



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

RFID Integrated Smart Access Control Equipment

Mohammed Ayan¹, Dr. Malatesh S H², Shabaz pasha³, Mohith Kiran G⁴, Sane Sai Srikanth⁵

UG Scholar, Dept. of Computer Science and Engineering, M S Engineering College, Bangalore, India¹

Head of Department, Dept. of Computer Science and Engineering, M S Engineering College, Bangalore, India

UG Scholar, Dept. of Computer Science and Engineering, M S Engineering College, Bangalore, India³

UG Scholar, Dept. of Computer Science and Engineering, M S Engineering College, Bangalore, India⁴

UG Scholar, Dept. of Computer Science and Engineering, M S Engineering College, Bangalore, India⁵

ABSTRACT: Access control systems are widely used to restrict unauthorized entry in laboratories, offices, and other secure areas. Many existing systems rely on a single authentication method such as RFID or password-based access, which can be compromised due to card loss, cloning, or password leakage.

In this work, a smart access control system using multi-factor authentication is designed and implemented using an ESP32 microcontroller. The proposed system integrates RFID authentication, PIN verification through a keypad, and mobile-based access, allowing the administrator to configure different security levels based on requirements.

The system includes an admin mode for managing authorized users, a lockout mechanism after multiple incorrect attempts, and a relay-controlled solenoid lock for physical access control. During implementation, power stability and hardware interaction challenges were observed and addressed through regulated power supply usage.

The developed system provides a low-cost, flexible, and customizable security solution suitable for academic institutions and controlled environments.

KEYWORDS: Access Control System, ESP32, RFID, Multi-Factor Authentication, Smart Lock, Embedded Security.

I. INTRODUCTION

Security and access control have become important concerns in educational institutions, offices, laboratories, and other restricted environments. Traditional locking systems such as mechanical keys or single-factor electronic locks provide limited protection, as keys can be duplicated and electronic credentials like RFID cards or passwords can be misused. Due to these limitations, there is a growing need for access control systems that offer higher security while remaining cost-effective and easy to deploy.

Many existing electronic access control systems rely on a single authentication method, such as RFID or PIN-based verification. Although these methods are convenient, they are vulnerable to threats like card loss, cloning, password guessing, and unauthorized sharing. To overcome these issues, multi-factor authentication (MFA) can be used, where access is granted only after verifying more than one independent factor. This approach significantly increases security by reducing the risk associated with any single authentication method.

In this project, a smart access control system using multi-factor authentication is designed and implemented using an ESP32 microcontroller. The system integrates RFID authentication, keypad-based PIN entry, and mobile-based access, allowing flexibility in selecting the required security level. An administrator can configure the system to operate in single-factor, two-factor, or three-factor authentication modes depending on the application.

The proposed system also includes features such as admin mode for managing users, lockout after repeated incorrect attempts, and visual feedback using an OLED display. During implementation, practical challenges related to power stability and hardware integration were encountered, which helped in understanding real-world constraints of embedded security systems. The objective of this work is to develop a low-cost, customizable, and reliable access control solution suitable for controlled environments.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. METHODOLOGY

The methodology describes the design approach and working procedure followed to develop the proposed smart access control system. The system is designed by integrating both hardware and software components to achieve secure and reliable access control using multiple authentication factors.

2.1 Hardware Components

The core controller used in this system is the ESP32 microcontroller, selected due to its low cost, sufficient processing capability, and built-in communication features. The following hardware components are used:

RFID Reader (RC522): Used to read the unique identification number of authorized RFID cards.

Keypad Module: Allows users to enter a personal identification number (PIN) as an additional authentication factor.

OLED Display: Displays system status messages such as access granted, access denied, and error notifications.

Relay Module: Acts as an interface between the microcontroller and the locking mechanism.

Solenoid Lock: Provides physical locking and unlocking of the door.

Power Supply Unit: Supplies regulated voltage to ensure stable operation of the system.

All components are interconnected with the ESP32 using suitable communication protocols such as SPI, I2C, and digital GPIO pins.

