UNIVERSITY OF JAFFNA, SRI LANKA

Faculty of Engineering

DOOR LOCKING SYSTEM BY DUAL AUTHENTICATING SYSTEM USING RIFC CARD AND PASSWORD

PROJECT REPORT

EC6020 EMBEDDED SYSTEMS DESIGN

BY

GROUP D6

2019/E/136: SUBASINGHE S.A.B.D.

2019/E/137: SUBASKAR S.

26 JULY 2023

01. INTRODUCTION

PROBLEM STATEMENT

In recent years, Sri Lanka has experienced an increase in theft incidents, likely due to the prevailing economic crisis. As a response to this concerning trend, we propose the implementation of an advanced security system for various types of rooms, including office rooms, storerooms, and homes. To address the growing security concerns, our project aims to develop a door security system that incorporates dual authentication using RFID technology and password protection. This two-factor authentication approach will significantly enhance the overall security and provide a robust defense against unauthorized access attempts.

Solution

The Door Locking System with dual authentication will require users to present a valid RFID card and enter a correct password on a keypad to gain access. The system ensures that only authorized individuals can enter, enhancing the overall security of the premises.

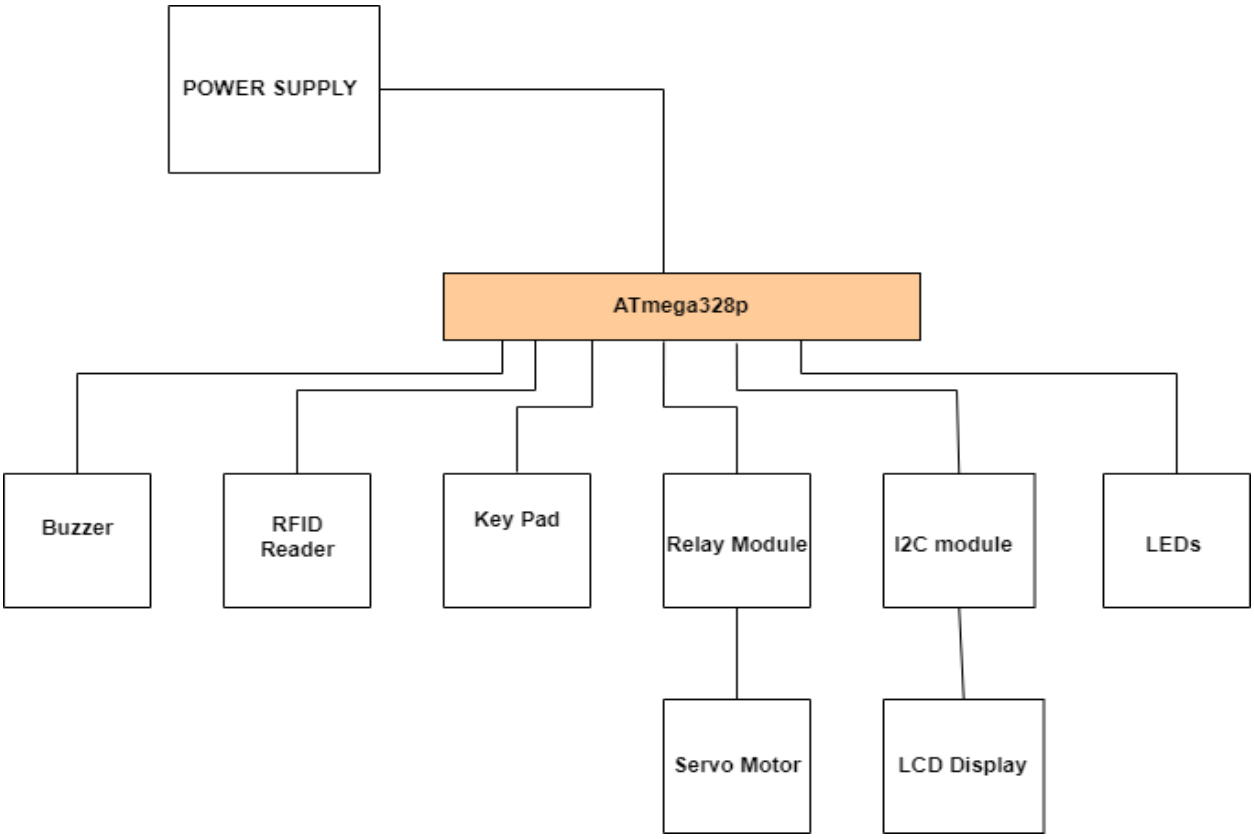
02. PROJECT DESIGN AND IMPLEMENTATION

HARDWARE DESIGN

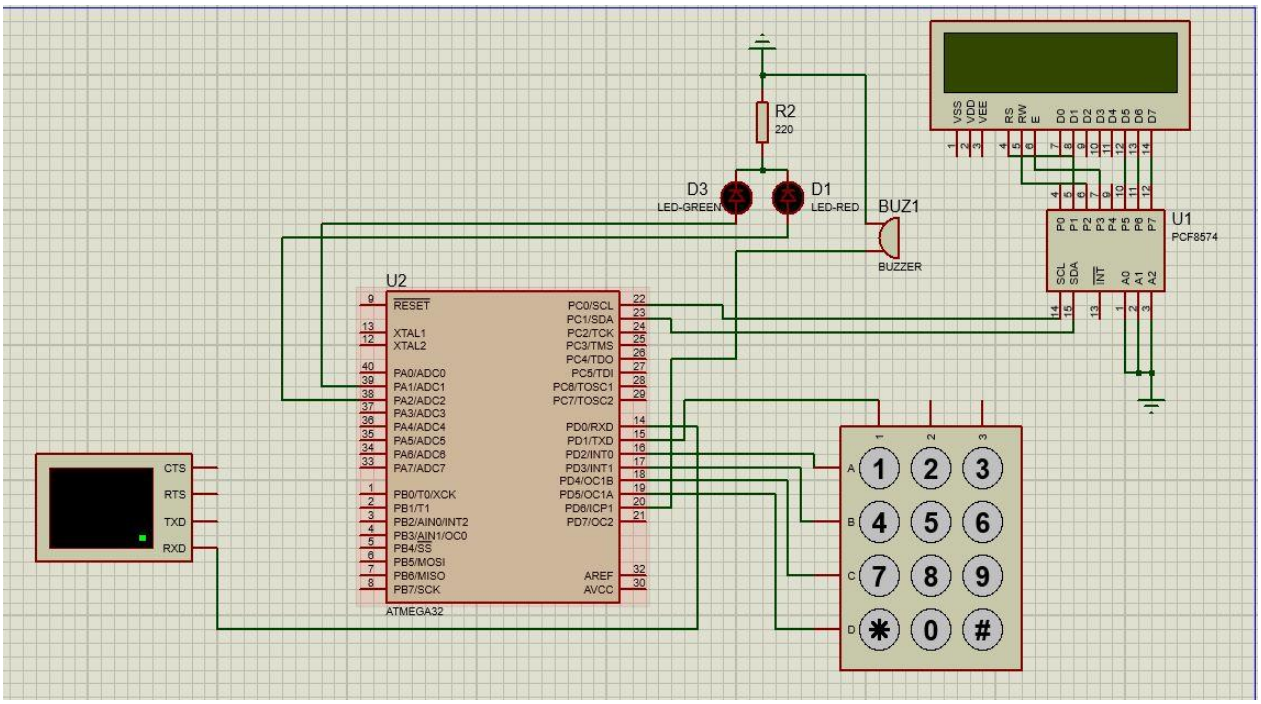
The hardware design consists of the following major components:

