A logo of a university

Description automatically generated

A logo for a company

Description automatically generated

A Mini-project Report on

### **NexGuard: RFID Lock System with Intrusion Alert**

Submitted to The Charutar Vidya Mandal University for the partial fulfillment for the award of Minor Degree /Honors Program in Internet of Things

under

BACHELOR OF ENGINEERING

By

|  |  |
| --- | --- |
| Name of the Student | Enrollment No. |
| Modi Hetvi Dipex | 12102040601028 |
| Patel Shiven Rajendrabhai | 12102040601064 |

Under the Supervision of

Dr . Dhaval Tailor Assistant Professor

A logo for a company

Description automatically generatedComputer Engineering

AD Patel Institute of Technology

A Constituent college of The CVM University

Vallabh Vidyanagar -388120

April 2024

##### **CONTENTS**

Title

Certificate Page

Compliance Certificate Page

Acknowledgement

Contents *i*

List of Figures *ii*

Abstract *iii*

Chapter 1 Introduction 10

* 1. [Problem Statement](#_TOC_250004)
  2. [Project Summary and Introduction](#_TOC_250003)
  3. [Aim and Objective of the Project](#_TOC_250002)

Chapter 2 System Analysis 13

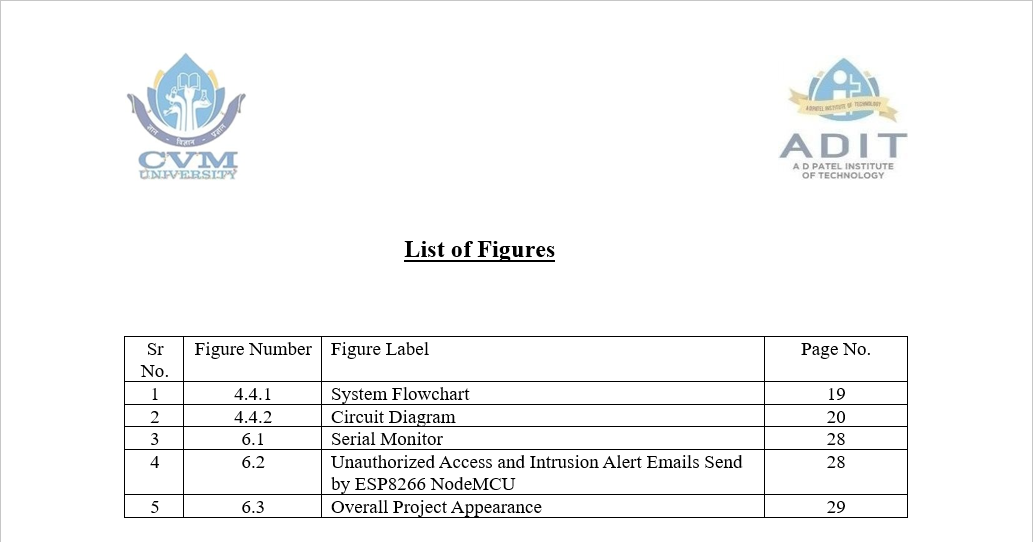
* 1. [Motivation](#_TOC_250001)
  2. [Brief Literature Survey](#_TOC_250000)

Chapter 3 Methodology 15

* 1. Description of Methodology

3.2 Explanation of Software and Hardware Components

|  |  |
| --- | --- |
| Chapter 4 System Design  4.1 System Requirements  4.2 System Architecture  4.3 Components Functionality  4.4 System Flowchart and Circuit Diagram | 18 |
| Chapter 5 Implementation  5.1 Hardware Setup  5.2 Software Setup  Chapter 6 Result and Evaluation | 22  29 |
| Chapter 7 Summary and Conclusion | 31 |
| Chapter 8 Future Work | 32 |
| Chapter 9 Bibliography/References | 33 |
|  |  |



## Acknowledgement

I would like to express our sincere gratitude to the dedicated individuals and teams who played instrumental roles in the development and implementation of our spam email classification system.

First and foremost, I would like to thank our project guide, Dr. Dhaval Tailor, for providing us with valuable guidance and support throughout the project. He was always available to clarify our doubts and provide us with insightful feedback that helped us to improve the work.

I would like to extend my appreciation to our college faculty members who provided us with the necessary resources and facilities to complete this project. Their encouragement and support were instrumental in helping us stay motivated and focused.

I am also grateful to my teammates for their tireless efforts and dedication in completing this project. Without their contributions, this project would not have been possible.

Once again, I extend my heartfelt thanks to everyone who has helped us in completing this project successfully.

### COMPLIANCE CERTIFICATE

This is to certify that the research work embodied in this Mini- project report entitled “**NexGuard : RFID Lock System with Intrusion Alert**” is carried out by the following students at **A D Patel Institute of Technology** for partial fulfillment of the requirements for the award of Minor Degree/Honors Program in **Internet of Things** under Bachelor of Engineering to The Charutar Vidya Mandal University. This research is the authentic record of work carried out by us and is not submitted in past to any institute

or university.

|  |  |  |
| --- | --- | --- |
| Name of the Student | Enrollment No. | Signature |
| Modi Hetvi Dipex | 12102040601028 |  |
| Patel Shiven Rajendrabhai | 12102040601064 |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  | Dr. Dhaval Tailor |
|  |  | Assistant Professor  Electrical Engineering |

Date: Place:

### CERTIFICATE

This is to certify that the research work embodied in this Mini-project report entitled “**NexGuard : RFID Lock System with Intrusion Alert**” is carried out by the following students at **A D Patel Institute of Technology** for partial fulfillment of the requirements for the award of Minor Degree/Honours Program in **Internet of Things** under Bachelor of Engineering in to The Charutar Vidya Mandal University. This research work has been carried out under my supervision and it is up to my satisfaction.

|  |  |
| --- | --- |
| Name of the Student | Enrollment No. |
| Modi Hetvi Dipex | 12102040601028 |
| Patel Shiven Rajendrabhai | 12102040601064 |

Dr. Dhaval Tailor Dr. Bhagirath Prajapati

Assistant Professor Head of Department

Electrical Engineering A D Patel Institute of Technology

Date: Place:

### MINI-PROJECT REPORT APPROVAL CERTIFICATE

This is to certify that the research work embodied in this project report entitled “**NexGuard : RFID Lock System with Intrusion Alert**” is carried out by the following students at **A D Patel Institute of Technology** is approved for the award of Minor Degree/Honours Program in **Internet of Things** under Bachelor of Engineering, The Charutar Vidya Mandal University.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Signature of External Examiner] Khushali Shah

s

Date: Place:

