MADRAS INSTITUTE OF TECHNOLOGY
ANNA UNIVERSITY

IT5611 EMBEDDED SYSTEMS AND INTERNET OF THINGS LABORATORY

Entry Monitoring System Using RFID Integrated Identity Cards

PROJECT REPORT

SUBMITTED BY:

1) MOHESH B 2021506050

2) MONISHA H 2021506051

3) MUTHUVARSHINI S – 2021506054

DEPARTMENT OF INFORMATION TECHNOLOGY
ANNA UNIVERSITY, MIT CAMPUS

CHROMPET, CHENNAI – 600 044

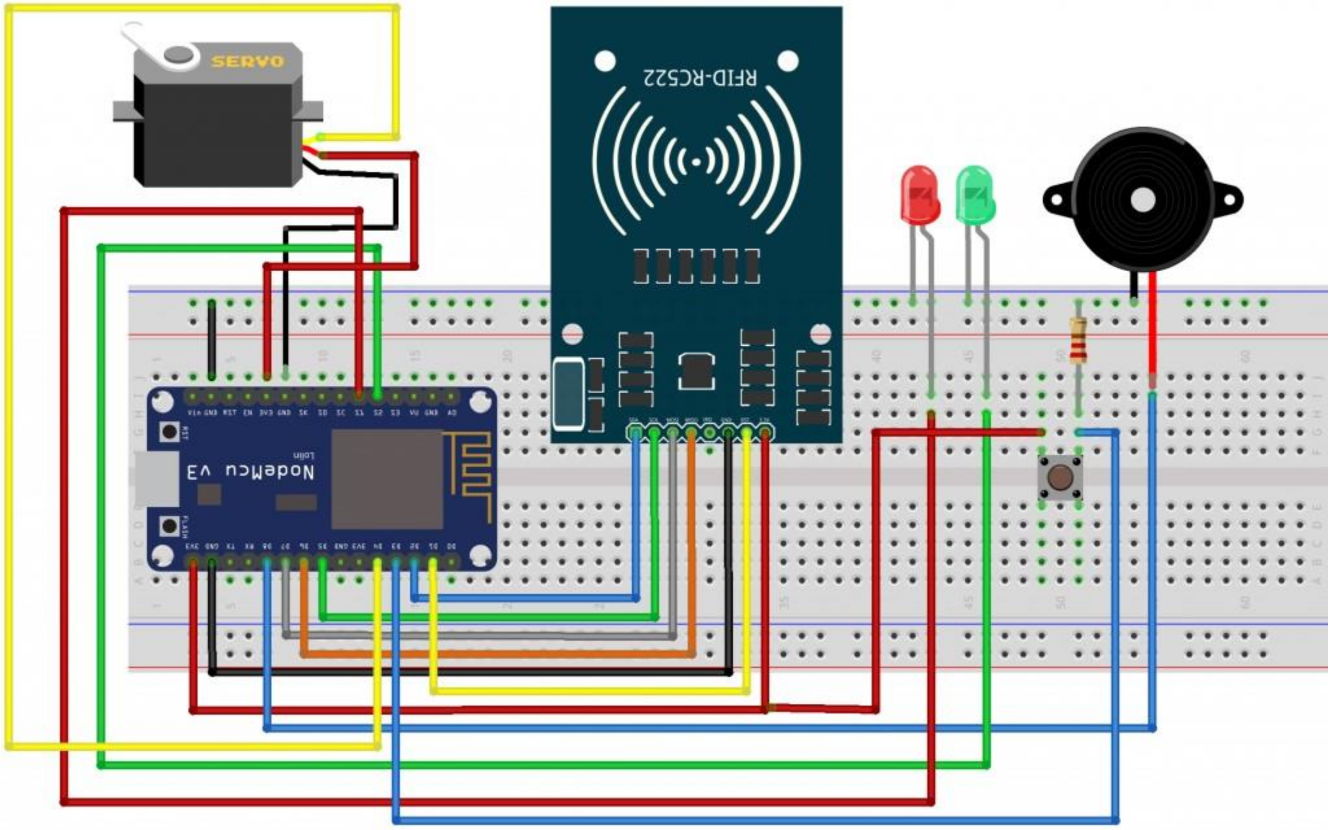
OBJECTIVE:

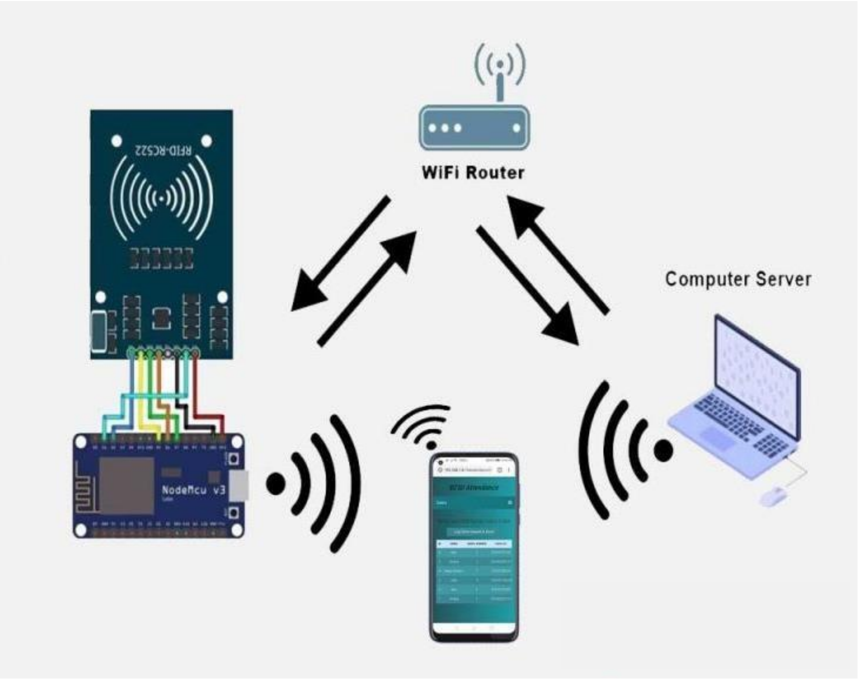
The primary objective of this project is to design and implement an automated entrance monitoring system using RFID technology and an Arduino microcontroller. The system aims to enhance security, streamline access control, and improve the efficiency of monitoring and managing entry points in various facilities, such as offices, schools, and residential complexes. The specific objectives are as follows:

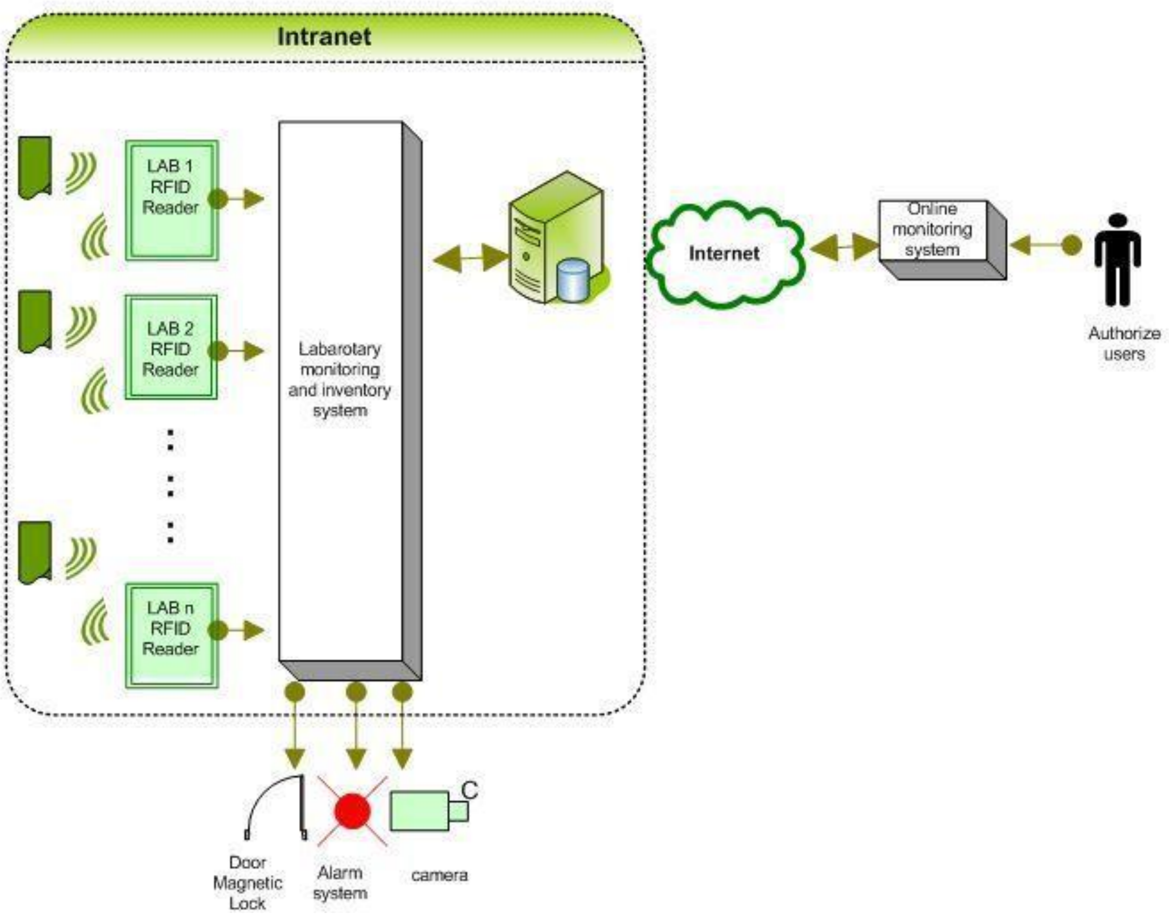
1. Automate Access Control: To develop a system that automates the process of granting or denying access based on the presence of authorized RFID tags, thereby reducing the need for manual checks and supervision.
2. Enhance Security: To improve security by ensuring that only individuals with authorized RFID tags can gain access to the premises, thus preventing unauthorized entry and enhancing the overall safety of the facility.
3. Efficient Monitoring and Logging: To implement a reliable logging system that records each access attempt, including both successful and unsuccessful entries, providing a detailed log for security audits and monitoring purposes.
4. User-Friendly Interface: To create an intuitive and user-friendly interface, including visual and auditory feedback mechanisms (such as LCD displays and buzzers), to inform users of their access status in real-time.
5. Scalability and Flexibility: To design a system that is easily scalable and adaptable to different environments and requirements, allowing for future upgrades and the integration of additional features, such as remote monitoring and centralized control via network interfaces.
6. Cost-Effectiveness: To develop a cost-effective solution using readily available and affordable components (such as Arduino boards and RFID readers) that can be easily implemented and maintained.
7. Minimal Intrusion: To ensure the system operates with minimal disruption to regular activities, allowing for smooth and efficient entry and exit of individuals without significant delays or inconvenience.

By achieving these objectives, the project aims to create a robust and efficient entrance monitoring system that leverages the capabilities of RFID technology and Arduino microcontrollers to enhance security and streamline access control processes.

Circuit diagram:







Algorithm for RFID and Arduino-Based Entrance Monitoring System

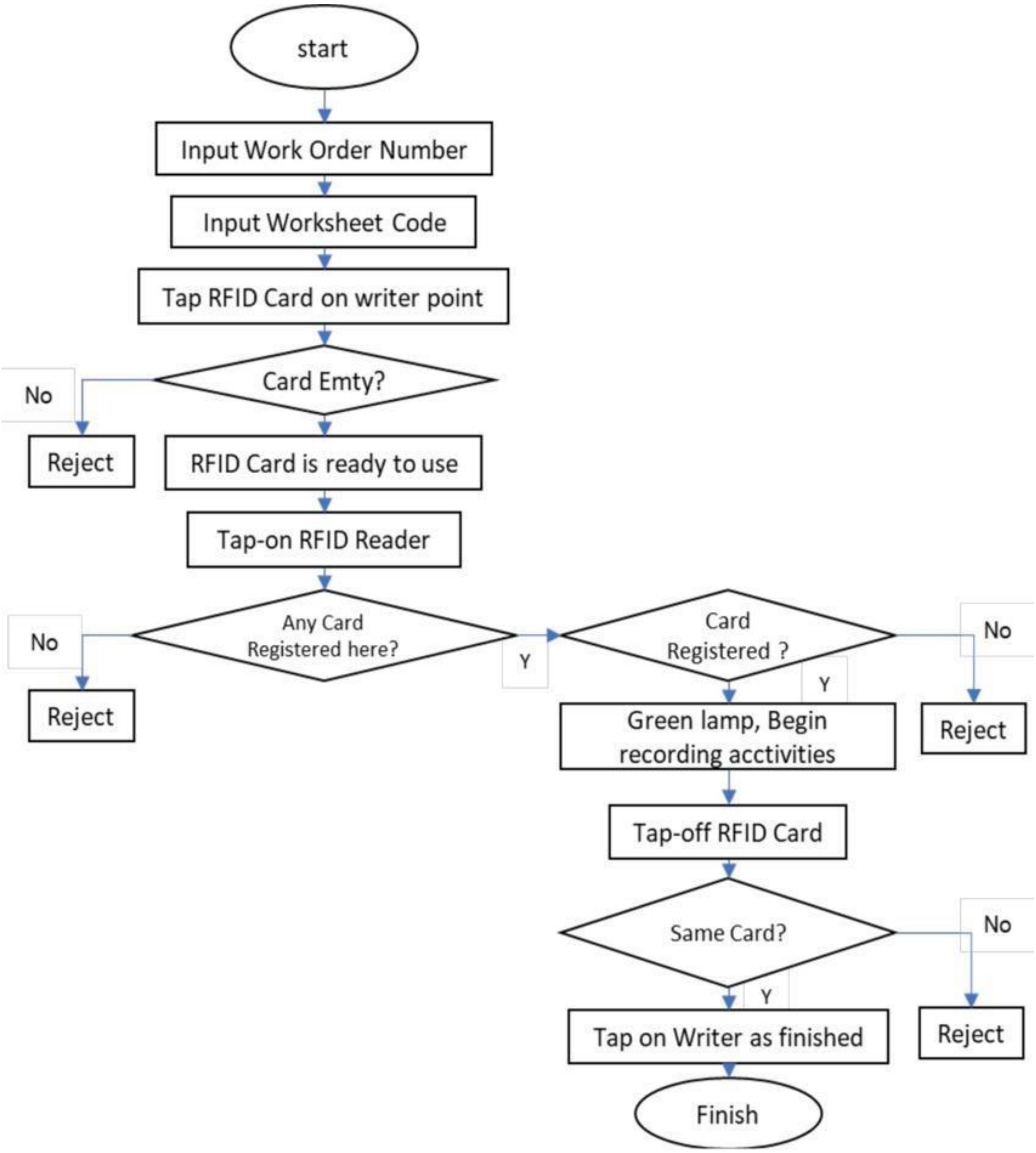
1. **Initialization:**
   - Initialize the Arduino microcontroller.
   - Initialize the RFID reader and ensure it is connected to the Arduino.
   - Initialize the display system (LCD/LED) and the buzzer.
   - Load the database of authorized RFID tags into the Arduino's memory or ensure connectivity to an external database.
2. **Main Loop:**
   - Continuously check for an RFID tag within the reader's range.
3. **Tag Detection:**
   - When an RFID tag is detected, read its unique ID.
4. **Data Processing:**
   - Compare the detected RFID tag's ID against the list of authorized IDs stored in the database.
5. **Decision Making:**
   - If the RFID tag ID is found in the database (Authorized):
     - Grant access:

        - Activate the mechanism to open the gate/turnstile.
        - Display "Access Granted" on the display.
        - Sound a short confirmation beep on the buzzer.
        - Log the access attempt as successful in the database.
- If the RFID tag ID is not found in the database (Unauthorized):
    - Deny access:
        - Do not open the gate/turnstile.
        - Display "Access Denied" on the display.
        - Sound a long error beep on the buzzer.
        - Log the access attempt as unsuccessful in the database.