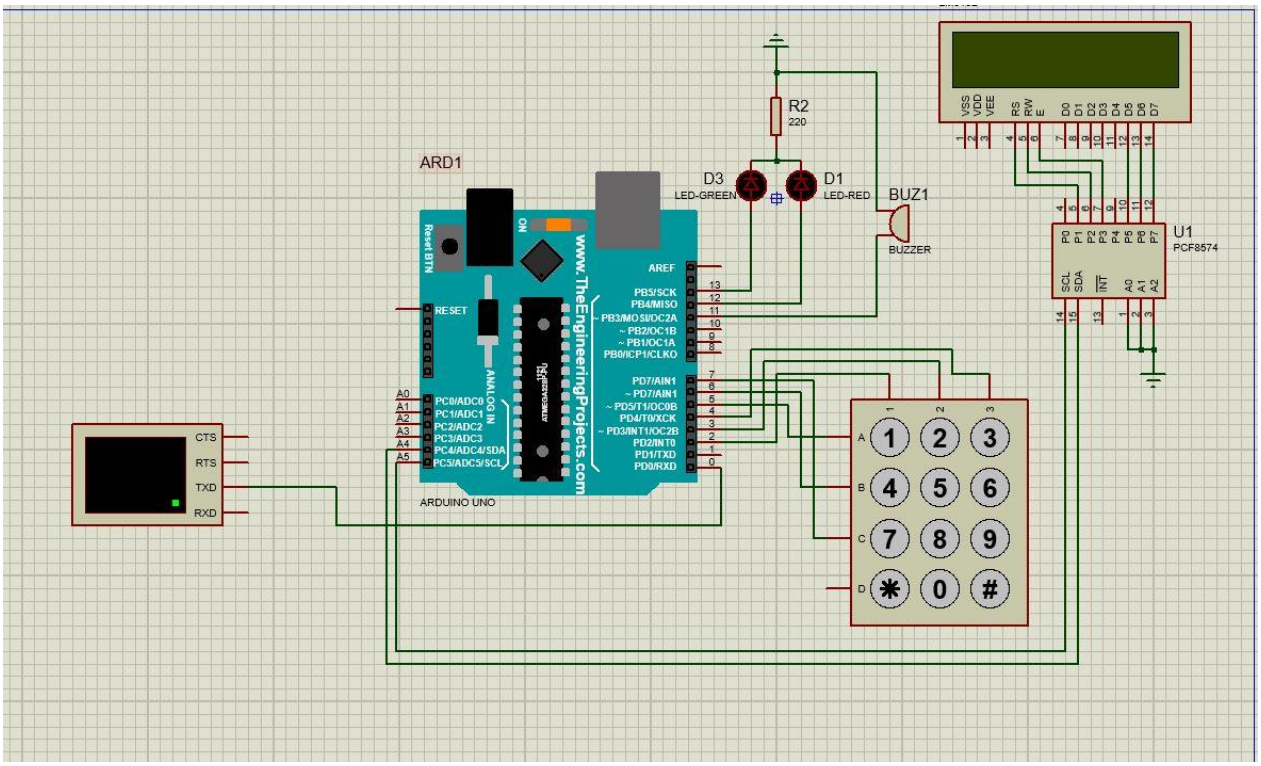
- *Arduino Uno*: The central microcontroller unit responsible for processing data and controlling other modules.
- *RFID Reader*: Interfaced with Arduino to read RFID cards for authentication.
- *Keypad*: Interfaced with Arduino to accept user passwords for authentication.
- *Servo Motor*: Used to control the physical door locking mechanism.
- *LCD Display*: Provides feedback and instructions to users during the authentication process.
- *LEDs and Buzzer*: Provide visual and auditory feedback on authentication status.

