

Course Code

CSE406

Course Title

Internet of things

Section : 01 Semester : Summer2025

Project report on RFID Door unlock system

Submitted To

Dr. Raihan Ul Islam

Associate Professor

Department of Computer Science and Engineering

Submitted By

Jobayer Faisal Fahim	2022-2-60-130
Akash Saha	2022-2-60-081
Shafiqul Islam Fahim	2022-2-60-085
Mahir Faysal	2022-2-60-044

Date of Submission : September 1, 2025

Contents

1. Introduction	3
2. Objectives	3
3. Background	4
Traditional Door Security Systems:	4
RFID Technology:	4
IoT-Based Security:	4
Related Works:	4
4. System Architecture	5
System Architecture Overview	5
Protocols used in the Project:	6
Network Layer (Connectivity & Data Transmission):	6
Application Layer (ThingsBoard Platform):	7
SPI Protocol :	8
Logical Diagram:	9
Detailed Data Flow:	10
5. Hardware and Software Requirements:	11
Software Tools:	12
6. Implementation:	13
Circuit Design & Pin-diagram:	13
Working Principle:	13
Data Sent to ThingsBoard:	14
ThingsBoard Dashboard Widgets:	14
7. Results and Discussion	14
8. Applications	17
9. Advantages	17
10. Limitations	17
11. Future Scope	17
12. Conclusion	18

1. Introduction

The rapid evolution of the Internet of Things (IoT) has transformed the way devices interact with humans and the environment. One of the most prominent applications of IoT is in the field of smart security systems. Traditional door locking mechanisms are prone to theft, key duplication, and human error (such as forgetting keys). To overcome these challenges, smart access control systems have been designed, combining RFID (Radio Frequency Identification) technology and IoT platforms.

This project presents a Smart Door Security System that uses RFID for access control and integrates with the ThingsBoard IoT platform for real-time monitoring and visualization. The system allows only authorized users to unlock the door, while unauthorized attempts are logged and displayed on a dashboard. It not only increases physical security but also ensures digital traceability by keeping detailed access log.

The integration of RFID with IoT provides a two-layer security mechanism:

1. **Physical Security** – Ensures only people with valid RFID cards can unlock the door.
2. **Digital Monitoring** – Logs every attempt (success or failure) and visualizes it for the user/admin.

Thus, this project demonstrates a low-cost, scalable, and secure access control solution suitable for homes, offices, hostels, and industrial areas.

2. Objectives

The main goals of the project are:

- To develop an RFID-based smart door system using the ESP8266 NodeMCU microcontroller.
- To integrate the system with the ThingsBoard IoT platform using MQTT protocol for communication.
- To visualize system outputs (door status, authentication results, access logs) in real time.
- To implement alerts for unauthorized access attempts to enhance security.
- To demonstrate the feasibility of IoT-enabled smart security solutions for real-world use.

3. Background

Traditional Door Security Systems:

Conventional locks and keys have been used for centuries. While simple and cost-effective, these systems face multiple issues: keys can be lost, stolen, or duplicated. In workplaces, managing multiple keys for employees becomes impractical.

RFID Technology:

RFID is a wireless identification technology that uses radio waves to identify objects. It consists of:

- **RFID Tags (Passive/Active)** – Store a unique ID number.
- **RFID Reader (e.g., RC522)** – Reads the tag and sends the ID to a microcontroller.
- **Backend System** – Validates the ID.

RFID is widely used in inventory management, library systems, transport cards, and security systems.

IoT-Based Security:

IoT platforms such as ThingsBoard, Blynk, and AWS IoT provide remote monitoring of devices. In the context of door security, IoT adds features such as access logs, remote control, and alerts.

Related Works:

- Some researchers have implemented RFID-based doors but without IoT, making them standalone systems with no logs.
- Others integrated IoT but used costly solutions like Raspberry Pi instead of low-cost ESP8266.
- Our project combines the best of both worlds: RFID authentication + ThingsBoard IoT visualization using a low-cost microcontroller.

4. System Architecture

System Architecture Overview

1. Sensors

- **RFID Sensor (e.g., RC522):** Used to read RFID cards or tags to detect authorized access.