2.2 Software Design

The software logic of the system is developed using the Arduino programming environment. The program continuously monitors user input from the RFID reader, keypad, and mobile interface.

The authentication process follows a step-by-step verification procedure:

The system waits for an RFID card scan.

If the card is valid, the system prompts the user to enter a PIN using the keypad.

In higher security modes, mobile-based authentication is also required.

If all required authentication factors are verified successfully, access is granted.

If authentication fails, the system displays an error message and increments the attempt counter.

To enhance security, a lockout mechanism is implemented. If a user enters incorrect credentials multiple times, the system temporarily disables access and requires administrator intervention.

2.3 Admin Mode Operation

An administrator mode is included to manage system configuration. Using a predefined admin credential, the administrator can:

Add or remove authorized RFID cards

Change PIN values

Configure the number of authentication factors

Reset lockout conditions



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This feature makes the system flexible and adaptable for different security requirements.

2.4 Practical Implementation Considerations

During implementation, several practical challenges were observed, particularly related to power stability and hardware interaction. Sudden voltage drops and improper power regulation affected system performance, highlighting the importance of using a stable power supply. These issues were addressed by improving power management and ensuring proper grounding of all components.

III. SYSTEM ARCHITECTURE AND WORKING FLOW

The system architecture defines how the hardware and software components interact to perform secure access control. The proposed system is designed in a modular manner so that each component performs a specific function while working together as a complete unit.

RFID Smart Access Control - Block Diagram

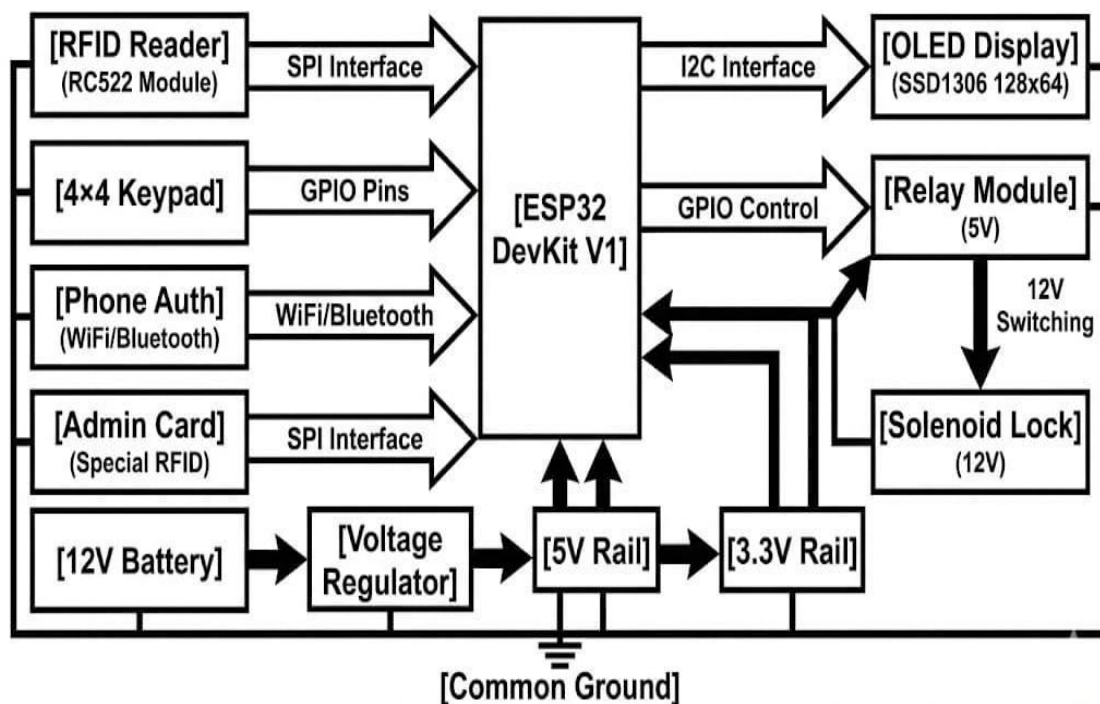


Fig1. System Block Diagram

3.1 System Architecture

The architecture of the smart access control system consists of five main blocks:

Input Unit

This unit includes the RFID reader, keypad, and mobile interface. These components are responsible for collecting authentication inputs from the user.