Block diagrams



Schematics

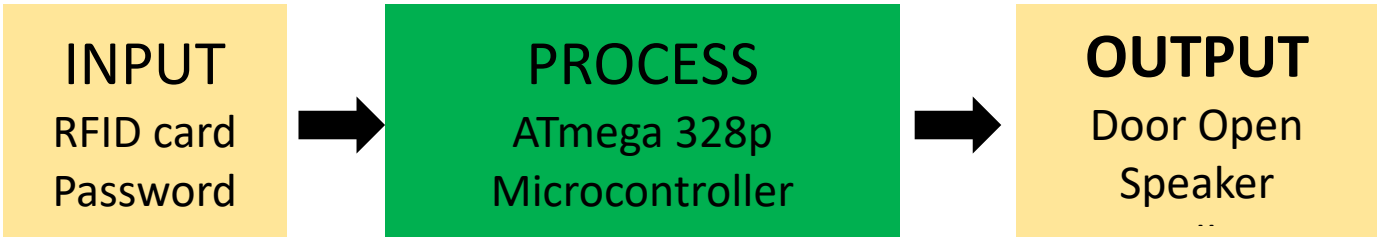


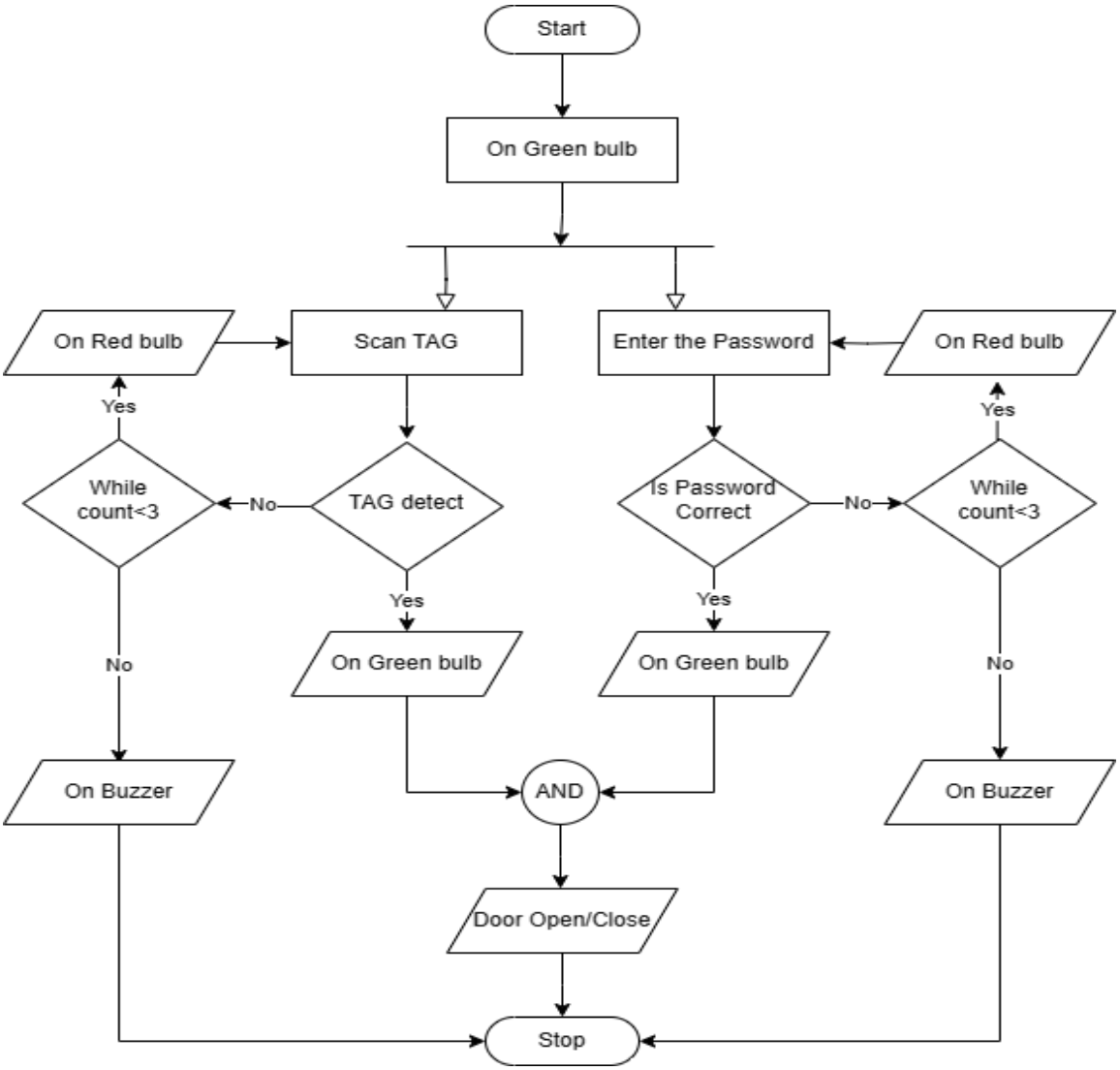


INTERFACING

- *RFID Reader*: Interfaced using SPI protocol for communication with Arduino Uno.
- *Keypad*: Interfaced using digital pins for sending/receiving data from the Arduino.
- *Servo Motor*: Interfaced using a digital pin to control the servo angle for locking/unlocking the door.
- *LCD Display*: Interfaced using I2C protocol for communication with Arduino Uno.
- *LEDs and Buzzer*: Interfaced using digital pins for visual and auditory feedback.

