International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 1, Jan-Feb 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Smart Door Lock System with Multi-Level Authentication

Bhagyesh Pawar[1], Vaibhav Deore[2], Tushar Savkar[3], Mrs. Y. R. Thakare[4]
Student at Computer Technology, SNJB's Shri Hiralal Hastimal (Jain Brothers, Jalgaon) Polytechnic Chandwad, Nashik[1,2,3]
Professor at Computer Technology, SNJB's Shri Hiralal Hastimal (Jain Brothers, Jalgaon) Polytechnic Chandwad, Nashik[4]
Email: bhagyesh0507@gmail.com, vaibhavdeore9812@gmail.com, sawakar373@gmail.com

----------**********----------

Abstract:

Security of residential and commercial premises has become a major concern due to increasing incidents of unauthorized access, theft, and security breaches. Traditional mechanical locking systems suffer from several drawbacks such as key duplication, loss of keys, lack of access control, and absence of monitoring facilities. Although modern smart locks provide enhanced security, many of them rely heavily on continuous internet connectivity, making them unreliable during network failures.

This project presents the design and implementation of a Smart Door Lock System with Multi-Level Authentication using the ESP32 microcontroller. The proposed system enhances security by integrating three authentication layers: Touch pattern authentication, RFID-based verification, and IR sensor-based presence detection. The touch pattern acts as the first level of security, allowing users to define a custom tap sequence stored securely in EEPROM. Upon successful pattern verification, RFID authentication is enabled, ensuring that only authorized RFID cards can proceed further. Finally, an IR sensor detects human presence near the door, preventing accidental or unauthorized unlocking.

A servo motor is used as the physical locking mechanism, providing precise and controlled locking and unlocking of the door. The system operates completely offline for authentication, ensuring uninterrupted security even during internet failure, while Wi-Fi is used only for optional web-based monitoring and control. Experimental results demonstrate reliable performance, fast response time, low power consumption, and cost-effective implementation. The system is suitable for homes, offices, and restricted areas requiring enhanced access control.

Keywords — **ESP32, Smart Door Lock, Multi-Level Authentication, Touch Pattern, RFID, IR Sensor, Servo Motor, EEPROM, IoT Security.**

----------**********----------

I. INTRODUCTION

Security systems have evolved significantly from traditional lock-and-key mechanisms to electronic and intelligent access control systems. Conventional door locks provide limited security and are vulnerable to key duplication, loss, or forced entry. With advancements in embedded systems and microcontroller technology, smart locking systems have gained popularity due to their enhanced security, flexibility, and automation capabilities.

Smart door lock systems aim to restrict access only to authorized individuals using electronic authentication techniques such as passwords, biometric verification, RFID cards, or mobile applications. However, many existing smart locks depend entirely on cloud connectivity and mobile applications, which can fail during internet outages, reducing system reliability.

To overcome these limitations, the proposed system introduces a multi-factor authentication approach that combines touch-based pattern recognition, RFID verification, and sensor-based presence detection. By implementing offline authentication with optional online monitoring, the system ensures high reliability, improved security, and ease of use.

II. LITERATURE REVIEW

Several researchers have explored smart door lock systems using different authentication techniques:

- Kumar and Patil (2021) proposed an IoT-based smart door lock system using mobile applications, highlighting improved convenience

but increased dependency on internet connectivity.

- Sharma and Singh (2020) developed an RFID-based access control system that allows only authorized cards but lacks multi-factor authentication.

- Joshi and Deshmukh (2022) implemented a smart lock using ESP32 and sensors, demonstrating the effectiveness of sensor-based security mechanisms.

- Verma and Kulkarni (2023) discussed a multi-factor authentication system combining password and RFID, emphasizing enhanced security over single-factor systems.

From the literature review, it is observed that multi-level authentication combined with offline operation significantly improves system security and reliability. This project builds upon these concepts by integrating touch pattern authentication, RFID verification, and IR sensor detection using a single ESP32 controller.