Processing Unit

The ESP32 microcontroller acts as the central processing unit. It processes the input data, verifies authentication credentials, and executes the decision logic based on the configured security level.

Display and Alert Unit



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

An OLED display provides real-time feedback such as system status, authentication prompts, and access messages. A buzzer is used to indicate successful or failed authentication attempts.

Control Unit

The relay module functions as a switching interface between the ESP32 and the solenoid lock. It ensures safe electrical isolation while controlling the locking mechanism.

Locking Mechanism

The solenoid lock physically locks or unlocks the door based on the authentication result.

All components share a common power source and ground connection to ensure synchronized operation. Communication between modules is achieved using standard protocols such as SPI, I2C, and digital GPIO signals.

3.2 Working Flow of the System

The working flow of the system follows a structured sequence to ensure secure access control:

When power is supplied, the system initializes all hardware modules.

The OLED display shows a prompt requesting user authentication.

The user scans an RFID card using the reader.

If the RFID card is valid, the system requests PIN input through the keypad.

In higher security modes, mobile-based authentication is also required.

The ESP32 verifies all provided credentials.

If authentication is successful, the relay is activated and the solenoid lock is released.

If authentication fails, an error message is displayed and the attempt count is increased.

After multiple incorrect attempts, the system enters lockout mode to prevent misuse.

The door automatically locks again after a predefined time delay.

This step-by-step flow ensures that unauthorized access is minimized while maintaining user convenience.

3.3 Security Levels

The system supports multiple security configurations:

Single-Factor Authentication: RFID only

Two-Factor Authentication: RFID + PIN

Three-Factor Authentication: RFID + PIN + Mobile access

The administrator can select the appropriate security level based on the application requirements.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. IMPLEMENTATION DETAILS

This section explains the practical implementation of the proposed smart access control system, including hardware interfacing, software logic, and system behavior during operation. The implementation focuses on reliability, ease of use, and security.

4.1 Hardware Implementation

All hardware components are connected to the ESP32 microcontroller based on their communication requirements:

The RFID RC522 module is interfaced using the SPI protocol to ensure fast and reliable card detection.

The keypad is connected through digital GPIO pins to allow PIN entry.

The OLED display is interfaced using the I2C protocol to display system messages and prompts.

The relay module is controlled through a GPIO pin and is used to switch the solenoid lock safely.

The solenoid lock is powered separately and activated through the relay to avoid overloading the microcontroller.

Proper grounding and voltage regulation are maintained to ensure stable operation. Special attention is given to power distribution, as unstable power supply was observed to affect system performance during testing.