6. **Logging:**
    - Record the timestamp, RFID tag ID, and access decision (granted or denied) in the log for future reference and auditing.
    - If the system is connected to a network send the log entry to a remote server or central database for centralized monitoring
    - **Return to Main Loop:**

   After processing each RFID tag, return to the main loop to wait for the next tag detect

FLOW CHART:


start
Input Work Order Number
Input Worksheet Code
Tap RFID Card on writer point
Card Emty?
No
Reject
RFID Card is ready to use
Tap-on RFID Reader
Any Card
Registered here?
No
Reject
Y
Card
Registered ?
No
Reject
Y
Green lamp, Begin
recording acctivities
Tap-off RFID Card
Same Card?
No
Reject
Y
Tap on Writer as finished
Finish

SOURCE CODE:

```
// Include necessary libraries
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>
#include <SoftwareSerial.h>  // Include the SoftwareSerial library

// Define the RFID sensor pins
#define SS_PIN 10
#define RST_PIN 9

// Define pins for devices
const int greenLedPin = 5;
const int redLedPin = 4;
const int buzzerPin = 7;
const int servoPin = 3;

// Define pins for Bluetooth communication
const int bluetoothRXPin = 0;  // HC-05 TX pin connected to Arduino RX pin
const int bluetoothTXPin = 1;  // HC-05 RX pin connected to Arduino TX pin

// Create instances
MFRC522 rfid(SS_PIN, RST_PIN);
Servo myServo;
SoftwareSerial bluetooth(bluetoothRXPin, bluetoothTXPin);  // RX, TX

// Define authorized UID and passcode
byte authorizedUID[4] = {0x13, 0xBB, 0xCE, 0x1C};
const String passcode = "Opensesay";

void setup() {
   // Initialize serial communications
   Serial.begin(9600);
   bluetooth.begin(9600);

   // Initialize SPI bus and RFID reader
   SPI.begin();
   rfid.PCD_Init();

   // Initialize devices and servo motor
   pinMode(greenLedPin, OUTPUT);
   pinMode(redLedPin, OUTPUT);
   pinMode(buzzerPin, OUTPUT);
   myServo.attach(servoPin);

   // Print initialization message
   Serial.println("Place an RFID card near the reader or enter passcode via Bluetooth...");
   bluetooth.println("Enter passcode:");
   digitalWrite(buzzerPin, HIGH);  // Initially, buzzer is off
}

void loop() {
   // Check for Bluetooth data
   if (bluetooth.available()) {
       handleBluetooth();
   }

   // Check for RFID card presence and read it
   if (rfid.PICC_IsNewCardPresent() && rfid.PICC_ReadCardSerial()) {
       handleRFID();
   }
}

void handleBluetooth() {
   // Read the Bluetooth data
   String receivedData = bluetooth.readStringUntil('\n');
   receivedData.trim();  // Remove any leading/trailing whitespace

   // Debug statement: print the received data
   Serial.println("Received data from Bluetooth: " + receivedData);

   // Compare received passcode with the correct passcode
   if (receivedData == passcode) {
       // Grant access and print the message to the serial monitor
       grantAccess();
       bluetooth.println("Access granted");
   } else {
       // Deny access and print the message to the serial monitor
       denyAccess();
       bluetooth.println("Access denied");
   }
}


void handleRFID() {
   // Compare card UID with the authorized UID
   if (memcmp(rfid.uid.uidByte, authorizedUID, 4) == 0) {
       grantAccess();
       Serial.println("Access granted");
   } else {
       denyAccess();
       Serial.println("Access denied");
   }

   // Halt PICC and stop encryption
   rfid.PICC_HaltA();
   rfid.PCD_StopCrypto1();
}
```

```
void grantAccess() {
  // Activate green LED and servo motor
  digitalWrite(greenLedPin, HIGH);
  myServo.write(90);  // Open door

  // Delay to keep the door open for a while
  delay(2000);

  // Return servo to the original position and turn off green LED
  myServo.write(0);
  digitalWrite(greenLedPin,  LOW);
}

void denyAccess() {
  // Activate red LED
  digitalWrite(redLedPin, HIGH);
  digitalWrite(buzzerPin, LOW);

  // Delay to keep red LED and buzzer on
  delay(1000);

  // Turn off red LED and buzzer
  digitalWrite(redLedPin, LOW);
  digitalWrite(buzzerPin,  HIGH);
}
```