## Abstract

The NexGuard RFID Lock System with RFID Access and Email Notification is an advanced security solution designed to safeguard door access and protect valuable assets such as jewelry, cash money, documents, and other similar items. leveraging modern technologies. Central to its operation is the integration of RFID (Radio-Frequency Identification) technology, reed switch sensors, and email notification capabilities. The system comprises essential components including an ESP8266 microcontroller module, an RFID reader, a reed switch sensor, a solenoid lock, and a buzzer. With this system, authorized users are granted access to the secured area by simply tapping an RFID card embedded with a unique tag. Upon detection of the authorized tag, the system activates the solenoid lock, granting access to the premises. In the event of an unauthorized attempt, where an invalid RFID tag is detected, the system promptly triggers a buzzer alarm. Simultaneously, an email notification is sent to a predefined email address, providing real-time updates on the unauthorized access attempt. Furthermore, the system incorporates a reed switch sensor to monitor the state of the door. If the door is opened without a valid RFID access, signifying a potential intrusion, the system promptly triggers a buzzer alarm to alert nearby individuals and sends an email notification to notify the user of the security breach. By combining access control mechanisms with intrusion detection capabilities and remote notifications via email, the NexGuard RFID Lock System offers comprehensive security measures, ensuring the safety and protection of the premises. Its seamless integration of modern technologies empowers users with real-time insights into access events, enhancing overall security and providing peace of mind.

## **Introduction**

#### Problem Statement

In today's complex security landscape, the protection of valuable assets such as jewelry, cash money, and sensitive documents is of paramount importance. However, traditional security measures often fall short in effectively safeguarding these assets against theft and unauthorized access. Common issues include the inability to monitor access events in real-time, the lack of comprehensive intrusion detection mechanisms, and limited means of notifying stakeholders about security breaches promptly.

Furthermore, as the sophistication of security threats continues to evolve at an unprecedented rate, there is a growing demand for advanced security solutions that leverage modern technologies to address these challenges comprehensively. Current systems often lack integration with cutting-edge technologies, leaving vulnerabilities that can be exploited by intruders.

Therefore, there is an urgent and critical need for an advanced security system that not only provides robust access control mechanisms but also incorporates sophisticated intrusion detection capabilities and real-time notifications to ensure the safety and protection of premises and valuable assets. Such a system should seamlessly integrate RFID (Radio-Frequency Identification) technology for convenient and secure access, utilize reed switch sensors to continuously monitor the state of doors, and leverage email notification capabilities to alert stakeholders about unauthorized access attempts promptly.

By addressing these multifaceted challenges and providing a holistic approach to security, the ideal solution will empower users with actionable real-time insights into access events, enhance overall security measures, and provide unparalleled peace of mind in knowing that valuable assets are adequately protected against potential threats.

This revised problem statement adds more detail and specificity to highlight the urgency and complexity of the security challenges faced, emphasizing the need for a comprehensive solution like the NexGuard RFID Lock System.

#### Project Summary and Introduction

The NexGuard RFID Lock System is an advanced security solution designed to protect valuable assets stored within a locker using modern technologies. Central to its operation is the integration of RFID technology, reed switch sensors, and email notification capabilities. The system comprises essential components including an ESP8266 microcontroller module, an RFID reader, a reed switch sensor, a solenoid lock, and a buzzer.

Authorized users gain access to the secured locker by tapping an RFID card embedded with a unique tag. Upon detection of the authorized tag, the system activates the solenoid lock, granting access. In the event of an unauthorized attempt, where an invalid RFID tag is detected or the door is opened without valid access, the system triggers a buzzer alarm and sends an email notification, providing real-time updates on the security breach.

By combining access control mechanisms with intrusion detection capabilities and remote notifications via email, the NexGuard RFID Lock System offers comprehensive security measures, ensuring the safety and protection of assets stored within the locker.

###### Project Introduction:

In today's dynamic security landscape, safeguarding valuable assets stored within lockers presents a significant challenge. Traditional security systems often lack the sophistication needed to provide robust protection and real-time alerts. To address these shortcomings and meet the evolving needs of security, the NexGuard RFID Lock System offers a cutting-edge solution that leverages modern technologies to enhance security measures.

This project aims to develop an advanced security system that integrates RFID technology, reed switch sensors, and email notification capabilities to safeguard valuable assets stored within a locker. The system's core components, including the ESP8266 microcontroller module, RFID reader, reed switch sensor, solenoid lock, and buzzer, work seamlessly together to grant authorized access and detect unauthorized attempts.

By providing real-time alerts via email and triggering audible alarms in response to security breaches, the NexGuard RFID Lock System offers comprehensive security measures, ensuring the safety and protection of assets stored within the locker. Through this project, we seek to empower users with actionable insights into access events, enhance overall security measures, and provide peace of mind in knowing that valuable assets are adequately protected against potential threats.

#### Aim and Objective of the Project

###### Aim:

###### The aim of this project is to design and implement the NexGuard RFID Lock System, an advanced security solution tailored to safeguard valuable assets stored within lockers. Leveraging modern technologies including RFID (Radio-Frequency Identification) technology, reed switch sensors, and email notification capabilities, the system aims to provide comprehensive protection against unauthorized access attempts and theft.

###### Objectives:

1. Designing and prototyping the hardware components required for the NexGuard RFID Lock System, including the ESP8266 microcontroller module, RFID reader, reed switch sensor, solenoid lock, and buzzer.
2. Developing the software algorithms necessary to control access to the locker based on RFID authentication and detect unauthorized access attempts through reed switch sensor monitoring.
3. Integrating email notification capabilities to provide real-time alerts to predefined recipients in the event of unauthorized access attempts or security breaches.
4. Testing and refining the system to ensure reliability, effectiveness, and ease of use in real-world applications.
5. Documenting the design, implementation, and testing process to facilitate replication and further development of the NexGuard RFID Lock System.

# System Analysis

#### Motivation

The motivation behind developing the NexGuard RFID Lock System stems from the increasing need for advanced security solutions that effectively safeguard valuable assets stored within lockers. With the proliferation of theft and unauthorized access incidents in various environments such as homes, offices, and commercial establishments, there is a growing concern for the security of these assets. Traditional lock-and-key mechanisms often prove inadequate in preventing unauthorized access attempts and providing timely alerts in the event of security breaches. However, rapid advancements in technology, particularly in areas such as RFID (Radio-Frequency Identification) technology and microcontroller systems, present opportunities to develop more sophisticated and effective security solutions. By leveraging these technologies, it is possible to create a system that offers enhanced security features, real-time monitoring, and remote notifications. The NexGuard RFID Lock System aims to provide a convenient and efficient method for controlling access to lockers containing valuable assets. Utilizing RFID technology allows authorized users to gain access with a simple tap of an RFID card, eliminating the need for physical keys or complicated authentication procedures. This not only enhances user convenience but also reduces the risk of lost or stolen keys. Furthermore, by implementing a comprehensive security solution like the NexGuard RFID Lock System, users can enjoy greater peace of mind knowing that their valuable assets are adequately protected. Real-time alerts and notifications enable prompt action to be taken in the event of unauthorized access attempts or security breaches, mitigating potential risks and minimizing losses. The modular design of the NexGuard RFID Lock System allows for flexibility in configuration and scalability to accommodate varying security needs and locker sizes, whether deployed in residential, commercial, or institutional settings. In summary, the motivation for developing the NexGuard RFID Lock System lies in addressing the shortcomings of existing security solutions, harnessing technological advancements to enhance security measures, and providing users with a reliable and convenient means of safeguarding their valuable assets.

