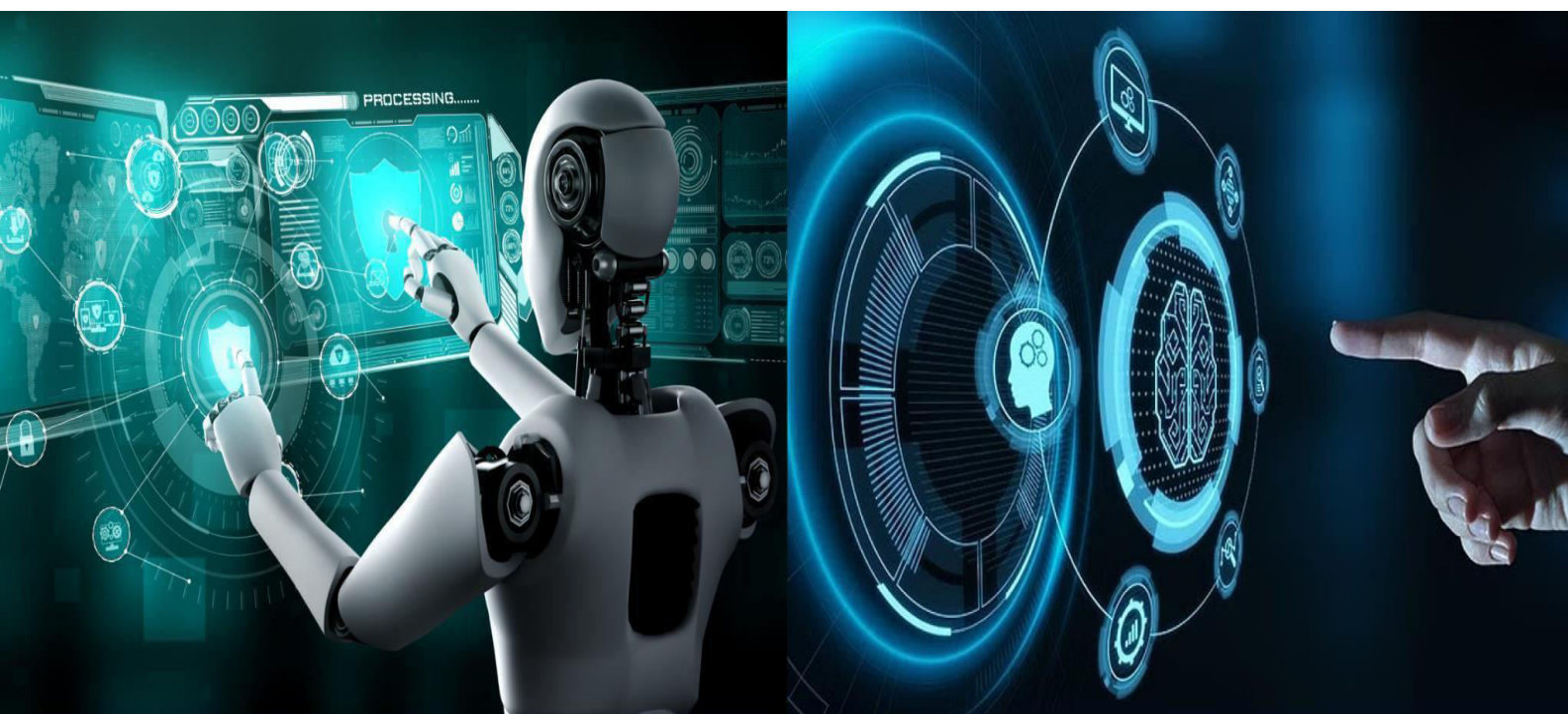


International Journal of Innovative Research in Computer and Communication Engineering

(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

Veda K V¹, Sushmitha M², Priyanka H³, T Akhila⁴, Dr. Malatesh SH⁵

Student, Dept. of Computer Science and Engineering, MS Engineering College, Bengaluru, Karnataka, India^{1,2,3,4}

HOD, Dept. of Computer Science and Engineering, MS Engineering College, Bengaluru, Karnataka, India⁵