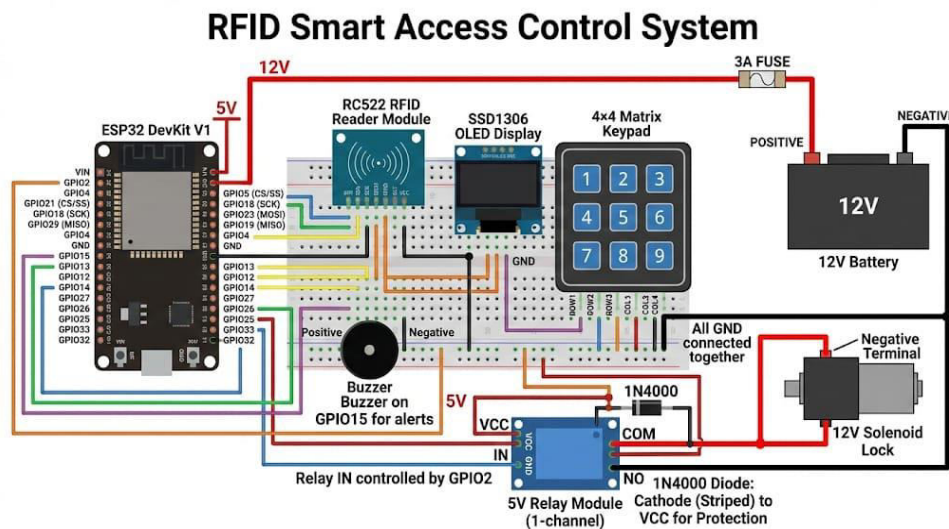


Fig.2. Circuit Wiring Diagram

4.2 Software Implementation

The system software is developed using the Arduino IDE. The program is structured into different functional modules to improve readability and maintenance. These modules handle RFID scanning, keypad input, display updates, authentication logic, and lock control.

The ESP32 continuously monitors input devices and processes authentication requests based on the configured security mode. Conditional logic is used to enable or disable authentication factors such as PIN or mobile access.

A timer-based mechanism is implemented to:

Automatically re-lock the door after access is granted



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Control lockout duration after multiple failed attempts

Error handling routines are included to prevent system crashes during unexpected input or communication failures.

Authentication Process - Smart Access Control System

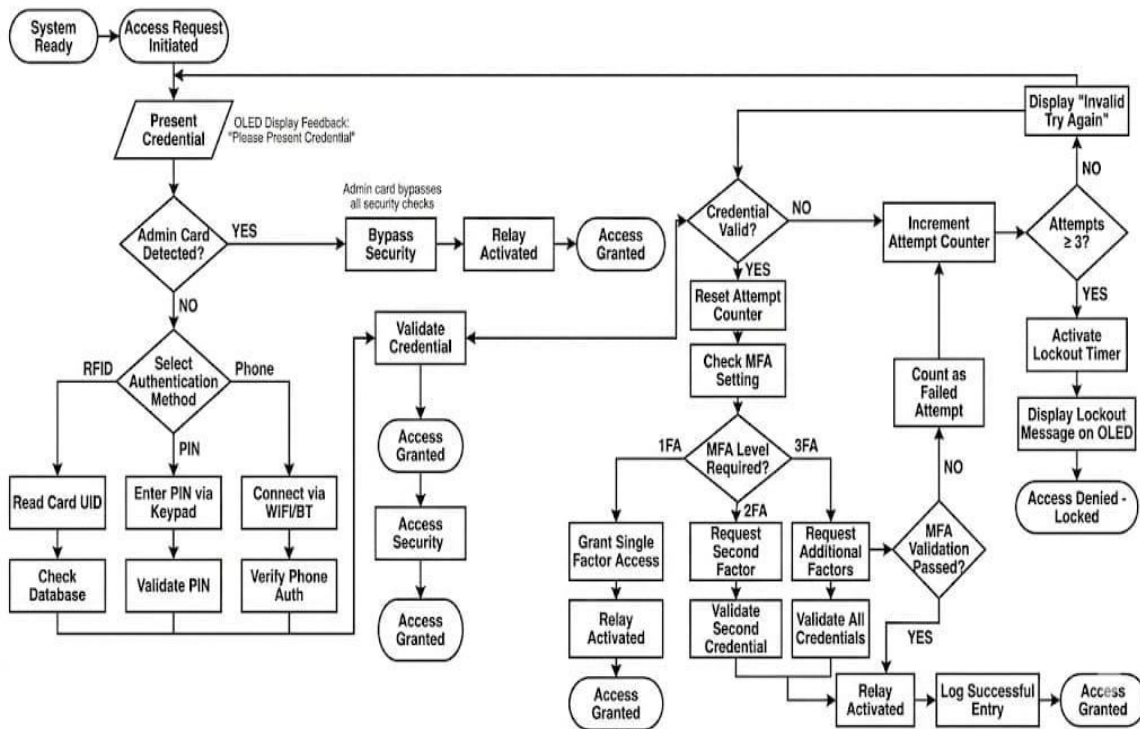


Fig3. Authentication Flowchart

4.3 Authentication Logic

The authentication logic is implemented using a sequential verification approach:

Each authentication factor is verified one after another.