2. Actuators

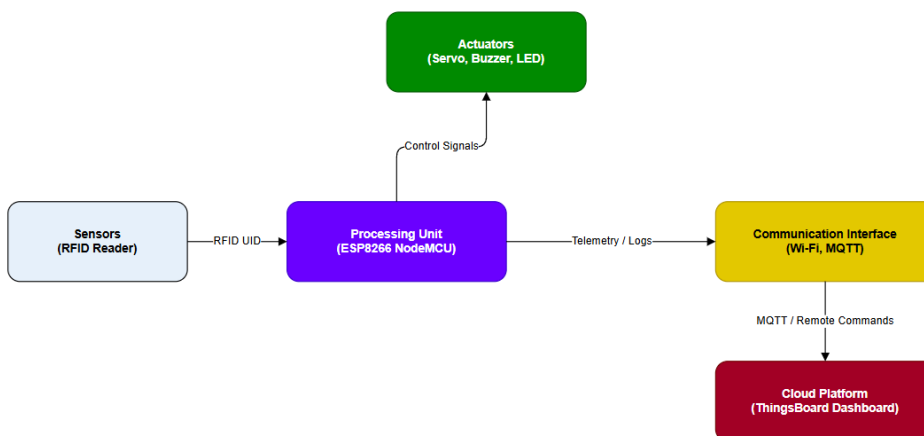
- **LED Indicators:** Used for status indications (e.g., green for access granted, red for access denied).
- **Buzzer:** Used to provide feedback (e.g., sound for success or error).

3. Processing Unit

- **ESP8266 NodeMCU:** A microcontroller with Wi-Fi capabilities, which handles all sensor readings, actuates the motors, and communicates with other systems.
- **Power Supply:** Provides the necessary voltage and current for the entire system, including sensors, actuators, and the microcontroller.

4. Communication Interface

- **Wi-Fi (ESP8266):** Allows communication between the door system and a central server or smartphone app.
- **MQTT Protocol:** Can be used for sending/receiving messages to/from a cloud server or local network to control and monitor the door remotely.



Protocols used in the Project:

Perception Layer (Sensing and Control)

This is the physical layer of the system, where hardware devices interact with the environment:

❖ **RFID Reader (RC522):**

- Detects RFID cards or tags.
- Send the unique tag ID to ESP8266 via SPI communication.

❖ **RFID Tags / Cards:**

- Each card has a unique 12-digit hexadecimal ID.
- Used as the identity of users (authorized or unauthorized).

❖ **ESP8266 NodeMCU (Microcontroller):**

- Acts as the brain of the system.
- Stores a database of authorized RFID IDs.
- Compares scanned card IDs with the database.
- Controls the servo motor/relay to lock or unlock the door.
- Sends authentication results to ThingsBoard via MQTT.

Network Layer (Connectivity & Data Transmission):

The **ESP8266 NodeMCU** has an in-built **Wi-Fi module**, which allows it to connect to the internet and communicate with the ThingsBoard server.

❖ **Wi-Fi Network:** Provides internet connectivity.

❖ **MQTT Protocol:**

- Lightweight publish/subscribe protocol used for IoT.
- NodeMCU publishes messages like *Card ID*, *Authentication Status*, *Door State* to ThingsBoard.
- ThingsBoard subscribes to these topics to visualize data.
- Optional: ThingsBoard can also send commands (like remote unlock) back to NodeMCU.

Data Sent to ThingsBoard (Telemetry):

- **card_id:** The scanned card's unique ID.
- **user:** Assigned username (if mapped).
- **auth_status:** Authorized / Unauthorized.
- **door_status:** Locked / Unlocked.
- **timestamp:** Time of access attempt

Application Layer (ThingsBoard Platform):

ThingsBoard acts as the **IoT Application Layer** that receives, stores, processes, and visualizes data.

❖ Dashboard Widgets:

- **Status Indicator:** Shows if the door is locked/unlocked.
- **Log Table:** Displays timestamp, card ID, user, and result.
- **LED Widget:** Green → Access , Red → Unauthorized.
- **Notification Widget:** Alerts when unauthorized access is detected.
- **Charts:** Displays daily/weekly access attempts.
- **Remote Button (Optional):** Admin can unlock/lock the door remotely.

❖ Data Processing Rules:

- ThingsBoard can trigger alarms if multiple failed attempts occur in a short time.
- Alerts can be extended to email/SMS notifications.