ABSTRACT: Secure access control is an essential requirement in residential, academic, and industrial environments. Traditional mechanical locking systems offer limited security and provide no way to track user activity. This project introduces a smart access control system that combines RFID technology with an ESP32-based IoT architecture. Each user is identified using a unique RFID card, while the ESP32 manages authentication, controls the door lock, and records entries to the cloud with accurate time stamps obtained through NTP. A special master RFID card enables administrative tasks such as adding or removing users without connecting the device to a computer. Data is stored in Firebase and can also be visualized on platforms such as Blynk and ThingSpeak. The system was tested for speed, accuracy, and stability, and results show reliable performance with minimal delay. Owing to its simplicity, scalability, and low cost, this system is well-suited for secure access applications in different sectors.

KEYWORDS: Radio Frequency Identification (RFID), access control, smart system, security, authentication, and automation. Depending on specific features, you might also add terms like IoT (Internet of Things), microcontroller (e.g., Arduino, NodeMCU), database, wireless communication, real-time monitoring, electronic lock, or GSM module (for alerts). The choice of keywords should reflect the project's unique components and contributions.

I. INTRODUCTION

This RFID system is built around the powerful ESP32 microcontroller, which functions as the central controller for all operations. Its primary responsibilities include processing input signals from various components, managing Wi-Fi communication for connectivity, and handling interactions with cloud services. This connectivity allows for a modern, networked access control solution. Key hardware components form the physical layer of the system. An RC522 RFID Reader is integrated to perform the core function of reading RFID cards and retrieving their unique identification numbers. Each user within the system is assigned a specific RFID card or tag, which possesses a globally unique serial number for identification purposes. The system's physical access control is managed by a Relay Module, which is responsible for controlling the door's locking and unlocking mechanisms based on the validity of the presented RFID tag. User interaction and feedback are crucial elements of the design. An OLED Display (SSD1306) provides visual status messages to the user, indicating states such as "IN," "OUT," "INVALID CARD," or "ADMIN MODE." To complement the visual feedback, a Buzzer and LEDs are incorporated to provide both audible and visual alerts for valid or invalid access attempts. Furthermore, physical buttons are included in the design, primarily for navigating the admin menu and for manual override functions. The system relies on specific software requirements to function correctly. The development and programming are done using the Arduino IDE, which requires the installation of ESP32 board support. Essential libraries for the system's operation include the Firebase ESP Client Library for cloud communication, the MFRC522 RFID Library for interfacing with the reader, and the Adafruit SSD1306 & GFX Libraries for managing the OLED display. The software also incorporates NTP time configuration to ensure accurate timekeeping, with optional integration possibilities for services like Blynk or ThingSpeak using their respective API keys.

II. METHODOLOGY

1. System Design and Planning

The overall system architecture is designed by identifying hardware components such as ESP32, RFID reader, relay module, OLED display, and software requirements including cloud services and databases.

2. Hardware Integration

The RFID reader, relay, buzzer, LEDs, and OLED display are interfaced with the ESP32 microcontroller. Proper power



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

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

supply and secure wiring are ensured for reliable operation.

3. RFID Authentication Process

When an RFID card or tag is scanned, the reader captures the unique ID and sends it to the ESP32. The controller verifies the ID against authorized entries stored locally or in the cloud.

4. Access Control Decision

If the RFID tag is valid, the relay is activated to unlock the door and a success message is displayed. If invalid, access is denied and an alert is indicated using a buzzer or LED.

5. Data Logging and Cloud Integration

Entry and exit details along with time stamps are uploaded to a cloud database using WiFi. This enables real-time IN/OUT monitoring and secure data storage.

6. Time Synchronization

The system uses NTP servers to synchronize time accurately. This ensures precise logging of access events.

7. User Interface and Administration

Administrators can add, remove, or view authorized users through menu buttons and an OLED interface. This simplifies access management without complex procedures.

8. Monitoring and Visualization

Data is visualized using platforms like ThingSpeak or Blynk, allowing remote monitoring of access logs and system status through dashboards.

9. Testing and Validation

The system is tested for accuracy, response time, security, and reliability under various scenarios to ensure proper functioning.