III. PROBLEM STATEMENTS

Most existing door locking systems suffer from one or more of the following problems:

- Dependence on physical keys that can be lost or duplicated
- Single-factor authentication that is vulnerable to unauthorized access
- Complete dependency on internet connectivity
- Lack of flexibility and customization
- High cost of biometric systems

Therefore, there is a need for a low-cost, reliable, and secure smart door lock system that provides multi-factor authentication and operates efficiently even without internet connectivity.

IV. SYSTEM ARCHITECTURE

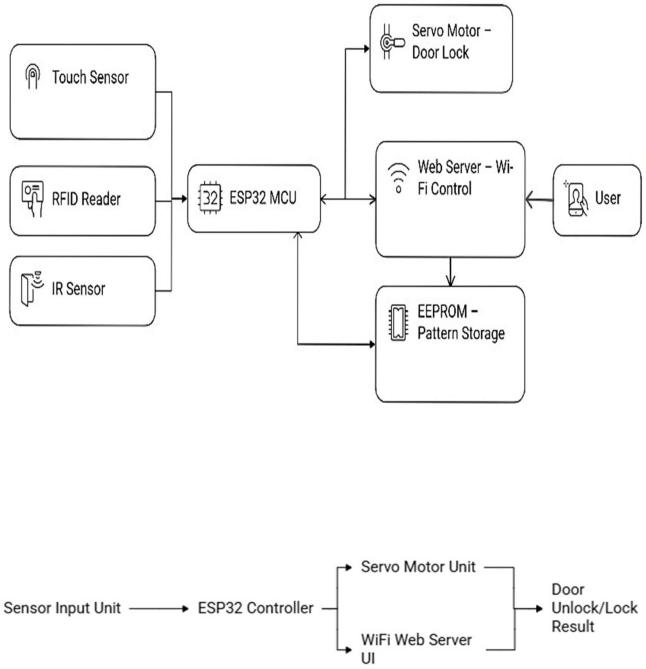


Figure: System Flow Diagram

V. DESIGN AND IMPLEMENTATION CONSTRAINTS

6.1 External Interface Requirements

- Touch sensor interface for user input
- RFID reader interface via SPI
- IR sensor digital input
- Servo motor PWM output
- Web interface for monitoring and control

6.2 Other Non-Functional Requirements

Performance Requirements:

- Fast authentication response
- Reliable offline operation
- Accurate servo motor control
- Low power consumption

6.3 Software and Hardware Requirements

Software Requirements:

- Arduino IDE
- ESP32 board support package

- Embedded C/C++
- Web browser for monitoring

Hardware Requirements:

- ESP32 microcontroller
- Touch sensor module (TTP223)
- RFID RC522 module
- IR sensor
- Servo motor
- Power supply (5V)

VI. TEST CASES

Test Case	Input	Expected Output	Status
Touch pattern correct	User Define set pattern	Proceed to RFID	Pass
Wrong pattern	Random taps	System reset	Pass
Valid RFID	Authorized card	IR enabled	Pass
Invalid RFID	Unknown card	Access denied	Pass
IR detected	Human presence	Door unlock	Pass

Requirement Gathering and Analysis

The requirement gathering and analysis phase involves identifying the functional and non-functional needs of the Smart Door Lock System. Functional requirements include secure door locking and unlocking, multi-level authentication using touch pattern, RFID verification, and IR-based presence detection. Non-functional requirements focus on system reliability, offline operation, low power consumption, and ease of use. During this phase, hardware components such as ESP32, RFID reader, touch sensor, IR sensor, and servo motor were selected based on cost, availability, and performance. The analysis ensured that the system meets security needs while remaining affordable and reliable.

System Design

The system design phase defines the overall structure of the smart door lock system. A layered architecture is adopted, consisting of input devices (touch sensor, RFID reader, IR sensor), a processing unit (ESP32 microcontroller), and an output device (servo motor lock). The system follows a state-based authentication design, where each authentication step must be successfully completed before moving to the next stage. The design also includes EEPROM for permanent storage of the touch pattern and an optional web interface for monitoring and control.