#### Brief Literature Survey

A literature survey for the NexGuard RFID Lock System project would involve reviewing existing research, patents, and commercial products related to RFID-based security systems, access control mechanisms, and intrusion detection technologies. Here's a brief overview of what such a literature survey might entail:

2.2.1 RFID-Based Security Systems:

Explore academic literature and industry publications focusing on the integration of RFID technology in security systems. Look for studies on RFID authentication methods, tag encryption techniques, and real-world implementations of RFID-based access control systems. Understanding the principles and advancements in RFID technology will provide valuable insights for designing the authentication mechanism of the NexGuard system.

2.2.2 Reed Switch Sensors in Security Applications:

Research studies and technical papers that discuss the use of reed switch sensors in security applications. Investigate the effectiveness of reed switches in detecting door state changes and potential intrusion events. Understanding the capabilities and limitations of reed switch sensors will inform the design of the intrusion detection feature in the NexGuard system.

2.2.3 Email Notification Systems in Security:

Review literature on email notification systems used in security applications. Look for research papers and commercial solutions that discuss the implementation of real-time alerting mechanisms via email. Analyze the reliability, latency, and scalability of email notifications for security events. This will help in designing the notification feature of the NexGuard system to provide timely alerts to stakeholders.

2.2.4 Microcontroller-Based Security Systems:

Explore literature on microcontroller-based security systems, focusing on projects or research papers that utilize microcontrollers for access control and intrusion detection. Investigate the choice of microcontroller platforms, software development methodologies, and integration of sensors and actuators. This will provide insights into the design and implementation of the control logic for the NexGuard system using the ESP8266 microcontroller module.

# Methodology

#### Description of the Methodology:

The methodology for developing the NexGuard RFID Lock System involves a systematic approach to address various aspects of system design, implementation, and validation. Initially, thorough requirements analysis is conducted to define both functional and non-functional requirements based on user needs, security considerations, and regulatory requirements. Stakeholder input is gathered through interviews and surveys to ensure alignment with desired features, usability expectations, and performance criteria. This information is documented in a detailed specification document, serving as a blueprint for system development. Subsequently, the system architecture is designed, encompassing hardware components such as the ESP8266 microcontroller module, RFID reader, reed switch sensor, solenoid lock, and buzzer, along with software components including authentication algorithms, intrusion detection logic, and email notification systems. Interfaces and communication protocols between system components are defined, and detailed diagrams illustrate data and control flow within the system.

Moving forward, a prototype of the NexGuard system is developed using off-the-shelf components and development tools. This involves assembling electronic circuits for hardware components and implementing firmware for the microcontroller, authentication logic, intrusion detection algorithms, and email notification functionality for software components. The prototype undergoes iterative refinement based on feedback from initial testing. The implementation phase focuses on optimizing codebase for performance, reliability, and maintainability, while additional features or enhancements are integrated based on stakeholder requirements or emerging technologies. Comprehensive testing is conducted to verify the functionality, performance, and security of the NexGuard system. This includes unit testing of individual components, integration testing to ensure seamless operation of all system elements, and system testing to assess end-to-end functionality and compliance with requirements. Finally, real-world validation of the NexGuard RFID Lock System is performed to evaluate its effectiveness and usability. Feedback from end-users and stakeholders is solicited to identify any issues or areas for improvement, which are addressed through iterative refinement of the system design and implementation. Throughout the methodology, adherence to best practices in software engineering, hardware development, and compliance with relevant standards and regulations are maintained to ensure the quality and reliability of the NexGuard RFID Lock System.

#### Explanation of Hardware and Software Components:

**Hardware Components:**

* ESP8266 Microcontroller Module: The central processing unit responsible for managing communication between hardware components, processing authentication requests, and controlling system operation.
* RFID Reader: Reads unique identification codes from RFID cards or tags to authenticate users and grant access to the secured area.
* Reed Switch Sensor: Monitors the state of the door by detecting changes in the magnetic field when the door is opened or closed, triggering alerts for unauthorized access attempts.
* Solenoid Lock: Controls access to the secured area by releasing the locking mechanism when activated by the microcontroller upon successful authentication.
* Buzzer: Serves as an audible alarm to alert nearby individuals to unauthorized access attempts or security breaches.
* Power Supply: The power supply converts AC power from mains electricity into DC power to ensure the proper operation of system components.
* Relay Module: The relay module serves as an electromechanical switch, enabling the microcontroller to control high-power devices like solenoid locks by providing isolation between low-voltage control signals and high-voltage loads.

###### Software Components:

* Firmware for ESP8266 Microcontroller: Controls communication between hardware components, manages authentication requests, monitors sensor input, and controls lock and buzzer operation.
* RFID Authentication Logic: Verifies the validity of RFID tags and grants access to the secured area upon successful authentication.
* Intrusion Detection Algorithm: Monitors changes in the door state detected by the reed switch sensor and triggers alerts and alarms for unauthorized access attempts or security breaches.
* Email Notification System: Sends real-time email notifications to predefined recipients in the event of unauthorized access or security breaches, ensuring stakeholders are promptly informed and enabling swift action.

# System Design

### **System Requirements:**

1. Hardware:

RFID module, NodeMCU, Buzzer, Relay module, Solenoid Door Lock, Battery.

1. Software:

RFID Authentication Algorithm, NodeMCU Firmware, Intrusion Detection Software, Messaging System Software.

1. Communication:

RFID Communication Protocol, Wi-Fi Connectivity.

1. User Interface:

Minimal LED or display indicators, Optional Mobile Application.

1. Scalability and Customization:

Scalable architecture, Customization options for access levels.

1. Power Management:

Low Power Consumption, Optional Power Supply switching.

1. Compatibility:

Compatibility with existing RFID standards.

1. Documentation:

Comprehensive user manuals, installation guides, and system architecture documentation.

1. Regulatory Compliance:

Adherence to data protection and safety standards for a secure and compliant deployment.

* 1. **System Architecture:**

The system architecture of the NexGuard RFID Lock System combines hardware and software components to ensure comprehensive security measures. Hardware components include the ESP8266 Microcontroller Module, which acts as the system's central processing unit, managing communication between components. The RFID Reader reads RFID tags for user authentication, while the Reed Switch Sensor monitors the door's state to detect unauthorized access attempts.

