprint Sensor (R307):** Captures and verifies the fingerprint of the authorized user for biometric authentication.
- **4×4 Matrix Keypad:** Allows users to enter a secure 4-digit PIN as the second authentication layer**.**
- **LCD Display (I2C):** Displays system instructions, authentication status, and error messages to the user.
- **Relay Module:** Controls the electronic locking mechanism based on authentication results.
- **Solenoid Door Lock:** Acts as the physical locking device that opens only after successful verification.
- **Buzzer Alarm:** Provides security alerts during unauthorized access attempts or repeated failed authentications.

The Arduino Uno processes the data received from all authentication modules and controls the relay and buzzer according to the programmed logic. [2].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

Authentication Logic



The smart locker system follows a strict sequential authentication process. Each stage must be completed successfully before moving to the next stage. This layered verification approach improves overall system security.[4].

Step 1: RFID Check: The authentication process begins when the user places an RFID card near the RC522 reader. The Arduino reads the Unique Identification Number (UID) of the card and compares it with the stored authorized IDs. If the RFID card is valid, the system proceeds to the PIN verification stage. If the card is invalid, access is denied and the system remains locked..

Step 2: PIN Verification: After successful RFID authentication, the user is prompted to enter a 4-digit PIN using the keypad. The entered PIN is compared with the stored password in the microcontroller memory. If the PIN is correct, the fingerprint authentication stage is activated. If an incorrect PIN is entered, the system denies access and records the failed attempt[3].

Step 3: Fingerprint Authentication: Once the RFID and PIN are verified, the user places a finger on the R307 fingerprint sensor. The sensor captures the fingerprint image and compares it with pre-registered fingerprint templates stored in the sensor memory. If the fingerprint matches successfully, the system grants access by activating the relay module and unlocking the solenoid lock. [2], [4],[3].

Technical Decision Logic

The operational flow is governed by a Boolean "AND" logic gate. The electronic lock will only trigger a "HIGH" signal to the relay when all conditions are simultaneously satisfied within a set timeframe.

The system's decision-making logic can be represented as follows:

```
IF (RFID_Status == VALID)
  AND (PIN_Status == CORRECT)
  AND (Fingerprint_Status == MATCHED)
THEN
  ACTIVATE Relay
  OPEN Solenoid Lock
```


DOI: 10.48175/IJARSCT-35624

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, May 2026 Impact Factor: 8.2

DISPLAY "Access Granted"
ELSE
KEEP System Locked
ACTIVATE Buzzer Alarm
DISPLAY "Unauthorized Access"
RESET Authentication Process

This multi-factor authentication mechanism ensures that even if one security layer is compromised, unauthorized access cannot be achieved without passing the remaining authentication stages.[4], [5][1].

Results and Discussion

The proposed smart locker system was implemented and tested under different real-time conditions to evaluate its performance, reliability, and security effectiveness. The testing focused on the accuracy of authentication modules, response time, and system reliability.

Experimental Setup

The prototype was constructed using the ESP32 microcontroller as the central processing unit, chosen for its dual-core processing capability and built-in Wi-Fi and Bluetooth functionalities [1].

The following hardware components were integrated:

Arduino Uno: Used as the main controller for processing authentication data and controlling system operations.
RC522 RFID Reader: Operates at 13.56 MHz for RFID card detection and verification.
R307 Fingerprint Sensor: Used for biometric fingerprint matching with high accuracy.
4×4 Matrix Keypad: Used for secure PIN entry.
LCD Display: Provides user interaction and displays authentication messages.
Relay Module and Solenoid Lock: Used for physical locking and unlocking operations.
Buzzer: Used for security alerts during failed access attempts.

IV. PERFORMANCE ANALYSIS AND RESULTS

The system was tested with multiple authorized and unauthorized users to evaluate its accuracy and latency.

Authentication Accuracy: The RFID module successfully detected and verified authorized RFID cards within a range of approximately 2–3 cm. The fingerprint sensor demonstrated reliable performance and accurately matched registered fingerprints under normal conditions. The keypad correctly validated the entered PIN without significant delay.[2]

Response Time : The overall authentication process was completed within a few seconds. RFID scanning and PIN verification occurred almost instantly, while fingerprint matching required slightly more processing time. The relay activated immediately after successful verification, resulting in fast and smooth operation of the solenoid lock.[1], [4].

System Reliability: The sequential authentication logic ensured that access was granted only when all three authentication stages were completed successfully. During testing, the system consistently denied access when incorrect RFID cards, wrong PINs, or unmatched fingerprints were used. After three failed attempts, the buzzer alarm was triggered and the system temporarily blocked further access attempts.[2].

Security Enhancement: The integration of RFID, PIN, and fingerprint authentication significantly improved security compared to traditional single-factor lock systems. Even if an RFID card was stolen, unauthorized users could not access the system without the correct PIN and fingerprint. This layered approach increased protection against duplication, guessing attacks, and unauthorized entry.