Implementation

In the implementation phase, the system is developed using the Arduino IDE and programmed in embedded C++. All hardware components are interfaced with the ESP32 according to the designed pin configuration. The authentication logic is implemented using a state machine approach. Touch pattern recognition, RFID authentication, and IR detection are coded and tested individually before integrating them into a complete system. EEPROM is used to store the user-defined touch pattern, and servo motor control logic is implemented for locking and unlocking the door.

Deployment

The deployment phase involves installing the smart door lock system in a real-world environment. The hardware components are mounted securely on the enclosure. The ESP32 is powered, and the system is tested under normal operating conditions. Initial configuration such as setting the touch pattern and testing RFID cards is performed. The system is verified for proper operation in both offline mode and optional Wi-Fi mode.

Maintenance

The maintenance phase ensures long-term reliability and proper functioning of the system. It includes regular inspection of hardware components, checking sensor accuracy, and ensuring stable power supply. Software maintenance involves updating

firmware if required, changing the touch pattern through the web interface, and replacing faulty components when necessary. Proper maintenance helps improve system lifespan and security performance.

Components	Cost	Quantity	Cost Estimation (₹)
ESP32 Devkit V1	400	1	400
Touch Sensor (TTP223)	85	1	100
RFID RC522	200	1	200
IR Sensor	100	1	100
5v Power Supply	200	1	200
Breadboard	80	1	80
Jumper wire	100	30	100
Enclosure	200	1	200
Total Cost			₹1,400

Table: Components with appr. Cost

Risk Identification:

- Failure of touch sensor due to improper timing or noise
- Unauthorized access if RFID card is lost or stolen
- Power supply failure causing system shutdown
- Servo motor malfunction due to mechanical wear
- Software bugs affecting authentication flow
- Wi-Fi connectivity failure affecting remote monitoring

Risk Analysis:

- Touch sensor timing errors may lead to false rejection but have low security impact
- RFID card loss poses medium security risk but is controlled by multi-level authentication
- Power failure has high impact but low probability with stable power supply
- Servo motor failure affects physical locking but can be resolved through maintenance
- IR sensor false detection has low impact due to final verification logic
- Software errors may affect system reliability and require debugging
- Wi-Fi failure has low impact as authentication works offline

VII. OVERVIEW OF RISK MITIGATION, MONITORING, MANAGEMENT

Risk mitigation strategies were implemented to reduce system vulnerability. Touch pattern timing limits and reset mechanisms reduce false authentication. Multi-level authentication minimizes the risk of unauthorized access even if one factor is compromised. EEPROM ensures data retention during power loss. Regular monitoring of sensor outputs and servo movement helps detect faults early. Offline authentication guarantees continuous operation, while periodic testing and firmware updates help manage long-term risks.

Software Requirement Specification:

System Implementation Software Required:

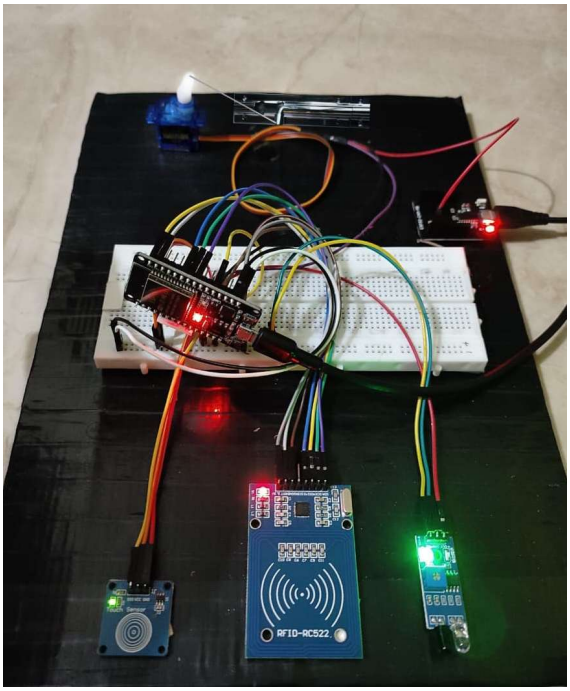
- **Arduino IDE** – Used for writing, compiling, and uploading code to the ESP32 board
- **ESP32 Board Package** – Required to program and manage ESP32 hardware in Arduino IDE
- **ESP32 WiFi Library (WiFi.h)** – Used to connect ESP32 to Wi-Fi and host web-based monitoring/control
- **Web Server Library (WiFiServer.h)** – Used to create HTTP server for LOCK/UNLOCK and pattern update webpage
- **SPI Library (SPI.h)** – Required for SPI communication between ESP32 and RFID module