The Solenoid Lock controls access to the secured area, and the Buzzer provides audible alerts in response to security breaches.

Software components play a crucial role in system operation. The firmware for the ESP8266 Microcontroller governs overall system functionality, including authentication, intrusion detection, and hardware control. The RFID Authentication Logic verifies RFID tag validity and grants access upon successful authentication. Meanwhile, the Intrusion Detection Algorithm monitors changes in the door state, triggering alerts for unauthorized access attempts. Additionally, the Email Notification System sends real-time email notifications to predefined recipients in the event of security breaches, ensuring stakeholders are promptly informed.

In operation, when an RFID tag is presented, the RFID reader sends its data to the ESP8266 Microcontroller for authentication. The microcontroller verifies tag validity using the authentication logic and activates the Solenoid Lock to grant access upon successful authentication. Simultaneously, the intrusion detection algorithm monitors the Reed Switch Sensor for changes in the door state. If unauthorized access is detected, the microcontroller triggers the Buzzer for audible alerts and activates the Email Notification System to send real-time alerts to predefined recipients.

Communication within the system is managed by the microcontroller, which coordinates interactions between hardware components. It communicates with the RFID reader, Reed Switch Sensor, Solenoid Lock, and Buzzer to ensure seamless operation. Additionally, the Email Notification System communicates with an email server to deliver real-time alerts to stakeholders. While not explicitly mentioned in the architecture, a user interface may be included for system configuration and monitoring, allowing users to manage RFID tags, view access logs, and configure email notification settings.

* 1. **Components Functionality:**

The NexGuard RFID Lock System incorporates essential components for seamless functionality. The RFID Module utilizes RFID technology to initiate secure, contactless user entry. Acting as the system's brain, the NodeMCU executes the RFID Authentication Algorithm, governs access control decisions, and orchestrates component communication. The Buzzer enhances situational awareness by generating audible alerts in response to security events. The Relay Module, an electronic switch, controls the Solenoid Door Lock, ensuring secure and regulated physical access. Powered by a Battery, the system maintains continuous functionality, promoting autonomy. Intrusion Detection Software monitors RFID events, triggering alerts for unauthorized access attempts. The Messaging System Software facilitates internal communication and emergency notifications. Optionally, a User Interface provides visual indicators of system status. Wi-Fi Connectivity supports remote management. Collectively, these components form a comprehensive and user-friendly access control system with enhanced security features.

**4.4 System Flowchart and Circuit Diagram:**

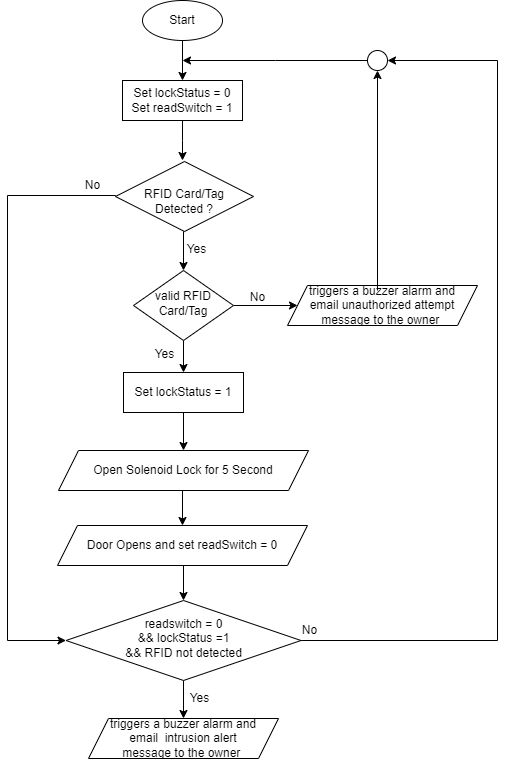
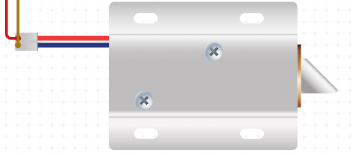
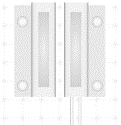
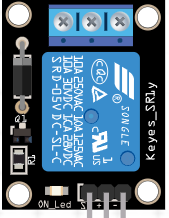
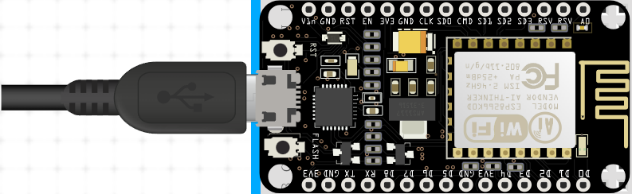


Figure 4.4.1: System Flowchart

**

**



**

**

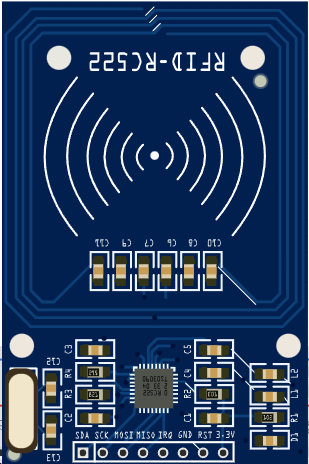
**

Figure 4.4.2: Circuit Diagram

# Implementation

During the implementation phase of the NexGuard RFID Lock System, the focus is on translating the system architecture and design specifications into working hardware and software components. This involves assembling the hardware components, such as the ESP8266 Microcontroller Module, RFID Reader, Reed Switch Sensor, Solenoid Lock, and Buzzer, into a functional system. Additionally, firmware development for the microcontroller is undertaken to manage system operation, including RFID authentication, intrusion detection, and hardware control. The RFID Authentication Logic and Intrusion Detection Algorithm are implemented to verify RFID tag validity, detect unauthorized access attempts, and trigger appropriate responses. Furthermore, the Email Notification System is integrated to enable real-time alerts to be sent to predefined recipients in the event of security breaches. Throughout the implementation process, rigorous testing and validation procedures are conducted to ensure the reliability, functionality, and security of the NexGuard RFID Lock System.

* 1. **Hardware Setup:**

The hardware setup for the NexGuard RFID Lock System involves assembling the necessary components and configuring them to work together seamlessly. Here's an overview of the hardware setup:

5.1.2 ESP8266 Microcontroller Module:

* Features:

WiFi connectivity

GPIO pins for interfacing with peripherals

Low power consumption

* Advantages:

Cost-effective

Versatile

Compatible with Arduino IDE

* Disadvantages:

Limited processing power and memory compared to more advanced microcontrollers

* Description:

The ESP8266 microcontroller module serves as the central processing unit of the system, facilitating communication between hardware components and executing control logic.