If any verification step fails, access is denied immediately.

Successful verification of all required factors results in unlocking the door.

An attempt counter is maintained to track incorrect entries. If the number of failed attempts exceeds a predefined limit, the system enters lockout mode, temporarily disabling further access attempts.

4.4 Testing and Debugging

The system is tested under different conditions to evaluate reliability and response time. Testing includes:

Multiple RFID scans

Correct and incorrect PIN entries

Power cycling behavior

Lock activation and release timing

During testing, issues related to power stability and peripheral initialization were observed. These issues were addressed by adjusting power connections and adding initialization delays in the software.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

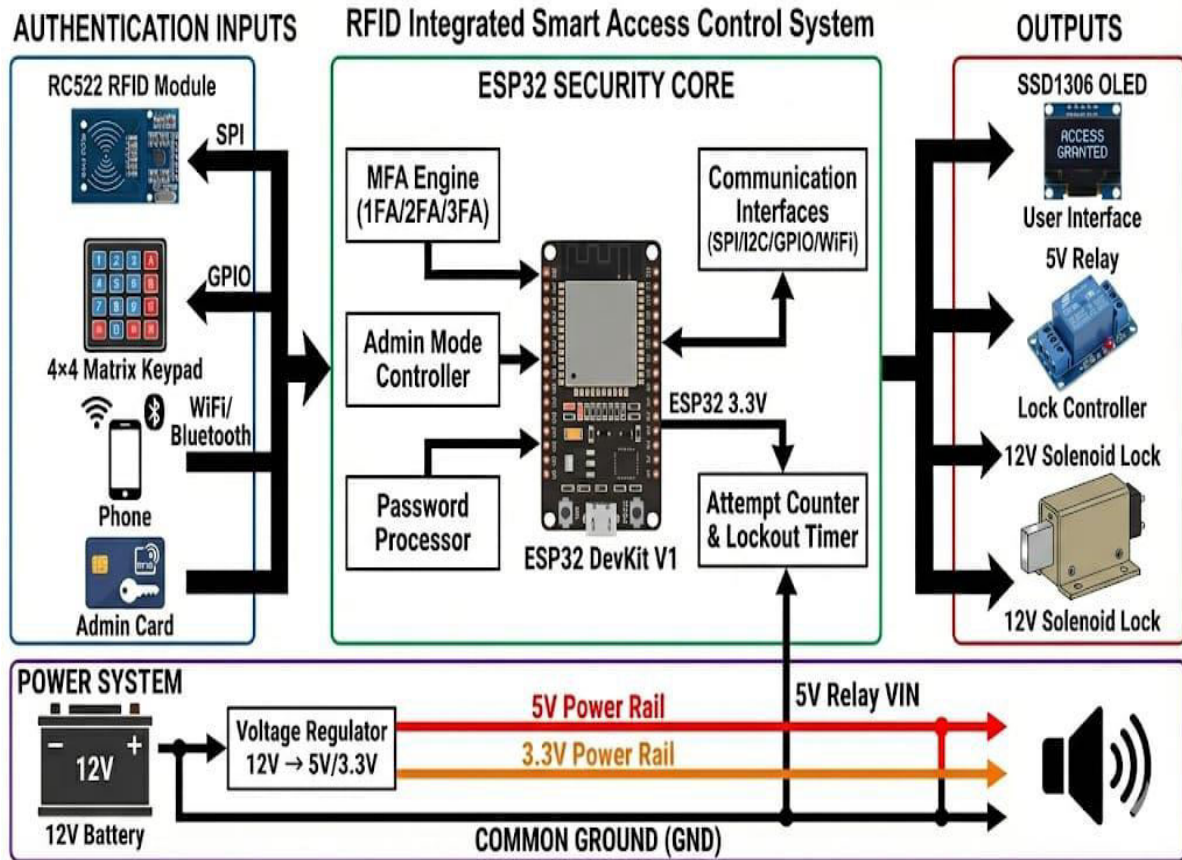


Fig4. System Architecture Diagram

V. RESULTS AND DISCUSSION

This section discusses the outcomes obtained after implementing and testing the proposed smart access control system. The system was evaluated based on functionality, reliability, and security performance.

