# RFID BASED DOOR LOCKING SYSTEM WITH SMS ALERT

## A MINI-PROJECT REPORT

***Submitted by***

| **VIKRAM S** | **210701504** |
| --- | --- |
| **KUMARAVEL N** | **210701127** |
|  |  |

***in partial fulfilment of the award of the degree***

***of***

# BACHELOR OF ENGINEERING

**IN**

**COMPUTER SCIENCE AND ENGINEERING**

**RAJALAKSHMI ENGINEERING COLLEGE, CHENNAI**



## RAJALAKSHMI ENGINEERING COLLEGE, CHENNAI

**An Autonomous Institute**

# CHENNAI APRIL 2024

## BONAFIDE CERTIFICATE

Certified that this project **“RFID BASED DOOR LOCKING SYSTEM WITH SMS ALERT**” is the bonafide work of “**VIKRAM S(210701504), KUMARAVEL N(210701127)”** who carried out the project work under my supervision.

**SIGNATURE SIGNATURE**

**Dr. P. Kumar, Dr.N. Duraimurugan, M,E., Ph.D.**

**HEAD OF THE DEPARTMENT,**

Professor and Head, Academic Head, Associate Professor,

Computer Science & Engineering Computer Science & Engineering

Rajalakshmi Engineering Rajalakshmi Engineering College

College (Autonomous) (Autonomous)

Thandalam, Chennai -602105. Thandalam, Chennai -602105.

Submitted for the **ANNA UNIVERSITY** practical examination Mini-Project work viva voce held on \_

**INTERNAL EXAMINER EXTERNAL EXAMINER**

## ACKNOWLEDGEMENT

We express our sincere thanks to our beloved and honourable chairman **MR. S. MEGANATHAN** and the chairperson **DR. M. THANGAM MEGANATHAN** for their

timely support and encouragement.

We are greatly indebted to our respected and honourable principal **Dr. S.N. MURUGESAN** for his able support and guidance.

No words of gratitude will suffice for the unquestioning support extended to us by our head of the department **Dr. P. Kumar** for being ever supporting force during our project work.

We also extend our sincere and hearty thanks to our internal guide **Dr.N.Duraimurugan,M.E., Ph.D** for his valuable guidance and motivation during the completion of this project. Our sincere thanks to our family members, friends and other staff members of information technology.

## TABLE OF CONTENTS

**CHAPTER NO. TITLE PAGE**

[**ABSTRACT 7**](#_gjdgxs)

1. **INTRODUCTION 8**
   1. [INTRODUCTION 8](#_30j0zll)
   2. [SCOPE OF THE WORK 8](#_1fob9te)
   3. [PROBLEM STATEMENT 8](#_3znysh7)
   4. [AIM AND OBJECTIVES OF THE PROJECT](#_2et92p0) 9
2. **LITERATURE SURVEY 10**
3. **SYSTEM SPECIFICATIONS 12**
   1. [HARDWARE SPECIFICATIONS FOR APPLICATION 1](#_tyjcwt)2
   2. SOFTWARE SPECIFICATIONS FOR APPLICATION 12
   3. HARDWARE SPECIFICATIONS FOR PROTOTYPE 12
4. **MODULE DESCRIPTION 13**
5. **SYSTEM DESIGN 14**
   1. [FLOWCHART 1](#_3dy6vkm)4
   2. [CIRCUIT DIAGRAM 1](#_1t3h5sf)5
6. **SAMPLE CODING 16**
7. **SCREEN SHOTS 20**
8. **CONCLUSION AND FUTURE ENHANCEMENT 21**

[**REFERENCES**](#_4d34og8) **22**

**LIST OF FIGURES**

| **FIGURE NO** | **FIGURE NAME** | **PAGE NO.** |
| --- | --- | --- |
| 5.1 | FLOW CHART | 14 |
| 5.2 | CIRCUIT DIAGRAM | 15 |
| 7.1 | CONNECTION | 20 |