* Additional Information:

The ESP8266 chip integrates a WiFi module and a powerful microcontroller, making it suitable for IoT projects.

* Advanced Features:

Supports TCP/IP protocols for Internet connectivity.

Can operate as a standalone device or as part of a larger network.

Offers deep sleep modes for power conservation in battery-powered applications.

5.1.2 RFID Reader:

* Features:

Read range

Data transfer rate

Compatibility with various RFID tag types

* Advantages:

Fast and convenient access control

Contactless operation

* Disadvantages:

Vulnerable to signal interference

Potential for unauthorized cloning of RFID tags

* Description:

The RFID reader reads unique identification codes stored on RFID tags, enabling secure authentication of users.

* Additional Information:

RFID readers come in various form factors, including handheld, desktop, and fixed-mount models.

* Advanced Features:

Read range can vary from a few centimeters to several meters

Data transfer rates can range from a few kilobits per second to several megabits per second.

5.1.3 Read Switch Sensor:

* Features:

Normally open/closed configuration

High reliability

Simple operation

* Advantages:

Low cost

Long lifespan

Immune to environmental factors

* Disadvantages:

Susceptible to mechanical wear

Limited detection range

* Description:

The reed switch sensor detects changes in the magnetic field when the door is opened or closed, providing real-time status information.

* Additional Information:

Reed switch sensors consist of two ferromagnetic contacts sealed within a glass tube.

* Advanced Features:

Some reed switch sensors feature encapsulation for protection against environmental factors such as dust, moisture, and corrosion.

5.1.4 Solenoid Lock:

* Features:

Electrically operated locking mechanism

Compact size

Durable construction

* Advantages:

Fast response time

High security

Suitable for retrofitting existing door systems

* Disadvantages:

Requires continuous power supply

Potential for mechanical failure

* Description:

The solenoid lock controls access to the secured area by locking or unlocking the door mechanism in response to signals from the microcontroller.

* Additional Information:

Solenoid locks utilize an electromagnetic solenoid to control the locking mechanism.

* Advanced Features:

Some solenoid locks offer monitoring capabilities, allowing for feedback on the lock's status (locked or unlocked).

5.1.5 Buzzer:

* Features:

Audible alarm output

Adjustable volume

Compact size

* Advantages:

Immediate audible alerts

Suitable for noisy environments

* Disadvantages:

Limited to providing auditory feedback

May not be suitable for all users.

* Description:

The buzzer emits audible alarms to alert nearby individuals to unauthorized access attempts or security breaches.

* Additional Information:

Buzzers are electroacoustic transducers that convert electrical signals into audible sound.

* Advanced Features:

Some buzzers offer adjustable volume settings or multiple sound patterns to suit different applications.

5.1.6 12V Power Supply:

* Features:

Voltage regulation for stable power output.

Overcurrent protection to prevent damage to components.

Different form factors such as wall adapters, batteries, or power distribution units.

* Advantages:

Provides consistent and reliable power to system components.

Can be customized to meet specific voltage and current requirements.

Ensures uninterrupted operation of the system.

* Disadvantages:

May introduce heat dissipation issues, especially with high-power devices.

Bulkier compared to other components, depending on the power requirements.

* Description:

The power supply converts AC voltage from the mains electricity into DC voltage suitable for powering electronic devices. It regulates the voltage to ensure stable operation and protects against overcurrent to prevent damage.

* Additional Information:

Power supplies can be classified based on their output voltage and current ratings, such as linear or switching power supplies.

* Advanced Features:

Some power supplies feature remote monitoring and control capabilities, allowing users to monitor output voltage, current, and temperature remotely.

5.1.7 Relay Module:

* Features:

Electromechanical switching for controlling high-power devices.

Isolation between control signals and load circuits.

Different configurations including single-channel and multi-channel variants.

* Advantages:

Provides a safe and reliable method for controlling high-power devices.

Offers isolation between the low-voltage control signal and the high-voltage load, enhancing safety.

Can be easily integrated into the system using standard interface protocols.

* Disadvantages:

Mechanical parts may wear out over time, requiring maintenance or replacement.

Relays consume power when activated, which may impact overall power consumption.

* Description:

The relay module acts as an electromechanical switch, controlled by the microcontroller to switch high-power devices like solenoid locks. It provides isolation between the low-voltage control signal from the microcontroller and the high-voltage load, ensuring safety and reliability in controlling electrical circuits.

**5.2 Software Setup:**

The software setup for the NexGuard RFID Lock System involves configuring the firmware for the ESP8266 microcontroller module and developing the necessary software components to manage system operation. Here's an overview of the software setup:

5.2.1 ESP8266 Firmware Configuration:

* Install the Arduino IDE or another compatible development environment for programming the ESP8266 microcontroller module.
* Configure the IDE to support the ESP8266 board by installing the necessary board definitions and libraries.
* Write and upload the firmware code to the ESP8266 microcontroller module, implementing the control logic for RFID authentication, intrusion detection, and hardware control.

5.2.2 RFID Authentication Logic:

* Develop the RFID authentication logic to verify the validity of RFID tags and grant access to the secured area upon successful authentication.
* Implement functions to interface with the RFID reader, parse RFID tag data, and compare it against authorized tag IDs stored in memory.
* Handle authentication failures by triggering appropriate responses, such as activating the buzzer and sending email notifications.

5.2.3 Intrusion Detection Algorithm:

* Develop the intrusion detection algorithm to monitor changes in the door state detected by the reed switch sensor and trigger alerts for unauthorized access attempts.
* Implement functions to monitor the status of the reed switch sensor, detect door openings and closings, and differentiate between authorized and unauthorized access events.
* Integrate the intrusion detection logic with the overall system operation to coordinate responses to security breaches.

5.2.4 Email Notification System:

* Develop the email notification system to send real-time email notifications to predefined recipients in the event of security breaches.
* Implement functions to establish a connection with an email server, compose and format alert messages, and send emails with relevant information about the security event.
* Configure email notification settings, including recipient email addresses, email server credentials, and message formatting options.

5.2.5 Integration and Testing:

* Integrate the developed software components with the ESP8266 firmware, ensuring compatibility and proper interaction between modules.
* Conduct thorough testing of the software setup to verify the functionality, reliability, and security of the NexGuard RFID Lock System.
* Perform integration testing to validate end-to-end system operation, including RFID authentication, intrusion detection, hardware control, and email notification functionality.

**5.3 Challenges encountered and Resolutions:**

Here are some potential challenges encountered during the development of the NexGuard RFID Lock System and possible resolutions:

5.3.1 Hardware Integration Issues:

* Challenge: Ensuring seamless integration and proper communication between hardware components, such as the RFID reader, reed switch sensor, solenoid lock, and buzzer, can be challenging.
* Resolution: Thoroughly review datasheets, pinout diagrams, and communication protocols for each hardware component. Test individual components separately before integrating them into the system. Debug and troubleshoot any connectivity issues using serial debugging and logic analyzers.