SOFTWARE DESIGN INCLUDING POSSIBLE DIAGRAMS





IMPLEMENTATION

- Initialize the system and peripherals during setup.
- Continuously check for RFID card presence and authenticate it using the RFID reader.
- If a valid RFID card is detected, prompt the user to enter a password using the keypad.
- Verify the entered password against the stored password for authentication.
- If both RFID and password authentication are successful, open the door using the servo motor.
- Provide appropriate feedback on the LCD display, LEDs, and buzzer for the authentication status.
- Reset the authentication status after a certain period to ensure subsequent users need to re-authenticate.

03. CHALLENGES FACED AND SOLUTIONS

CHALLENGES:

- Ensuring proper communication between the RFID reader and Arduino via SPI.
- Handling different RFID card formats and UID formats for validation.
- Managing the servo motor's position for smooth door locking/unlocking.

SOLUTIONS:

- Careful study of the RFID reader datasheet and using SPI communication routines to communicate with the reader.
- Developing a robust UID validation function to match valid RFID tags.
- Fine-tuning the servo motor control to achieve accurate door locking/unlocking.

03. TIMELINE

The project duration is estimated to be 6-7 weeks, divided into the following milestones:

TASK TO BE COMPLETED	EXPECTED TIME DURATION (WEEK)						
	9	10	11	12	13	14	15
Topic selection & Feasibility Study							
Gathering information about project							
Designing the requirement							
Writing proposal							
Buy Components							
Implement the design in breadboard							
Program the microcontroller							
Test the working condition of the design							
Implement the design in real environment							
Final presentation							

04. COMPONENTS AND COST

The following components will be required for the project:

NO	ITEM	PRICE (LKR)
01	1xATmega328P microcontroller	1400.00
02	1x16MHz Crystal Oscillator	50.00
03	1x10Kohm resistors	10.00
04	2x 22pF capacitors	20.00
05	RFID Reader Module	700.00
06	Keypad	650.00
07	Door Lock	350.00
08	LCD Display	1000.00
09	I2C module	300.00
10	Servo motor	700.00
11	3xLED Bulb (Red,Gren)	45.00
12	Resistor 270 Ohm 10pcs	220.00
13	Active buzzer 5V	290.00
14	Relay Module 5V-1-channel	300.00
15	Power supply module 5V	800.00
16	Bread board 400 tie points 8.5x5.5cm	300.00
17	Jumper wires 20CM female to female 40pcs	300.00
18	Jumper wires 20CM male to male 40pcs	300.00
TOTAL		**7,735.00**

05. REFLECTION ON APPLIED KNOWLEDGE FROM THINGS LEARNED IN THE COURSE

Throughout the embedded system course, we learned various concepts and techniques, including microcontroller programming, interfacing, and hardware design. This project allowed us to apply our knowledge practically, integrating multiple hardware components and developing a functional door locking system with dual authentication.

The project provided hands-on experience in solving real-world problems, understanding datasheets, debugging, and system integration. Moreover, it strengthened our understanding of microcontrollers, sensors, and actuators, helping us gain valuable skills for future embedded system projects.

06. CONCLUSION

The Door Locking System with Dual Authentication using RFID cards and Passwords is a secure and efficient solution to enhance access control. The integration of RFID and keypad authentication provides an additional layer of security, making unauthorized access significantly difficult.

This project demonstrates the successful implementation of embedded system principles to create a functional, real-world application that can be further improved and customized for specific security requirements.

07. REFERENCES

[1] Ni Ni San Hlaing | San San Lwin "Electronic Door Lock using RFID and Password Based on Arduino" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-3, April 2019, pp.799-802, URL: https://www.ijtsrd.com/papers/ijtsrd22875.pdf

[2] Kumar Chaturvedula .U.P, “RFID Based Embedded System for Vehicle Tracking and Prevention of Road Accidents”, International Journal of Engineering Research & Technology (IJERT) , Vol. 1 Issue 6, August – 2012, ISSN: 2278-0181

[3] Parvathy A, Venkata Rohit Raj, Venumadhav, Manikanta, “RFID Based Exam Hall Maintenance System’’, IJCA Special Issue on “Artificial Intelligence Techniques - Novel Approaches & Practical Applications” AIT, 2011

[4] Orji, E. Z., U. I. Nduanya, and C. V. Oleka. "Microcontroller Based Digital Door Lock Security System Using Keypad." International Journal of Latest Technology in Engineering, Management & Applied Science 8.1 (2019): 92-97.