## LIST OF ABBREVIATION

**ABBREVIATION ACRONYM**

**SMS** Short Message Service

**GSM** Global System for Mobile Communications

**RFID** Radio Frequency Identification

**MCU** Microcontroller Unit

**SIM** Subscriber Identity Module

**LCD** Liquid Crystal Display

# Abstract

This project presents the design and development of a secure and user-friendly door access control system utilizing Radio Frequency Identification (RFID) technology. The system offers convenient keyless entry for authorized personnel while maintaining robust security measures. It achieves this through a combination of RFID tag verification and a real-time alert mechanism.The core functionality revolves around an RFID reader positioned near the door. Users gain access by presenting a designated RFID tag, typically a key fob or card, to the reader. The system employs a microcontroller unit (MCU) to interact with the reader and manage the access control process. Upon detecting a tag, the MCU retrieves the unique identifier associated with it. This identifier is then compared against a pre-programmed database of authorized users stored within the system's memory. If the scanned tag matches a valid user, the MCU transmits a signal to the door lock, triggering its release and granting access. Conversely, if the tag is unrecognized or unauthorized, the system immediately initiates the alert mechanism. This alert can be configured in various ways to suit specific needs. Potential options include activating a visual indicator like an LED light, sounding an audible alarm, or sending real-time notifications via SMS or mobile app push messages. The real-time alert feature offers a significant advantage by notifying designated personnel, such as security personnel or building managers, of unauthorized access attempts. This allows for immediate response and investigation, potentially deterring further intrusion attempts and enhancing overall security. The project emphasizes user convenience alongside security. RFID tags offer a faster and more reliable access method compared to traditional keys. Additionally, the system can be programmed to manage access rights for different users, allowing temporary or restricted access for specific situations. Furthermore, the system can be integrated with additional security features. Data logs can be maintained, recording access attempts with timestamps and user identification. This data can be used for auditing purposes or to identify access patterns. Overall, this RFID-based door access control system with a real-time alert mechanism provides a secure and user-friendly solution for managing access points in various environments, including residential buildings, offices, restricted areas, or any location requiring controlled entry.

**CHAPTER 1**

**INTRODUCTION**

## INTRODUCTION

This project proposes a secure and user-centric door access control system utilizing Radio Frequency Identification (RFID) technology. It prioritizes convenience with keyless entry for authorized personnel while maintaining robust security. This is achieved through a combination of RFID tag verification and a real-time alert mechanism. Further development could explore integration with existing security systems for comprehensive monitoring and advanced access management functionalities like user access logs and temporary access control.

## SCOPE OF THE WORK

The research looks at a safe and user-friendly door access control system that uses Radio Frequency Identification (RFID) technology. It focuses user comfort, providing keyless entry for authorized workers while retaining strong security. This is accomplished by integrating RFID tag verification with a real-time alerting system. This novel solution simplifies access control, improves security with rapid unlawful access warnings, and provides significant user comfort. It provides a convincing solution for varied access control requirements in a variety of settings, including residential buildings, offices, and restricted locations.

## PROBLEM STATEMENT

This project explores an Arduino Uno-based RFID access control system. It prioritizes user convenience with keyless entry and enhanced security through real-time SMS alerts for unauthorized access (GSM module). This innovative approach streamlines access control and offers a compelling solution for various environments. Further development could explore integration with existing security systems for advanced management features.



## AIM AND OBJECTIVES OF THE PROJECT

This project aims to create a secure door access system using an Arduino Uno and RFID tags for authorized entry. An additional layer of security comes from a GSM module that sends SMS alerts upon intrusion detection. The Arduino reads RFID tags, controls the door lock, and triggers an alert with relevant information if the door is opened without a valid tag. This system offers a balance between convenience with keyless entry and enhanced security with intruder notification.

**CHAPTER 2**

## LITERATURE SURVEY

Door access control systems play a crucial role in safeguarding physical security. Traditional methods using physical keys are prone to loss or duplication. RFID technology offers a compelling alternative, providing keyless entry with enhanced security and convenience. This survey explores existing research on RFID-based door access control systems, focusing on real-time alert mechanisms for unauthorized access attempts.

Several studies highlight the advantages of RFID for access control. One system integrates RFID tags with a central server for user authentication and access control, replacing physical keys with secure and convenient tags. Another utilizes an RFID reader and an electromagnetic lock, incorporating a GSM module for sending SMS alerts upon unauthorized access attempts, demonstrating a basic real-time alert mechanism.

Research has delved into advancements in user authentication and access management. An Arduino-based system for RFID tag verification and door access control emphasizes the ease of implementation using readily available platforms. It explores various RFID tag types (active vs. passive) for access control applications, highlighting the importance of understanding tag characteristics for optimal system design.