5.1 Functional Results

The developed system successfully performed multi-factor authentication using RFID, PIN entry, and mobile-based access as configured. The following observations were made during testing:

The RFID module correctly detected authorized cards and rejected unknown cards.

The keypad allowed accurate PIN entry and displayed appropriate messages for correct and incorrect inputs.

The OLED display provided clear feedback such as authentication prompts, access status, and error notifications.

The relay and solenoid lock operated correctly, unlocking the door only after successful authentication.

The lock automatically re-engaged after a predefined time interval.

These results confirm that the system functions as intended under normal operating conditions.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

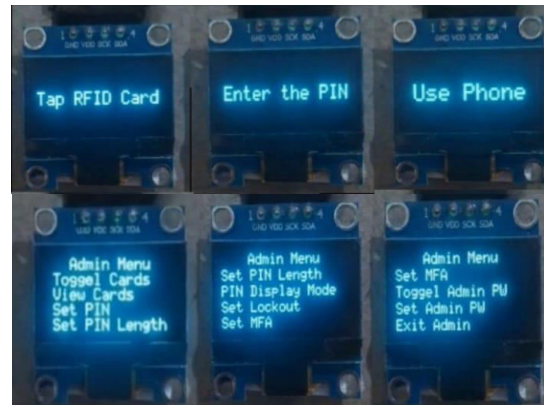


Fig 5. Functional Results

5.2 Security Performance

The use of multi-factor authentication significantly improved system security compared to single-factor systems. Even if one authentication factor was compromised, unauthorized access was prevented by the remaining factors.

The lockout mechanism further enhanced security by temporarily disabling access after multiple incorrect attempts, reducing the risk of brute-force attacks.

5.3 Reliability and Practical Observations

During extended testing, the system showed reliable performance when powered using a regulated power supply. However, instability was observed when using unregulated or low-current power sources. This highlighted the importance of proper power management in embedded security systems.

Minor delays were introduced in the software to ensure proper initialization of all peripherals, which improved system stability during startup.

5.4 Discussion

The results demonstrate that the proposed system provides an effective balance between security and usability. While higher authentication levels increase security, they may slightly increase user interaction time. Therefore, the ability to configure authentication levels makes the system adaptable for different applications.

Overall, the system achieved its design objectives and proved suitable for controlled access environments such as laboratories and restricted rooms.

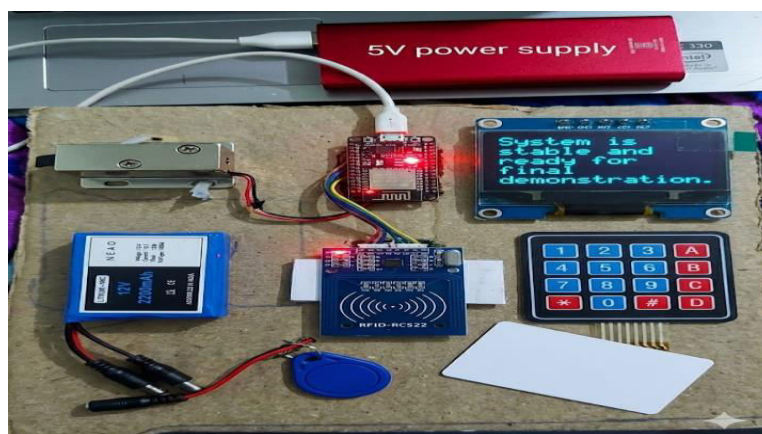


Fig6. Final Hardware Implementation of the Smart Access Control System



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. LIMITATIONS

Although the proposed smart access control system demonstrates effective functionality, certain limitations were identified during implementation and testing. These limitations are mainly related to hardware constraints and practical operating conditions.