- **MFRC522 RFID Library (MFRC522.h)** – Used to read RFID UID and authenticate authorized cards
- **Servo Motor Library (ESP32Servo.h)** – Used to control servo motor angle for lock/unlock mechanism
- **EEPROM Library (EEPROM.h)** – Used to store and retrieve touch pattern permanently (non-volatile memory)

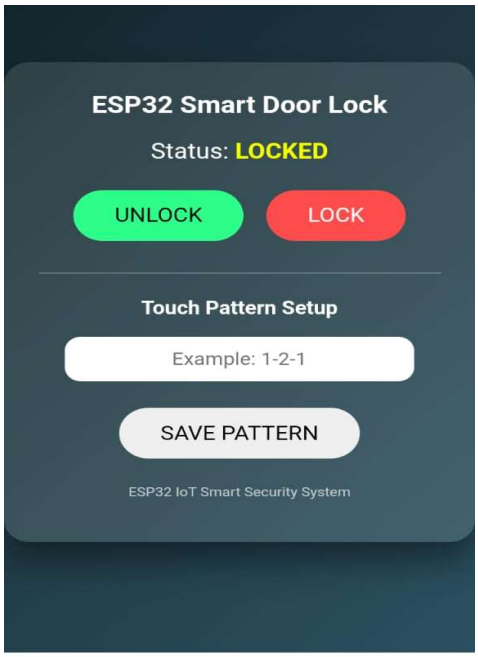
Product Scope:

The scope of the Smart Door Lock System includes designing and implementing a secure access control system using ESP32 with multi-level authentication. The system provides keyless door access using touch pattern and RFID verification, along with IR-based presence detection. It supports offline authentication for enhanced reliability and optional web-based monitoring for user convenience. The project is intended for residential homes, offices, laboratories, and restricted areas. Future enhancements such as biometric authentication, mobile application control, alert systems, and cloud logging are beyond the current scope but can be integrated later.

VIII. RESULT



Smart Door Lock Model



Web Control

IX. CONCLUSION

The Smart Door Lock System with Multi-Level Authentication provides a secure, reliable, and cost-effective access control solution. By combining touch pattern authentication, RFID verification, and IR sensor-based presence detection, the system significantly improves security compared to traditional and single-factor smart locks. Offline authentication ensures uninterrupted operation, making the system suitable for real-world applications such as homes, offices, and restricted areas.

X. REFERENCES

1. A. Kumar and S. Patil, "Design and Implementation of Smart Door Lock System Using ESP32," *International Journal of Engineering Research and Technology (IJERT)*, Vol. 9, Issue 6, 2020.

2. R. Sharma and P. Singh, "RFID Based Door Access Control System," *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, Vol. 8, Issue 4, 2019.

3. S. Verma and N. Kulkarni, "Multi-Factor Authentication Based Smart Door Lock System," *International Journal of Computer Applications (IJCA)*, Vol. 174, No. 22, 2021.

4. M. Joshi and K. Deshmukh, "IoT Based Smart Home Security System Using ESP32," *IEEE International Conference on Smart Technologies*, 2021.

5. P. Kulkarni and A. Deshmukh, "Smart Door Lock System Using Touch Sensor and Microcontroller," *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE)*, Vol. 7, Issue 5, 2019.

6. A. Verma, N. Gupta, "Implementation of Servo Motor Based Electronic Locking System," *International Journal of Engineering and Technical Research (IJETR)*, Vol. 5, Issue 2, 2017.