Beyond basic user authentication, another study explores an RFID system combined with biometrics for access control. This system captures user images upon unauthorized access attempts, offering an additional security layer through multi-factor authentication. This integration highlights the potential for more sophisticated security measures.

Security considerations are paramount. While some systems rely on a central server for user authentication, others explore integrating access control systems with building management systems. This integration offers centralized control and monitoring capabilities, providing a more comprehensive security solution.

Further research and development can explore advanced functionalities. User access logs can be implemented to track entry and exit times, providing valuable audit trails. Time-based access restrictions can be programmed, allowing authorized personnel access only during designated periods. These functionalities contribute to a more comprehensive and secure access control solution.

In conclusion, the growing body of research on RFID-based door access control systems demonstrates the effectiveness of RFID technology for keyless entry and user authentication. The inclusion of real-time alert mechanisms for unauthorized access attempts adds a vital layer of security. Future advancements will likely explore integration with existing security systems and the development of more sophisticated access management functionalities. This project contributes to this ongoing development by exploring an Arduino Uno-based system with an SMS alert mechanism, offering a user-friendly and secure solution for various access control needs.

# CHAPTER 3

## SYSTEM SPECIFICATIONS

## HARDWARE SPECIFICATIONS FOR APPLICATION

| Processor | **:** | Pentium IV Or Higher |
| --- | --- | --- |
| Memory Size | **:** | 256 GB (Minimum) |
| HDD | **:** | 40 GB (Minimum) |

## SOFTWARE SPECIFICATIONS

| Operating System | **:** | WINDOWS 10 AND PLUS |
| --- | --- | --- |
| Application | **:** | ARDUINO IDE |

* 1. **HARDWARE COMPONENTS FOR PROTOTYPE**

| Sensor | **:** | IR-Sensor |  |
| --- | --- | --- | --- |
| Board | **:** | Arduino Uno |  |
| Actuator | **:** | Micro Servo Motor 9g |  |
| Communication |  | **:** GSM Module |  |

## RFID Module:

**CHAPTER 4**

## MODEL DESCRIPTION

This is the core model for user authentication and keyless entry. It involves RFID tags carried by authorized personnel and an RFID reader at the access point. The reader transmits radio waves to identify and verify the tags, granting access to those with valid credentials..

## Microcontroller Module:

This project leverages an Arduino Uno, a popular microcontroller platform. The Arduino Uno acts as the brain of the system, processing data from the RFID reader and controlling the door lock mechanism. It verifies the tag ID against a stored list of authorized users and triggers the appropriate action (unlock or lock) based on the verification outcome.

## Communication Module (GSM Module):

The project incorporates a GSM module for real-time alerts. This module enables the system to send SMS notifications to a designated phone number upon unauthorized access attempts. This real-time communication enhances security by informing personnel about potential security breaches.

## Access Control Module:

This overarching module governs the entire system's functionality. It defines the rules and protocols for user access, including authorized personnel, access times (if applicable), and the response to unauthorized attempts.The Access Control Model essentially determines who can enter, when they can enter, and where within the controlled area they can go. It acts as the central authority, ensuring the system grants access only to authorized personnel under the appropriate circumstances. This model interacts with other models in the system, like the RFID model for user identification and the microcontroller model for access control decisions.



# CHAPTER 5

## SYSTEM DESIGN

## FLOW CHART

A flowchart is a type of diagram that represents an algorithm, workflow or process. The flowchart shows the steps as boxes of various kinds, and their order by connecting the boxes with arrows. This diagrammatic representation illustrates a solution model to a given problem.