EXPLANATION :

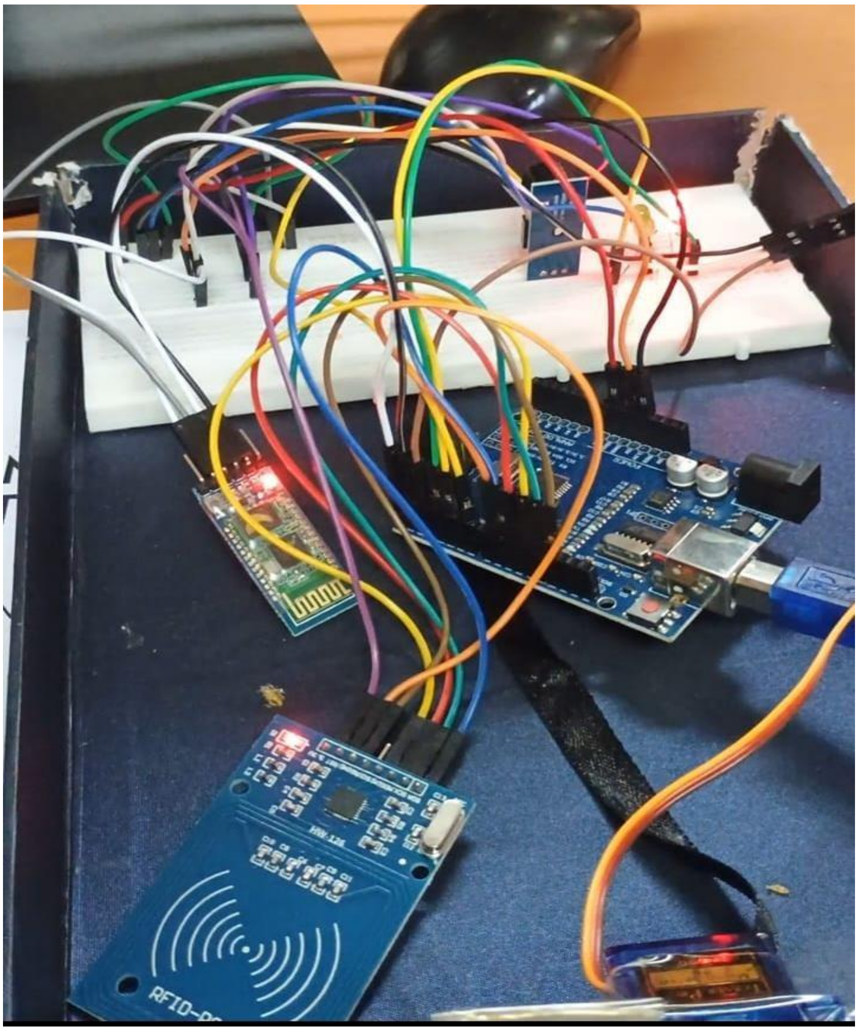
This code integrates an RFID sensor, a Bluetooth module, a servo motor, and LED indicators to create a security system. It begins by including the necessary libraries and defining the pins used for the RFID sensor, LEDs, buzzer, servo motor, and Bluetooth communication. Instances of the RFID, servo, and Bluetooth modules are created, and an authorized RFID UID and passcode are defined. In the setup function, the serial communications, SPI bus, and devices are initialized. The code prompts the user to either present an RFID card or enter the passcode via Bluetooth.