08. APPENDIX

AVR c code

File Edit Selection Find View Goto Tools Project Preferences Help

final.c

```c
#include <avr/io.h>
#include <util/delay.h>
#include <avr/interrupt.h>
#include <stdbool.h>
#include <string.h>

#define F_CPU 16000000UL
#define BAUD_RATE 9600
#define UBRR_VALUE ((F_CPU / (BAUD_RATE * 16UL)) - 1)

// Function prototypes
void USART_Init(unsigned int ubrr);
void USART_Transmit(unsigned char data);
unsigned char USART_Receive(void);
void printString(const char* str);
void printNumber(uint16_t num);
bool validateRFIDTag(const char* ID);
void openCloseDoor(void);
bool checkRFIDAuthentication(void);
bool checkPasswordAuthentication(void);
void resetAuthentication(void);

// Global variables
char receivedData;
volatile bool isRFIDAuthenticated = false;
volatile bool isPasswordAuthenticated = false;

// Define your RFID tags' UIDs here
const char validRFIDTags[3][16] = {
    "73 46 FA 1A",
    "68 46 FA 1A",
    "89 3C 2C C2"
};

const char storedPassword[] = "123#";

int main(void) {
    // Initialization code for UART and other hardware
    USART_Init(UBRR_VALUE);
    while (1) {
        // Check for RFID authentication
```

File Edit Selection Find View Goto Tools Project Preferences Help

final.c

```c
int main(void) {
    // Initialization code for UART and other hardware
    USART_Init(UBRR_VALUE);
    while (1) {
        // Check for RFID authentication
        if (!isRFIDAuthenticated) {
            isRFIDAuthenticated = checkRFIDAuthentication();
        }

        // Check for password authentication
        if (!isPasswordAuthenticated && isRFIDAuthenticated) {
            isPasswordAuthenticated = checkPasswordAuthentication();
        }

        // Handle door lock based on authentication status
        if (isRFIDAuthenticated && isPasswordAuthenticated) {
            openCloseDoor();
            _delay_ms(5000);  // Allow 5 seconds for door to be opened
            resetAuthentication();
        }
    }
    return 0;
}

void USART_Init(unsigned int ubrr) {
    UBRR0H = (unsigned char)(ubrr >> 8);
    UBRR0L = (unsigned char)ubrr;
    UCSR0B = (1 << TXEN0) | (1 << RXEN0);
    UCSR0C = (1 << UCSZ01) | (1 << UCSZ00);
}

void USART_Transmit(unsigned char data) {
    while (!(UCSR0A & (1 << UDRE0)));
    UDR0 = data;
}

unsigned char USART_Receive(void) {
    while (!(UCSR0A & (1 << RXC0)));
    return UDR0;
}

void printString(const char* str) {
```

Line 28, Column 36

File Edit Selection Find View Goto Tools Project Preferences Help

final.c

```
    return UDR0;
}

void printString(const char* str) {
    for (uint16_t i = 0; i < strlen(str); i++) {
        USART_Transmit(str[i]);
    }
}

void printNumber(uint16_t num) {
    char buffer[6];
    sprintf(buffer, "%u", num);
    printString(buffer);
}

bool validateRFIDTag(const char* ID) {
    for (uint8_t i = 0; i < 3; i++) {
        if (strcmp(ID, validRFIDTags[i]) == 0) {
            return true;
        }
    }
    return false;
}

void resetAuthentication(void) {
    isRFIDAuthenticated = false;
    isPasswordAuthenticated = false;
}
```