III. REQUIREMENTS

Functional Requirements

The functional requirements of the RFID Integrated Smart Access Control Equipment focus on providing secure, automated, and efficient access control for authorized users. The system must read RFID cards or tags using an RFID reader and verify the credentials against stored authorized data. Upon successful authentication, the system should grant access by activating electronic locking mechanisms such as relays or solenoid locks, while unauthorized access attempts should be denied. The system must support real-time processing of RFID data through a microcontroller to ensure fast response and reliable operation. It should display access status messages such as "Access Granted" or "Access Denied" using visual indicators like LEDs or displays, and provide audible alerts through a buzzer when required. The system should also maintain access logs for monitoring and security purposes. Wireless communication capabilities should be available for remote monitoring, data storage, and system configuration. Safety and security features such as tamper detection, secure data handling, and system reset mechanisms must be included to ensure dependable operation in real-world environments. Overall, these functional elements enable the RFID-based system to operate as an intelligent, secure, and user-friendly access control solution.

Non-Functional Requirements

The non-functional requirements of the RFID Integrated Smart Access Control Equipment ensure that the system operates reliably, securely, and efficiently under various conditions. The system must provide fast response time during card authentication and ensure high accuracy in identifying authorized users. Power consumption should be optimized to support continuous operation with minimal energy usage. The system must be robust and durable, capable of withstanding environmental factors such as dust, temperature variations, and minor physical disturbances. Reliability is essential, requiring consistent performance with minimal system failures. The user interface should be simple and intuitive, enabling easy operation for both administrators and users. Security is a critical requirement; the system must protect stored data, prevent unauthorized access, and ensure secure communication between components. The design should also allow scalability and future upgrades without major system modifications.

IV. SYSTEM ARCHITECTURE

System architecture refers to the high-level structure of a complex system, encompassing its components, relationships, interactions, and principles governing its design and operation.

1. User Credentials Data:

A collection of authorized user data, including unique RFID tag identifiers, used as the foundational input for



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

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

training/configuring the system and validating access.

2. Configuration and Enrollment:

Raw user credentials are processed, associated with access levels, and stored in a secure database to prepare high-quality structured data for the access control model.

3. Model Configuration/Validation:

The system is configured with rules and logic to grant or deny access based on learned patterns from enrolled data, creating a predictive classification or detection model.

4. System Evaluation:

The configured system is tested on validation scenarios to measure reliability, security, and overall functionality before deployment.

5. Hardware Preparation:

The evaluated system components (e.g., RFID reader, micro-controller, electric lock) are prepared and integrated into a functional, hardware-compatible setup suitable for installation.

6. Deployment:

The integrated system is deployed at entry points, enabling real-time access control on a low-cost embedded processing platform.

7. Input Receiver (RFID Reader):

The RFID reader continuously emits signals to detect and read RFID tags or key fobs when they approach, forwarding the ID number to the inference engine for access validation processing.

8. Network Communication:

The system communicates validation results or alerts across the network, enabling remote monitoring, logging of access events, and interaction with other components.

9. Alert/Lock System:

When an authorized tag is detected, the system triggers the electric lock to open; if unauthorized, it can trigger an alert (e.g., a buzzer) to provide immediate notification.

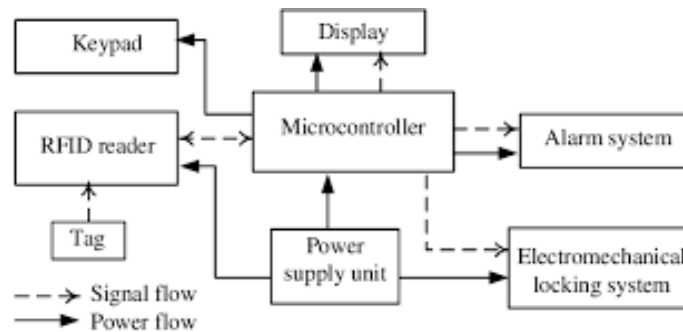


Fig 1: System architecture of RFID integrated smart access control equipment

V. WORK FLOW

1. Start

The system is powered ON.

2. Initialize system

All required variables, pins, and libraries are defined and set up.

3. Wait for RFID card

The system stays idle until an RFID card is presented.

4. Read RFID card

The card data is read by the RFID reader.