SPI Protocol :

The SPI protocol is used for communication between the ESP8266 NodeMCU (acting as the master device) and the RC522 RFID Reader (acting as the slave device). Here's how it works in detail:

1. SPI Communication Setup:

- **Master Device:** ESP8266 NodeMCU
- **Slave Device:** RC522 RFID Reader
- **SPI Pins:**
 - **MISO (Master In Slave Out):** Used to receive data from the slave device (RC522).
 - **MOSI (Master Out Slave In):** Used to send data from the master device (NodeMCU) to the slave device.
 - **SCK (Serial Clock):** Used to synchronize the data transfer between the master and slave.
 - **SDA/SS (Slave Select/Chip Select):** Used to select the slave device, which in this case is the RC522.

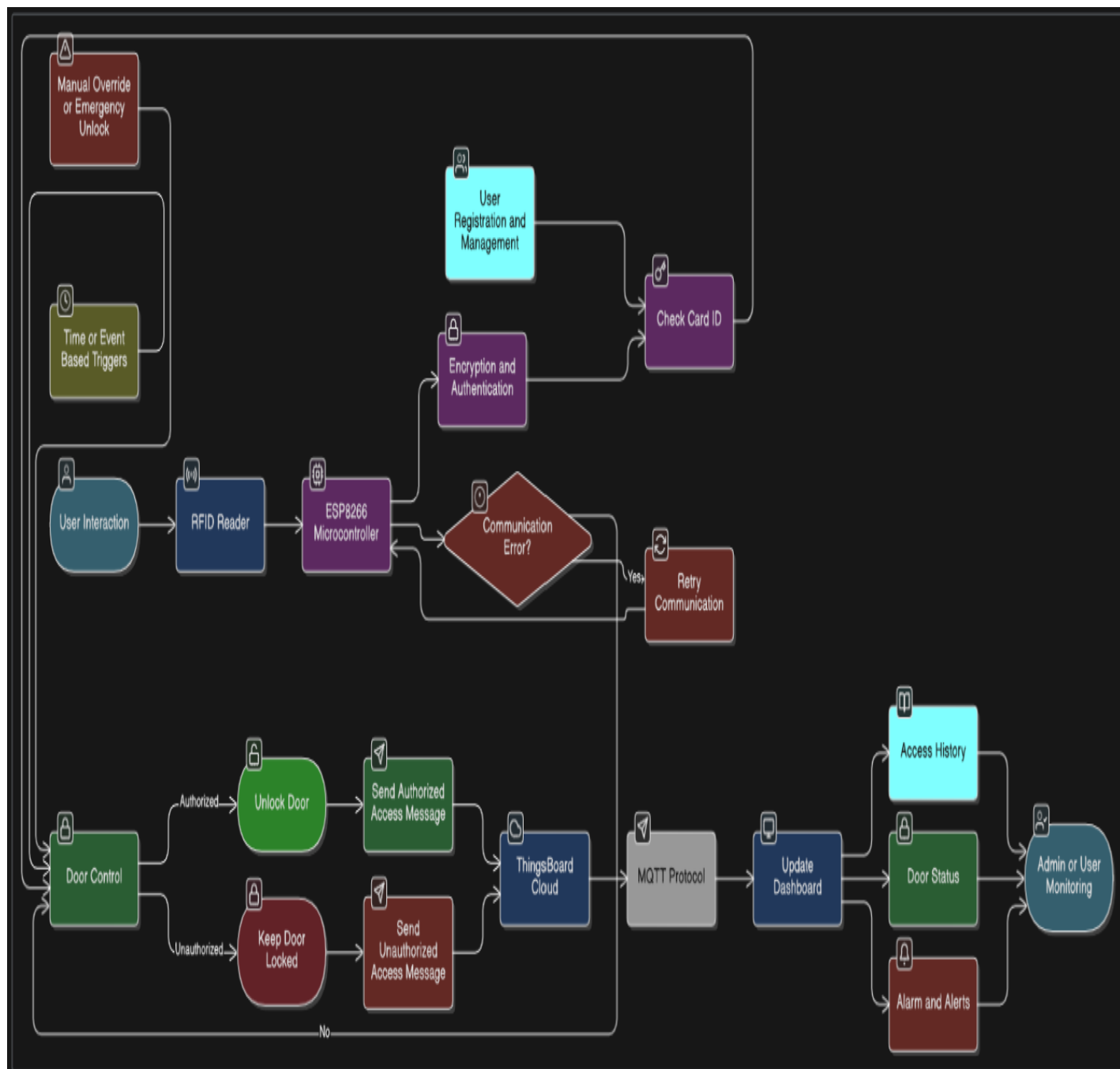
2. Data Flow in SPI Communication:

- The ESP8266 NodeMCU (Master) initiates communication by pulling the CS (Chip Select) pin low, signaling to the RC522 (Slave) that it's ready to communicate.
- The NodeMCU sends commands to RC522 via the MOSI line, instructing it to perform operations such as reading the RFID tag data.
- The RC522 sends data (such as the RFID tag ID) back to the NodeMCU through the MISO line.
- The NodeMCU uses the SCK line to synchronize the data transmission.