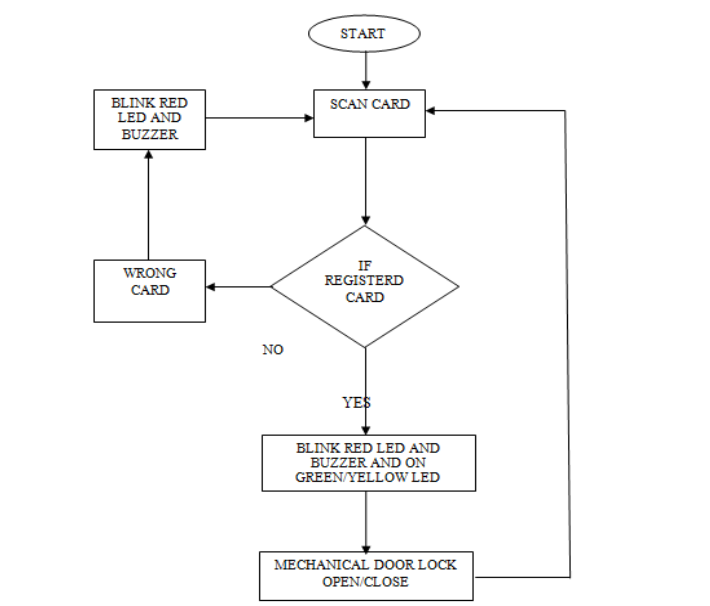


Figure 5.1 Flow Chart



## CIRCUIT DIAGRAM

The circuit diagram explains the connections made with the hardware components and the board. The Arduino uno is connected with the breadboard as the VCC and GND are connected with the rails. The Sensors, LCD and Servo motor is given connection with the rails and the other input/output pins are connected to digital as per the requirements.

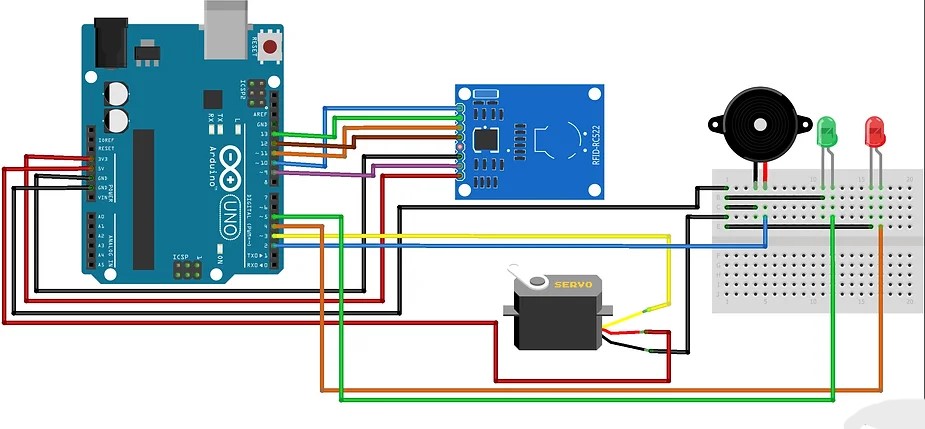


Figure 5.2 Circuit diagram From the above figure 5.2, the connections are made.



# CHAPTER 6

## CODING

#include <SPI.h>

#include <MFRC522.h>

#include <Servo.h>

#include <SoftwareSerial.h>

#define SS\_PIN 10

#define RST\_PIN 9

#define LED\_G 4 //define green LED pin

#define LED\_R 5 //define red LED

#define BUZZER 2 //buzzer pin

MFRC522 mfrc522(SS\_PIN, RST\_PIN); // Create MFRC522 instance.

Servo myServo; //define servo name

SoftwareSerial sim800(6, 7); // RX, TX

void setup()

{

Serial.begin(9600); // Initiate a serial communication

SPI.begin(); // Initiate SPI bus

mfrc522.PCD\_Init(); // Initiate MFRC522

myServo.attach(3); //servo pin

myServo.write(0); //servo start position

pinMode(LED\_G, OUTPUT);

pinMode(LED\_R, OUTPUT);

pinMode(BUZZER, OUTPUT);

noTone(BUZZER);

Serial.println("Put your card to the reader...");

Serial.println();

sim800.begin(9600);

Serial.println("Initializing...");

delay(1000);

// Test if the SIM800L module is responding

sim800.println("AT");

delay(1000);

if (sim800.available()) {

Serial.println("SIM800L Ready");

} else {

Serial.println("SIM800L not responding");

}

// Set SMS mode to text

 sendCommand("AT+CMGF=1", 1000);

}

void loop()

{

// Look for new cards

if ( ! mfrc522.PICC\_IsNewCardPresent())

{

return;

}

// Select one of the cards

if ( ! mfrc522.PICC\_ReadCardSerial())

{

return;

}

//Show UID on serial monitor

Serial.print("UID tag :");