5. Check access list

The system checks whether the scanned card is stored in the authorized access list.

6. If card is NOT authorized

- Red LED turns ON
- “Cancel” sound is played



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

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

- Access is denied and the process ends
- 7. If card IS authorized
 - A timer starts
 - The system waits for the user to enter a PIN
- 8. Check timer

The system checks whether the allowed time for PIN entry has expired.
- 9. If timer expires
 - Red LED turns ON
 - “Cancel” sound is played
 - Access is denied and the process ends
- 10.If timer has NOT expired

The system checks the entered PIN.
- 11.Check PIN correctness

The entered PIN is compared with the stored PIN.
- 12.If PIN is incorrect
 - Red LED turns ON
 - “Cancel” sound is played
 - Access is denied
- 13.If PIN is correct
 - Green LED turns ON
 - “Granted” sound is played
 - Access is granted
- 14.End

The system completes the access decision and returns to idle state. This step-by-step flow provides two-level security using RFID authentication followed by PIN verification.

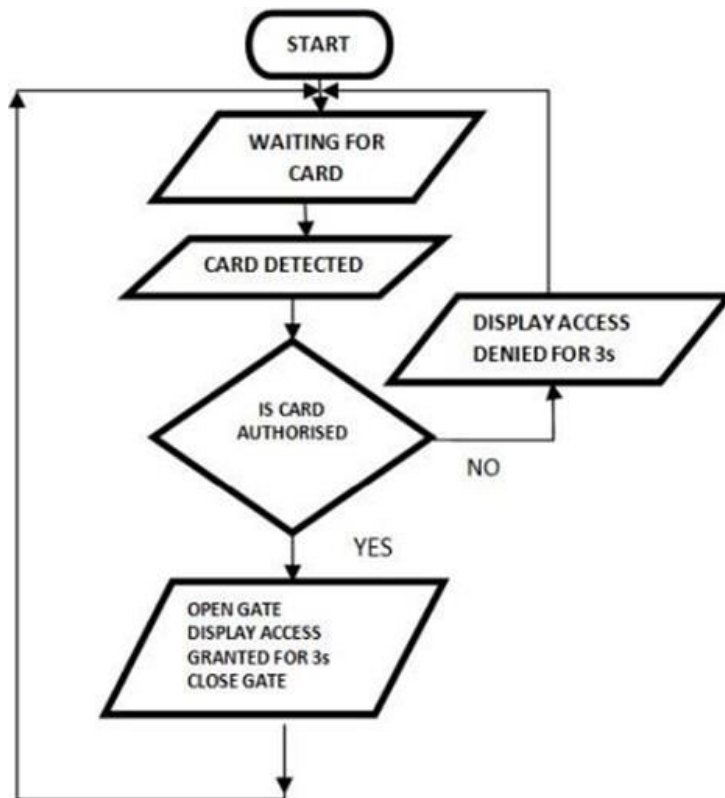


Fig 2:Flowchart of RFID integrated smart control Equipment



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

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

VI. FUTURE SCOPE

The Future Scope of this project includes:

- RFID-based smart access systems will become more automatic and intelligent in the future.
- Artificial Intelligence (AI) and Machine Learning will help detect unusual or suspicious entry behavior instead of only allowing or denying access.
- Integration with IoT and 5G will allow faster communication with cloud systems and other smart devices like lights and HVAC.
- Mobile phones and smartwatches will replace physical RFID cards using technologies like NFC and UWB for contactless entry.
- Blockchain technology will be used to store access records safely and prevent data tampering.
- Advanced encryption methods will improve security against future cyber threats.
- Energy-efficient and nano-RFID tags will reduce maintenance and support eco- friendly systems.
- Future systems will use multiple authentication methods, combining RFID with biometrics like face or iris recognition for better security.

VII. CONCLUSION

The integration of Radio Frequency Identification (RFID) technology into smart access control equipment offers a comprehensive and modern solution to traditional security challenges, fundamentally transforming how access is managed across various sectors, from corporate offices to healthcare facilities. By utilizing radio waves for automatic identification and data capture, RFID systems facilitate a seamless, contactless, and highly efficient user experience that eliminates the drawbacks of mechanical keys, manual logbooks, or line-of-sight barcode scanning.