The final results demonstrate that the proposed multi-factor smart locker system provides high security, reliability, fast response time, and stable operation, making it suitable for homes, offices, banks, laboratories, and other restricted-access environments.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, May 2026
Impact Factor: 8.2

V. DISCUSSION

The experimental results show that the proposed multi-factor smart locker system provides better security and reliability compared to traditional single-factor systems. RFID-only systems are vulnerable to card duplication, while fingerprint-only systems may experience recognition errors or spoofing attacks [1], [2]. By combining RFID authentication, PIN verification, and fingerprint recognition, the system ensures that access is granted only after successful completion of all authentication stages [3].

Although the multi-step authentication process slightly increases access time, it significantly improves protection against unauthorized entry [4]. During testing, the system operated accurately and consistently denied access when incorrect credentials were used. The relay-controlled solenoid lock and buzzer alarm functioned effectively, enhancing overall system security [2].

The system also supports monitoring and logging of access attempts, making it suitable for smart security applications in homes, offices, lockers, laboratories, and other restricted environments [1], [5]. Overall, the proposed system demonstrates improved security, reliability, and operational efficiency compared to conventional locking methods.

VI. CONCLUSION

The design and implementation of the proposed multi-factor smart locker system successfully demonstrate that security can be greatly improved through layered authentication techniques. By integrating RFID authentication, PIN verification, and fingerprint recognition, the system provides stronger protection against unauthorized access compared to traditional single-factor locking systems. The combination of these authentication methods reduces the risks associated with card duplication, password guessing, and biometric spoofing.

The experimental evaluation confirms that the sequential "AND" logic used in the system allows access only when all authentication stages are successfully verified. The relay-controlled solenoid lock operated reliably, while the buzzer alarm effectively prevented unauthorized access attempts. Although the multi-step authentication process slightly increases access time, it provides a higher level of security, reliability, and user safety.

The use of affordable and easily available components such as the Arduino Uno, RC522 RFID module, R307 fingerprint sensor, keypad, and solenoid lock makes the system cost-effective, scalable, and suitable for practical implementation. The proposed smart locker system can be effectively used in homes, offices, banks, laboratories, lockers, and other restricted-access environments requiring enhanced security.

Overall, this project presents a reliable, intelligent, and efficient security solution for modern access control systems and provides a strong foundation for future improvements in smart security and automation technologies.

REFERENCES

[1] T. Adeleke and O. Akinwale, "IoT-driven RFID attendance system for workforce management," in *Proceedings of the 2021 IEEE 5th International Conference on Internet of Things*, 2021, pp. 122–128.

[2] V. Anand and P. Karthik, "Smart campus attendance using RFID and cloud services," *International Journal of Smart Sensor and Ad Hoc Networks*, vol. 12, no. 4, pp. 91–97, 2022.

[3] A. Bose and S. Chatterjee, "IoT-based RFID attendance system with mobile app integration," *International Journal of Smart Systems and Applications*, vol. 6, no. 2, pp. 55–63, 2023.

[4] R. Chowdhury and A. Das, "Wi-Fi based attendance monitoring system using ESP8266," *International Journal of Engineering and Computer Science*, vol. 9, no. 6, pp. 24478–24482, 2020.

[5] D. Gupta, P. Kaur, and S. Bhatt, "Cloud integrated RFID attendance system for educational institutions," *Journal of Engineering Science and Technology*, vol. 17, no. 1, pp. 85–94, 2022.

[6] R. Jain and S. Patel, "Future trends in RFID and IoT-based attendance automation," in *Proceedings of the 2023 International Conference on Emerging Technologies in Computing*. Springer, 2023, pp. 411–416.

[7] M. Joshi and R. Deshmukh, "Automation of attendance system using RFID and IoT technologies," *International Journal of Engineering Research and Technology*, vol. 8, no. 7, pp. 227–231, 2019.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, May 2026 Impact Factor: 8.2

[8] S. Kumar, P. Meena, and V. Jha, "IoT-enabled RFID attendance monitoring system," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 8, no. 9, pp. 2034–2040, 2020.
[9] N. Patel and R. Singh, "RFID with GSM module for real-time attendance notification," *International Journal of Emerging Technologies in Engineering Research*, vol. 7, no. 5, pp. 89–93, 2019.
[10] N. Prasad and A. Kumar, "RFID-based smart attendance system with IoT integration," *International Journal of Information and Computer Security*, vol. 14, no. 3, pp. 187–195, 2022.
[11] M. Rahman and M. Alam, "Smart attendance system using IoT and cloud computing," *International Journal of Computer Trends and Technology*, vol. 69, no. 12, pp. 32–38, 2021.
[12] K. Ramesh and F. Ali, "Hybrid biometric-RFID authentication system for secure access," *International Journal of Computer Applications*, vol. 183, no. 29, pp. 17–23, 2021.
[13] K. Sahu and S. Pandey, "IoT-based RFID attendance and access control system," *International Journal of Scientific Research in Computer Science and Engineering*, vol. 9, no. 2, pp. 59–65, 2021.
[14] R. Sharma, A. Gupta, and M. Bansal, "RFID-based attendance system using Arduino," *International Journal of Advanced Research in Computer Science*, vol. 9, no. 3, pp. 45–49, 2018.
[15] A. Singh and D. Patel, "IoT-based attendance system using ESP8266 and RFID," in *Proceedings of the International Conference on Smart Computing and Communication*. IEEE, 2020, pp. 456–460.