The loop function continuously checks for Bluetooth data and the presence of an RFID card. If Bluetooth data is available, the handle Bluetooth function reads the data, trims any whitespace, and compares it with the authorized passcode. If the passcode matches, access is granted; otherwise, it is denied. The access status is communicated via the Bluetooth module. Similarly, if an RFID card is detected, the handle RFID function compares the card's UID with the authorized UID. Matching the UID grants access, while a mismatch results in denial. After processing the card, the RFID reader is halted, and encryption is stopped.

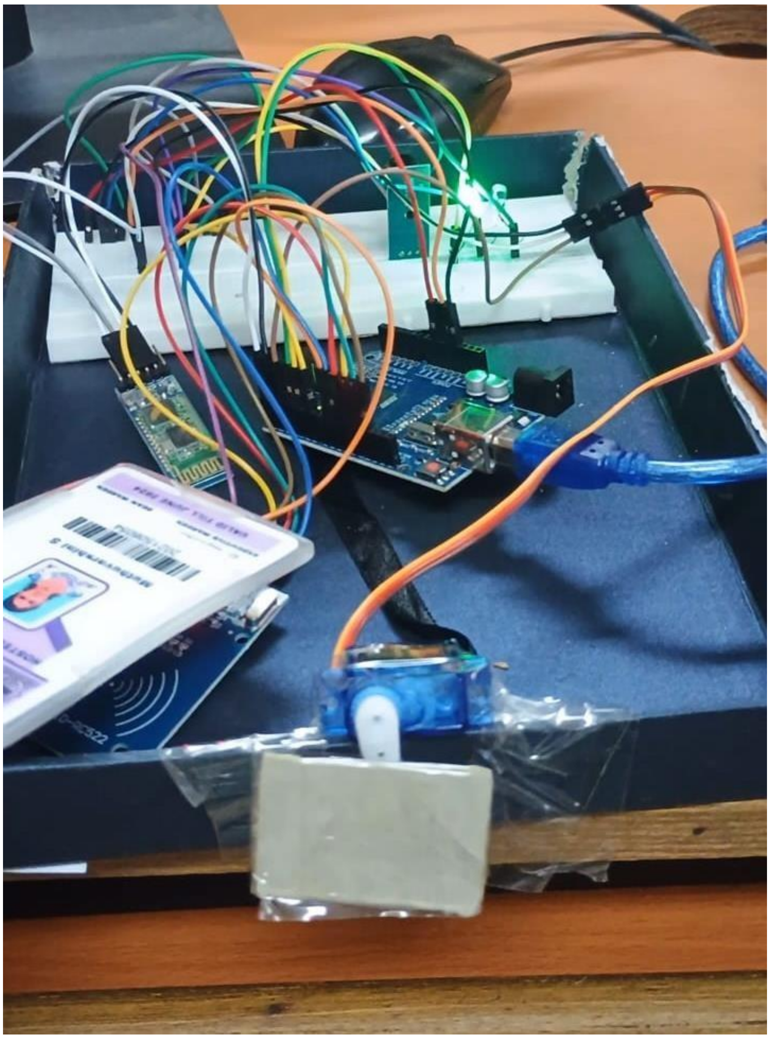
The **grant Access** and **deny Access** functions handle the actions taken upon access approval or denial. When access is granted, the green LED lights up, and the servo motor moves to open a door. The door remains open for two seconds before closing, and the green LED turns off. If access is denied, the red LED lights up, and the buzzer sounds for one second before both are turned off. This provides visual and auditory feedback to indicate whether access has been granted or denied.

OUTPUT:

1) If the red light is on, access is denied due to a wrong RFID.



2) If the green light is on, access is granted, and the door is opened.



DEMO VIDEO :

Link - https://drive.google.com/file/d/1-q7MOa9Vu-7DeVaObCG8RSVzZtpwsr2i/view?usp=drivesdk

CONCLUSION :

In conclusion, this security system effectively integrates RFID and Bluetooth technologies to control access, providing a reliable method for verifying authorized users through either an RFID card or a Bluetooth passcode. The system offers clear visual and auditory feedback using LEDs and a buzzer, and it operates a servo motor to physically grant or deny access by opening or closing a door. This ensures a secure and user-friendly experience for managing entry permissions.