5.3.2 RFID Tag Authentication:

* Challenge: Implementing a robust RFID tag authentication system that effectively verifies the validity of RFID tags while minimizing false positives and false negatives.
* Resolution: Develop a comprehensive authentication logic that includes cryptographic techniques or unique identifiers stored on RFID tags. Implement error handling mechanisms to address issues such as tag collisions or signal interference. Conduct extensive testing with different types of RFID tags to ensure compatibility and reliability.

5.3.3 Intrusion Detection Accuracy:

* Challenge: Achieving accurate intrusion detection to distinguish between authorized and unauthorized access attempts, especially in environments with high ambient noise or electromagnetic interference.
* Resolution: Calibrate the reed switch sensor sensitivity and threshold levels to minimize false alarms while detecting genuine intrusions reliably. Test the intrusion detection algorithm in various environmental conditions to validate its accuracy and effectiveness.

5.3.4 Email Notification Reliability:

* Challenge: Ensuring reliable delivery of email notifications in real-time, especially when relying on external email servers or network connectivity.
* Resolution: Implement robust error handling and retry mechanisms to handle network failures or email server downtime gracefully. Configure email server settings, such as SMTP authentication and port forwarding, correctly to ensure proper email delivery. Monitor email delivery logs and implement email status feedback mechanisms to track the success or failure of email notifications.

5.3.5 Security Considerations:

* Challenge: Addressing security vulnerabilities, such as RFID tag cloning, unauthorized access to system firmware, or email interception, to safeguard the integrity and confidentiality of the system.
* Resolution: Implement encryption techniques, secure authentication protocols, and access control mechanisms to protect sensitive data and system resources. Regularly update firmware and software components to patch security vulnerabilities and mitigate emerging threats. Conduct security audits and penetration testing to identify and address potential security weaknesses proactively.

1. **Result & Evaluation**

Following the implementation of the NexGuard RFID Lock System, several outcomes have been observed. Firstly, the system has proven highly effective in safeguarding locker assets. The integration of RFID technology and reed switch sensors ensures that only authorized users can access the lockers, thereby reducing the risk of theft or unauthorized access. Additionally, the solenoid lock mechanism provides an added layer of security by physically securing the lockers when not in use.

Furthermore, the system has been successful in mitigating unauthorized access attempts. In the event of an invalid RFID tag being detected or an attempt to open the locker without proper authorization, the system promptly triggers a buzzer alarm and sends real-time email notifications. This immediate response acts as a deterrent to potential intruders and alerts nearby individuals to the security breach.

In terms of reliability, the system has demonstrated consistent performance in controlling access to the lockers and providing security alerts. Users have reported satisfaction with the system's ease of use and its ability to effectively manage access to valuable assets. Moreover, the integration of the NexGuard RFID Lock System with existing infrastructure has been relatively seamless, requiring minimal disruption to operations.