 String content= "";

byte letter;

for (byte i = 0; i < mfrc522.uid.size; i++)

{

Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");

Serial.print(mfrc522.uid.uidByte[i], HEX);

content.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));

content.concat(String(mfrc522.uid.uidByte[i], HEX));

}

Serial.println();

Serial.print("Message : ");

content.toUpperCase();

if (content.substring(1) == "43 65 A0 FA") //change here the UID of the card/cards that you want to give access

{

Serial.println("Authorized access");

Serial.println();

delay(500);

digitalWrite(LED\_G, HIGH);

tone(BUZZER, 500);

delay(300);

noTone(BUZZER);

myServo.write(180);

delay(5000);

myServo.write(0);

digitalWrite(LED\_G, LOW);

}

else {

Serial.println(" Access denied");

digitalWrite(LED\_R, HIGH);

 tone(BUZZER, 300);

delay(1000);

digitalWrite(LED\_R, LOW);

noTone(BUZZER);

sendSMS("phone number", "Unauthorized access");

}

}

void sendCommand(String command, const int timeout) {

sim800.println(command);

delay(timeout);

while (sim800.available()) {

Serial.write(sim800.read());

}

}

void sendSMS(String number, String text) {

sendCommand("AT+CMGS=\"" + number + "\"", 1000);

sim800.println(text);

delay(100);

sim800.println((char)26); // ASCII code for CTRL+Z to send the SMS

delay(1000);

if (sim800.available()) {

Serial.println("SMS sent successfully");

} else {

Serial.println("SMS failed to send");