One of the primary limitations of the system is its dependency on stable power supply. During testing, it was observed that fluctuations in power input could affect system initialization and peripheral communication. This highlights the need for proper power regulation, especially in real-world deployments.

The system currently relies on RFID cards and PIN-based authentication, which may be vulnerable if RFID cards are lost, cloned, or shared. While multi-factor authentication reduces this risk, the absence of biometric verification limits the overall security level.

Another limitation is the lack of centralized data logging. The system operates locally and does not store access logs on a cloud server or database. As a result, long-term monitoring and remote audit of access records are not supported.

The physical security of the system also depends on proper installation. If hardware components such as wiring or modules are exposed, they may be vulnerable to tampering. Additional protective enclosures would be required for deployment in high-risk environments.

Despite these limitations, the system provides a strong foundation for secure access control and can be enhanced further through future improvements.

VII. FUTURE SCOPE

The proposed smart access control system can be further enhanced by incorporating additional features to improve security, scalability, and usability. One possible improvement is the integration of biometric authentication, such as fingerprint or facial recognition, which would add another strong security layer and reduce dependency on physical cards.

Another important future enhancement is the implementation of cloud-based data logging. Storing access records on a remote server would allow administrators to monitor entry logs, analyze usage patterns, and perform audits remotely. This feature would be especially useful in large institutions and organizations.

The system can also be extended with mobile application integration, enabling users to manage access permissions, receive alerts, and unlock doors remotely through a secure app. This would improve user convenience and administrative control.

In addition, incorporating artificial intelligence techniques for anomaly detection could help identify suspicious access behavior, such as repeated failed attempts or unusual access timings. This would further strengthen the security of the system.

These enhancements can be implemented without major changes to the existing hardware, making the proposed system flexible and scalable for future developments.

VIII. CONCLUSION

In this work, a smart access control system using multi-factor authentication was successfully designed and implemented using an ESP32 microcontroller. The system integrates RFID authentication, PIN verification through a keypad, and mobile-based access to provide enhanced security compared to traditional single-factor access control methods.

The developed system demonstrated reliable performance during testing, allowing access only to authorized users while preventing unauthorized entry through multiple security layers. Features such as admin mode, lockout mechanism after



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

repeated incorrect attempts, and automatic door locking contributed to improved system safety and flexibility. The use of an OLED display and buzzer provided clear user feedback, making the system easy to operate.

Practical challenges related to power stability and hardware integration were encountered during implementation, which highlighted the importance of proper power regulation and testing in embedded systems. Addressing these challenges improved system reliability and provided valuable hands-on learning experience.

Overall, the proposed system offers a cost-effective, customizable, and secure solution suitable for controlled environments such as laboratories, offices, and academic institutions. With further enhancements, the system can be extended to support advanced security features and large-scale deployments.

REFERENCES

1. Juels, "RFID Security and Privacy: A Research Survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381–394, Feb. 2006.
2. K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 3rd ed., Wiley, 2010.
3. D. G. Waddington and P. Cole, "Multi-Factor Authentication Systems: Concepts and Challenges," International Journal of Computer Applications, vol. 178, no. 7, pp. 20–25, 2019.
4. A . Kumar and Y. Zhou, "Human-Centric Smart Lock Systems Using IoT," International Journal of Engineering Research and Technology (IJERT), vol. 9, no. 6, pp. 115–120, 2020.
5. P. Soni and R. Patel, "Design and Implementation of Smart Door Lock System Using IoT," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 8, no. 4, pp. 1432–1437, 2019.
6. Dr. Malatesh S. H, S. Kattimani, P. Pallabavi, V. A. P, and D. M. G, "Intruder Detection and Protection System," International Journal of innovation Research in Technology (IJIRT), vol. 11, no. 12, p. 6287, May 2025, ISSN: 2349-6002.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details