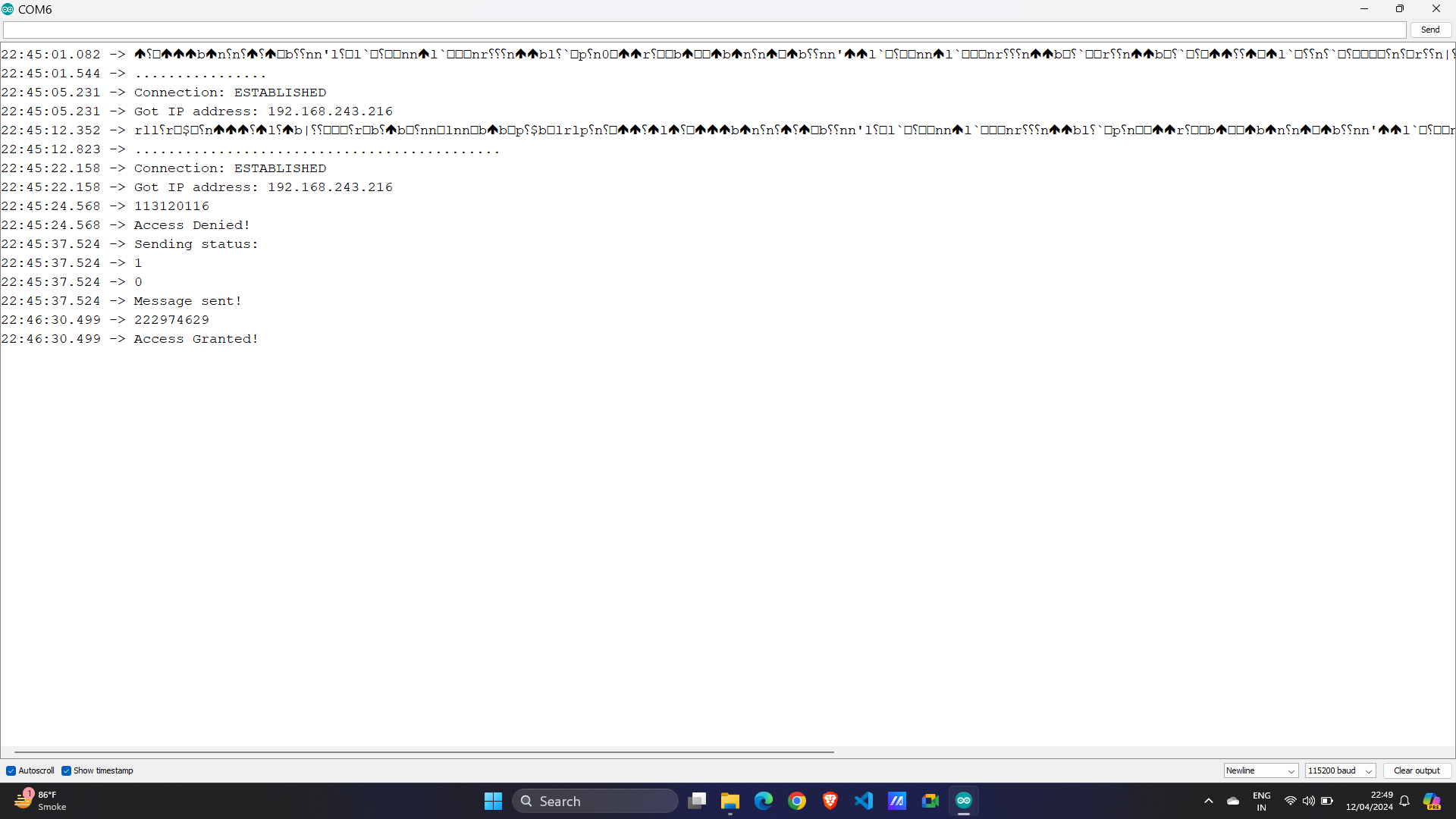


Figure 6.1: Serial Monitor

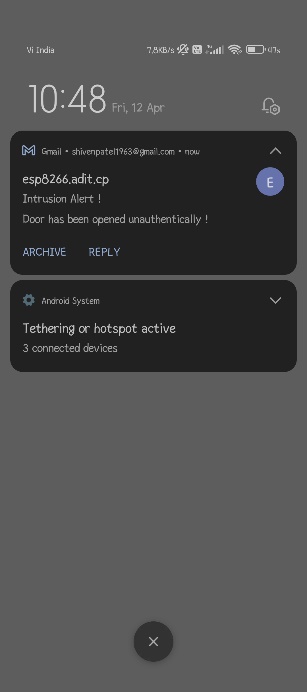
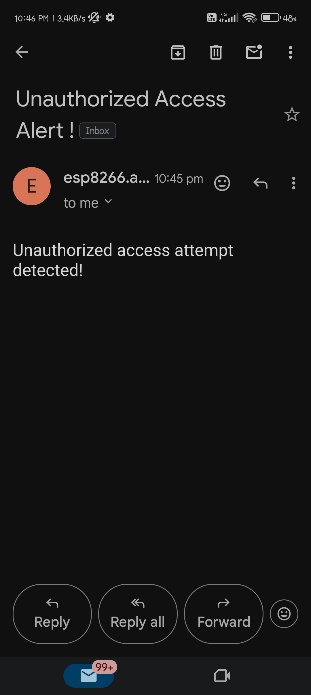
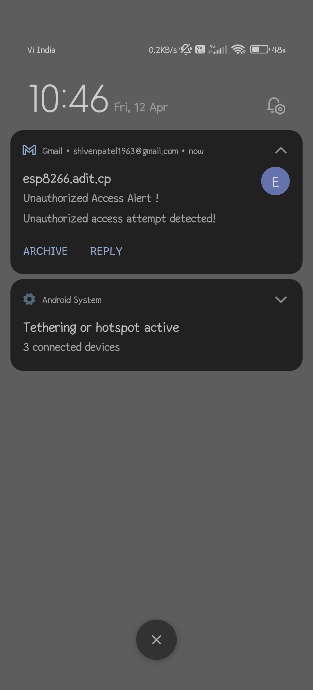
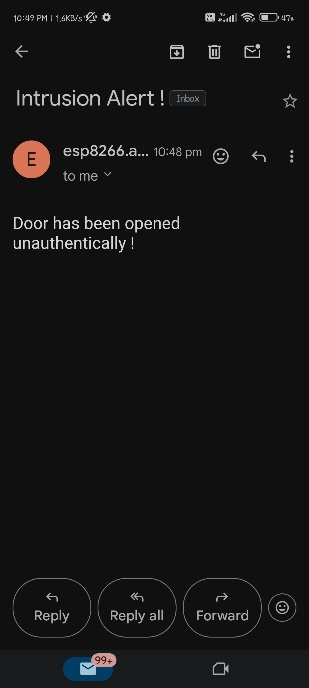
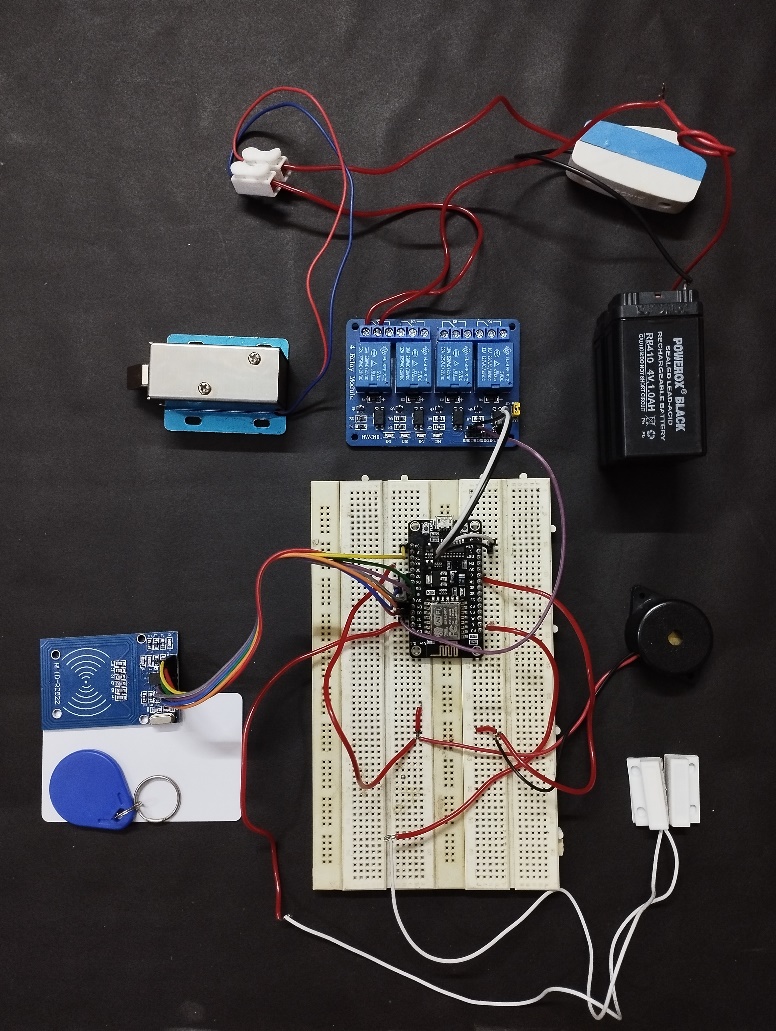


Figure 6.2: Unauthorized Access and Intrusion Alert Emails Send by ESP8266 NodeMCU