Logical Diagram:



Detailed Data Flow:



5. Hardware and Software Requirements:

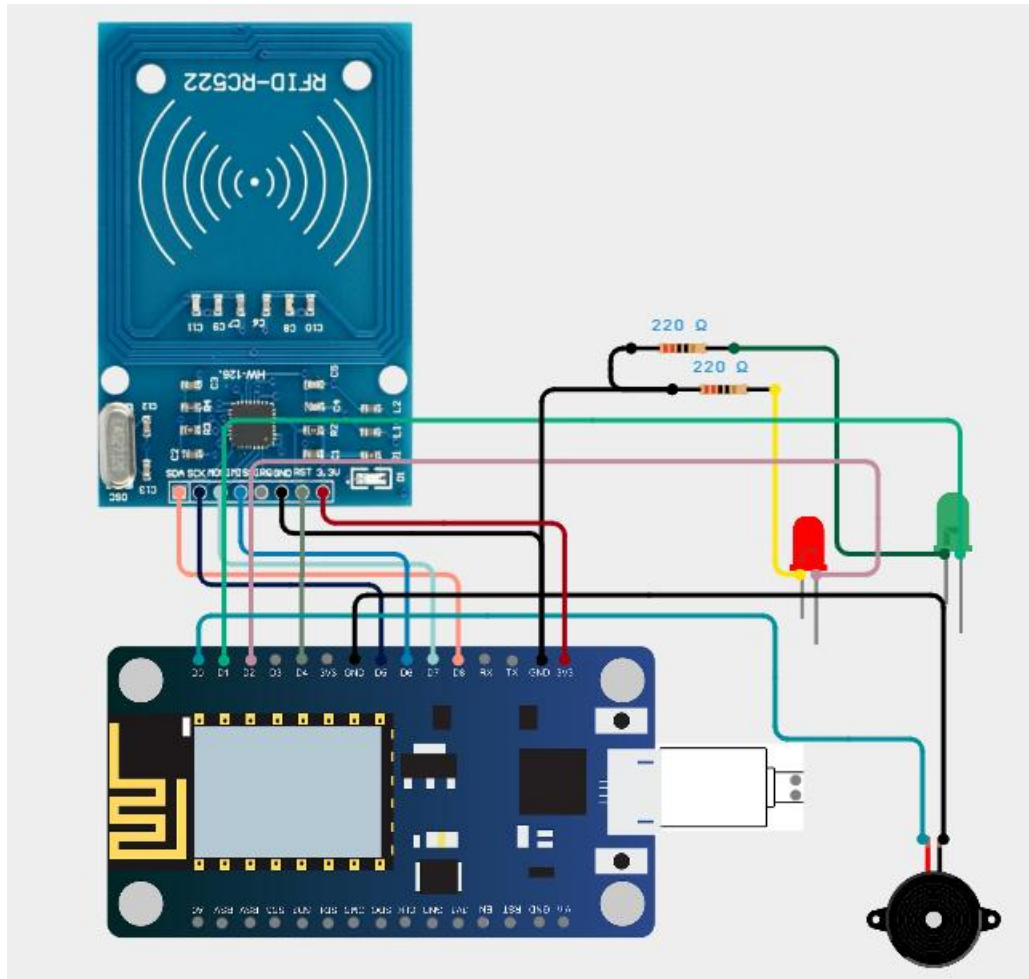
Hardware Name	Visual Presentation
ESP8266 NodeMCU – Wi-Fi-enabled microcontroller for IoT communication.	
RFID Reader (RC522) – Reads RFID tag IDs. RFID Tags/Cards – Unique IDs assigned to users.	
Jumper Wire	
LED	
Buzzer	

--	--

Software Tools:

1. **Arduino IDE** – For programming the NodeMCU.
2. **ThingsBoard IoT Platform** – For visualization.
3. **MQTT Protocol** – Lightweight messaging protocol used to send data.
4. **Libraries Used:**
 - SPI.h (for RC522 communication)
 - MFRC522.h (RFID functions)
 - ESP8266WiFi.h (Wi-Fi connection)
 - PubSubClient.h (MQTT client)

Circuit Design & Pin-diagram:



Working Principle:

1. RFID reader scans the card.
2. The card ID is compared with stored authorized IDs in NodeMCU.
3. If Authorized : Door unlocks, and a success message is sent to ThingsBoard.
4. If Unauthorized : Door stays locked, and an alert is sent to ThingsBoard.