The primary conclusion is that RFID-based access control provides significantly enhanced security and operational efficiency. Each access attempt, whether granted or denied, is automatically logged, creating a detailed and immutable audit trail for administrators and supporting compliance requirements. The unique identification data on encrypted RFID tags is difficult to duplicate or tamper with, reducing the risks of unauthorized entry compared to traditional methods. Furthermore, the system provides real-time monitoring capabilities, allowing for immediate response to security threats and the ability to instantly revoke or grant access permissions from a centralized location. This level of command and control offers unparalleled peace of mind to security managers.

Operationally, the shift to RFID technology yields substantial benefits and a strong return on investment in the long run. The automation of entry management reduces the need for extensive security personnel at entry points and minimizes human error associated with manual data entry. The quick, proximity-based authentication process speeds up throughput, which is especially beneficial in high-traffic areas, directly boosting overall productivity. Beyond simple access control, these smart systems are highly scalable and can be integrated with other facility management tools, such as time tracking for payroll automation, visitor management systems, or building automation systems (HVAC and lighting), leading to smarter, more autonomous facilities. Looking ahead, the future of RFID integrated access control is bright, marked by deeper integration with the Internet of Things (IoT) and Artificial Intelligence (AI). This convergence is poised to create smarter and more responsive security ecosystems that can predict trends, adapt to changing needs, and offer advanced functionalities like remote monitoring via mobile applications. Ultimately, while the initial setup costs may be higher than conventional systems, the long-term advantages in security, efficiency, scalability, and data-driven insights make RFID integrated smart access control equipment an essential investment for modern organizations striving for a secure and streamlined operational environment.

REFERENCES

- [1] P. Coussy, D. Gajski, M. Meredith and A. Takach, "An Introduction to High-Level Synthesis," Design & Test of Computers, IEEE, vol. 26, pp. 8-17, August 2009.
- [2] E. Ortiz-L6pez, M. Ibarra-Manzano, J. Andrade- Lucio and D. Almanza-Ojeda, "Access control using FPGA and RFID," Acta Universitaria, vol. 22, pp. 31-37, August 2012.
- [3] U. Farooq, M. ul Hasan, M. Amar, A. Hanif and M. Usman Asad, "RFID Based Security and Access Control System" IACSIT International Journal of Engineering and Technology, vol. 6, pp. 309-314, August 2014.
- [4] Y. Mishra, G. Kaur and S. Verma, "Arduino based smart RFID and attendance system with audio



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

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

- acknowledgement," International Journal of Engineering Research & Technology, vol. 4, pp. 363-367, January 2015.
- [5] R. Yadav and S. Nainan, "Design of RFID based student attendance system with notification to parents using GSM," International Journal of Engineering Research & Technology, vol. 3, pp. 1406-1410, February 2014.
- [6] O. C. Santos and J. G. Boticario, "Exploring Arduino for building educational context-aware recommender systems that deliver affective recommendations in social ubiquitous networking environments," Web-Age Information Management, vol. 8579, pp. 272-286, October 2014.
- [7] A. Zaric, C. C. Cruz, A. M. de Matos and M. R. Da Silva, "Pseudo localization principle for RFID based smart blood stock system," Antennas and Propagation, IEEE, vol. 9, pp. 1-4, April 2015.
- [8] H. Martin, E. San Millan, P. Peris-Lopez and J.E. Tapiador, "Efficient ASIC implementation and analysis of two EPC-C1G2 RFID authentication protocols," Sensors Journal, IEEE, vol. 13, pp. 3537-3547, October 2013.
- [9] MIF ARE: http://www.nxp.com/documents/data_sheet/MFR_C522.pdf
- [10] Identification cards: <https://www.iso.org/obp/ui/#iso:std:iso:iec:14443:-:ed2:v1:en>
- [11] Initialization and anticollision: http://read.pudn.com/downloads33/sourcecode/windows/systemll_06178/FDISI4443-3.pdf
- [12] R. Want, "An introduction to RFID technology", Pervasive Computing, IEEE, vol. 5, pp. 25-33, January 2006.
- [13] Microcontroller platform: <https://www.arduino.cc>



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