}

}

# CHAPTER 7

## SCREEN SHOTS

1. **CONNECTION**

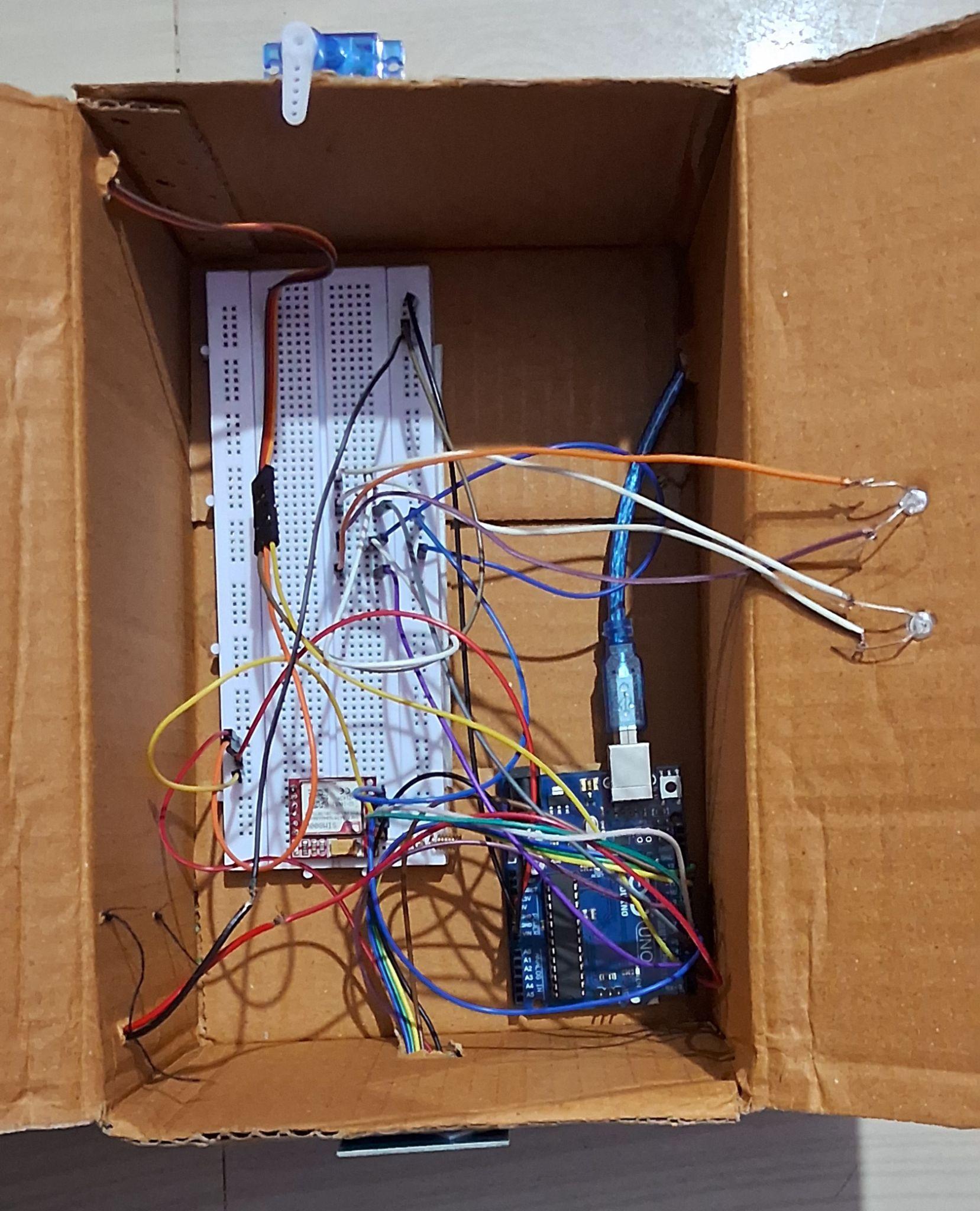
****

Figure 7.1 Connection Setup

RFID access control system with real-time alerts is secure and user-friendly. Future upgrades are exciting! Integrating with building management systems creates a central hub for access monitoring, streamlining security. Advanced user management with roles ensures personnel only access authorized areas. Adding biometrics like fingerprints strengthens security further. A mobile app for unlocking doors and receiving alerts enhances user convenience. We can also implement two-factor authentication and tamper detection for even stronger security. Data logging and reporting will aid security audits.



# CHAPTER 8

## CONCLUSION AND FUTURE ENHANCEMENT

This project demonstrably built a user-friendly and secure RFID-based door access control system with real-time alerts. While the current prototype effectively utilizes RFID technology for secure keyless entry and an Arduino Uno for processing, future advancements can significantly enhance its capabilities. Integration with existing building management systems could offer centralized control and monitoring of access points across entire facilities, streamlining security management. Advanced user management with roles and permissions would allow for more granular control, granting access to specific areas based on user designations, ensuring personnel only have access to authorized spaces. Biometric integration, such as fingerprint scanners or facial recognition, could be layered on top of RFID tags, creating a multi-factor authentication system that significantly strengthens security. Developing a mobile application for access control would offer greater user convenience, allowing users to unlock doors with their smartphones or receive real-time notifications directly through the app. Enhanced security features like two-factor authentication (e.g., requiring a PIN code alongside the RFID tag) could further fortify security protocols. Additionally, incorporating tamper detection mechanisms for the RFID reader and door lock would deter potential physical attacks. Finally, the system could be expanded to log access attempts (authorized and unauthorized) and generate reports for security audits. This data logging and reporting would provide valuable insights for monitoring access patterns and identifying potential security concerns. By implementing these future advancements, this project has the potential to transform from a functional prototype into a robust, user-friendly, and highly secure access control solution with broad applicability across various environments.

## REFERENCES

1. Chit, M. M. T., Srisiri, W., Siritantikorn, A., Kongruttanachok, N., & Benjapolakul, W. (2021, December). Application of RFID and IoT technology into specimen logistic system in the healthcare sector. In *2021 3rd International Conference on Advancements in Computing (ICAC)* (pp. 7-12). IEEE.
2. Makanjuola, O. A., Abegunde, O. O., Adedoyin, O. M., & Olatinwo, D. A. (2022, June). An Rfid-Based Access Control System Using Electromagnetic Door Lock and an Intruder Alert System. Journal of Electrical and Electronic Engineering, 22(11), 7-17.
3. Thornton, Frank, and Chris Lanthem. *RFID security*. Elsevier, 2006.
4. Rieback, Melanie R., Bruno Crispo, and Andrew S. Tanenbaum. "The evolution of RFID security." *IEEE Pervasive Computing* 5, no. 01 (2006):

62-69.

1. Pateriya, R. K., and Sangeeta Sharma. "The evolution of RFID security and privacy: A research survey." In *2011 International Conference on Communication Systems and Network Technologies*, pp. 115-119. IEEE, 2011.