Data Sent to ThingsBoard:

- Door Status: Locked/Unlocked
- Card/User ID
- Card Username
- Authentication Result: Authorized/Unauthorized
- Timestamp

ThingsBoard Dashboard Widgets:

1. **Status Indicator** → Lock/Unlock status.
2. **Text Display** → Last access user.
3. **Table Widget** → Access logs (Time, User ID, Status).
4. **LED/Color Indicator** → Green (Authorized), Red (Unauthorized).
5. **Chart Widget** → Number of accesses per day/week.

7. Results and Discussion

- The RFID reader successfully detected cards with an average response time of <1 second.
- Authorized users were able to unlock the door reliably.
- Unauthorized cards triggered alerts and were logged onto ThingsBoard.
- The ThingsBoard dashboard provided clear visualization of real-time access attempts.

Telemetry:

RFID DOOR

Device details

?

×

<

Details

Attributes

Latest telemetry

Calculated fields

Alarms

Events

>

Telemetry

+ 🔍

<input type="checkbox"/>	Last update time	Key ↑	Value	
<input type="checkbox"/>	2025-08-29 21:29:21	door_status	open	
<input type="checkbox"/>	2025-08-29 21:29:21	outcome	granted	
<input type="checkbox"/>	2025-08-29 21:29:21	timestamp	216183	
<input type="checkbox"/>	2025-08-29 21:29:21	uid	D9:4A:C8:01	
<input type="checkbox"/>	2025-08-29 21:29:21	username	DINA	

Items per page: 10

1 - 5 of 5

|< < > >|

DOOR STATUS:

Door Status

Last update 6h ago

closed

TIMESERIES TABLE:

Timeseries table

🔍 📊 🗨

🕒 Realtime - Current week (Sun - Sat)

Timestamp ↓	outcome	uid	username
2025-08-31 19:11:50	denied	A5:1E:28:03	

1 - 1 of 1

|< < > >|

Real time Alert system:

⚠ Alarms

🔍 ⚙ 📊 🗨

🕒 Realtime - Current week (Sun - Sat)

<input type="checkbox"/>	Created time ↓	Originator	Type	Severity	Status	Assignee	
<input type="checkbox"/>	2025-08-30 00:15:23	RFID DOOR	Someone tries to break your Door. Someone	Critical	Active Unacknowledged	👤 Unassigned	💬 ... ✓ ✕

Items per page: 10

1 - 7 of 7

|< < > >|

Powered by Thi

8. Applications

- **Smart Homes** – Controlled access for family members.
- **Offices** – Employee attendance and access control.
- **Hostels/Dormitories** – Monitor students' entry and exit.
- **Industrial Areas** – Restrict entry to sensitive zones.
- **Libraries/Research Labs** – Access for registered users only.

9. Advantages

- Contactless and fast authentication.
- Low-cost hardware implementation.
- Real-time IoT visualization improves transparency.
- Scalable to multiple doors/users.
- Remote control and monitoring are possible.

10. Limitations

- RFID cards can be lost or stolen, leading to misuse.
- Requires stable internet connection for IoT features.
- Limited processing capability of NodeMCU restricts complex security functions.

11. Future Scope

- **Biometric Integration:** Fingerprint/Face recognition with RFID for dual authentication.
- **Mobile Notifications:** SMS/Email alerts for each access attempt.
- **Cloud Storage:** Store long-term access logs for analysis.
- **AI Analytics:** Predict unusual access patterns using machine learning.
- **Integration with Smart Home Systems:** Connect with Alexa/Google Home for voice commands.

12. Conclusion

This project demonstrates a low-cost, reliable, and scalable smart door system using RFID and IoT. The integration with ThingsBoard ensures real-time monitoring, access logging, and enhanced security.

The results confirm that IoT-enabled security systems can significantly improve safety, usability, and transparency in residential, commercial, and industrial applications. With future enhancements like biometrics and AI integration, the system can evolve into a fully automated smart security solution.