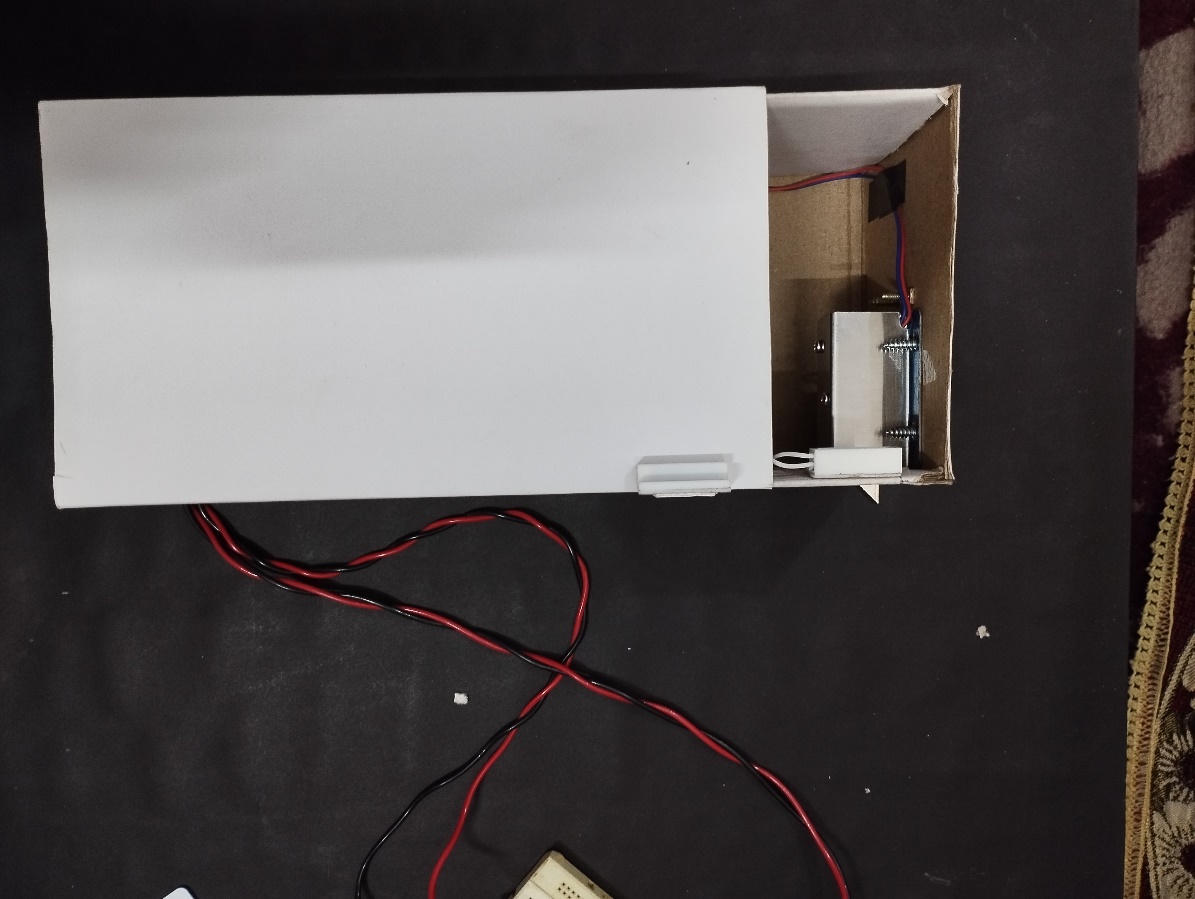




Figure 6.3: Overall Project Appearance

# Summary and Conclusion

In the culmination of the NexGuard RFID Lock System project, it's evident that the integration of RFID technology, reed switch sensors, and email notification capabilities has resulted in a sophisticated security solution. This system, meticulously developed to safeguard valuable assets, embodies a synergy of modern technologies aimed at fortifying access control mechanisms and detecting unauthorized intrusions.

Throughout the project lifecycle, numerous challenges emerged, each met with strategic resolutions to ensure the system's efficacy and resilience. The intricate process of hardware integration demanded meticulous attention to detail to guarantee seamless communication between components. Moreover, the implementation of robust RFID tag authentication posed a significant challenge, requiring the deployment of sophisticated algorithms to minimize false positives and negatives.

Intrusion detection accuracy emerged as another paramount concern, especially in environments prone to noise and interference. Calibration of the reed switch sensors and the implementation of debounce algorithms played instrumental roles in achieving reliable detection while mitigating false alarms. Additionally, ensuring the reliability of email notifications presented a challenge, necessitating the development of robust error-handling mechanisms to circumvent network failures and email server downtime.

Central to the project's success was the rigorous consideration of security implications. Addressing potential vulnerabilities, such as RFID tag cloning and unauthorized access to system firmware, demanded the implementation of stringent encryption techniques and access control protocols. Regular security audits and penetration testing were pivotal in identifying and rectifying vulnerabilities, ensuring the system's resilience against emerging threats.

As the project concludes, it is paramount to emphasize the importance of ongoing maintenance and vigilance. Continuous monitoring, firmware updates, and system audits will be indispensable in upholding the system's integrity and effectiveness over time. Furthermore, proactive measures to address emerging threats will be crucial in sustaining the system's viability and relevance in the ever-evolving landscape of security technology.

In essence, the NexGuard RFID Lock System stands as a testament to the fusion of innovation and practicality in addressing the pressing need for enhanced security measures. With its robust architecture, meticulous implementation, and unwavering commitment to security, the system embodies a paradigm shift in access control technology, offering unparalleled peace of mind and protection for valuable assets and premises

# Future Work

1. **Mobile Application Development:**

Develop a mobile application compatible with iOS and Android platforms to complement the existing hardware system.

Design an intuitive user interface (UI) that allows users to remotely monitor and control the RFID lock system from their smartphones.

Implement features such as real-time status updates, remote lock/unlock functionality, and notification settings customization within the app.

1. **Enhanced Security Features:**

Implement biometric authentication methods (e.g., fingerprint or facial recognition) within the mobile app for enhanced security.

Enable two-factor authentication (2FA) for user logins to prevent unauthorized access to the system.

Implement end-to-end encryption for communication between the mobile app and the RFID lock system to protect sensitive data.

1. **Advanced Monitoring and Analytics:**

Integrate advanced monitoring and analytics features into the mobile app to provide insights into access patterns, security breaches, and system performance.

Implement data visualization tools (e.g., charts, graphs) to present access event history and system health metrics in an easily understandable format.

Enable proactive alerts and notifications for anomalies or suspicious activities detected by the system, enhancing security awareness for users.

By embarking on these future endeavors, the NexGuard RFID Lock System can evolve into a comprehensive and versatile security solution that seamlessly integrates with mobile devices, offers advanced features for monitoring and control, and provides enhanced security and convenience for users.

# References

* International Journal of Engineering Research & Technology(IJERT):Vol.5Issue12- IoT based Smart Home Security System with Alert and Door Access Control Using Smart Phone[[http://www.ijert.org](http://www.ijert.org/)]
* IOP Conf.Series : Materials Science and Engineering 263:Home Security using Internet of Things-Anitha A, VIT Vellore.
* International Journal for Scientific Research & Development(IJSRD):Intrusion Detection System for Smart Home using Internet of Things-Govinda K, Sai Krishna Prasad K and Sai Ram Susheel. Technology (IJERT), 7(11), 775-779.
* https://iotprojectsideas.com/iot-smart-rfid-door-lock-system-using-nodemcu-esp8266/
* 2022, International Journal for Research in Applied Science and Engineering Technology: https://[www.academia.edu/91100725/IOT\_Based\_Smart\_Door\_Locked\_System\_Usin](http://www.academia.edu/91100725/IOT_Based_Smart_Door_Locked_System_Usin)g\_Node\_MCU