Arduino code

```
#include <LiquidCrystal_I2C.h>
#include <SPI.h>
#include <MFRC522.h>
#include <Keypad.h>
#include <Servo.h>
// RFID
#define SS_PIN 10  // Slave Select Pin for RFID module
#define RST_PIN 9  // Reset Pin for RFID module
#define buzzer 5
#define servoPin A0
#define led_Green A1
#define led_Red A2
```

```
MFRC522 rfid(SS_PIN, RST_PIN);  // Create MFRC522 instance
Servo servo;
LiquidCrystal_I2C lcd(0x27, 16, 2);  // Set the LCD I2C address and dimensions

int lockPos = -90;               //Locked position limit
int unlockPos = 00;             //Unlocked position limit
int pos = 0;
boolean locked = true;

// Keypad
const byte ROWS = 1; // Number of rows in the keypad
const byte COLS = 4; // Number of columns in the keypad
char keys[ROWS][COLS] = {
  {'1','2','3','#'}
  };
// byte rowPins[ROWS] = {5, 4, 3, 2};   // Connect keypad row pins to these
Arduino pins
// byte colPins[COLS] = {8, 7, 6};    // Connect keypad column pins to these
Arduino pins
byte rowPins[ROWS] = {2}; //connect to the row pinouts of the keypad
byte colPins[COLS] = {8, 7, 6, 3}; //connect to the column pinouts of the keypad
Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS, COLS);

// Password
const String storedPassword = "123#";  // Stored password for authentication
int nkey = 0;
byte lock = 0;
// Door Lock
//const int lockPin = 3;  // Digital pin to control the door lock

// State variables
//bool isLocked = true;  // Current lock state
bool isRFIDAuthenticated = false;  // RFID authentication status
bool isPasswordAuthenticated = false;  // Password authentication status

int letterDelay = 150;
String msg1 = "DOOR LOCK";
String msg2 = "SECURITY SYSTEM";


void setup() {

  Serial.begin(9600);
  SPI.begin();        // Initialize SPI bus
```

```
  rfid.PCD_Init(); // Initialize MFRC522 RFID module
  lcd.init();  // Initialize LCD display
  lcd.backlight();
  servo.attach(servoPin);
  servo.write(0);
  //pinMode(lockPin, OUTPUT);  // Set door lock pin as OUTPUT
  pinMode(0,OUTPUT);
  digitalWrite(0,LOW);
  pinMode(buzzer, OUTPUT);
  pinMode(led_Green, OUTPUT);
  digitalWrite(led_Green, LOW);
  pinMode(led_Red, OUTPUT);

  lcd.setCursor(3, 0);
  for(int i = 0; i < msg1.length() ; i++){
    lcd.setCursor(i+3, 0);
    lcd.print(msg1.charAt(i));
    delay(letterDelay);
  }
  for(int i = 0; i < msg2.length() ; i++){
    lcd.setCursor(i, 1);
    lcd.print(msg2.charAt(i));
    delay(letterDelay);
  }
  delay(2000);
  lcd.clear();

  lcd.clear();
  lcd.print(" Access Control ");
  delay(1000);
  lcd.setCursor(0, 1);
  lcd.print("Scan Your Card>>");
  Serial.print("NOW IN LOOP");
}

void loop()
{

  // Check for RFID authentication
  if (!isRFIDAuthenticated) {
    isRFIDAuthenticated = checkRFIDAuthentication();  //(1/0)
  }
```

```
  // Check for password authentication
  if (isPasswordAuthenticated == false && isRFIDAuthenticated == true) {
    isPasswordAuthenticated = checkPasswordAuthentication();
  }

  // Handle door lock based on authentication status

  if ((isRFIDAuthenticated == true) && (isPasswordAuthenticated == true)) {
    openCloseDoor();
    delay(5000);  // Allow 5 seconds for door to be opened
    //lockDoor();
    resetAuthentication();
  }
}
/////
bool checkRFIDAuthentication(){
  if (rfid.PICC_IsNewCardPresent() && rfid.PICC_ReadCardSerial())
  {

    //Show UID on serial monitor
    Serial.print("UID tag: ");
    lcd.clear();
    lcd.setCursor(0,0);
    lcd.print("Scanning");
    delay(2000);
    String ID = "";
    byte letter;
    for (byte i = 0; i < rfid.uid.size; i++)
    {
      Serial.print(rfid.uid.uidByte[i] < 0x10 ? " 0" : " ");
      Serial.print(rfid.uid.uidByte[i], HEX);
      ID.concat(String(rfid.uid.uidByte[i] < 0x10 ? " 0" : " "));
      ID.concat(String(rfid.uid.uidByte[i], HEX));
    }
    Serial.println();
    Serial.print("Message: ");

    ID.toUpperCase();
    lcd.setCursor(0,1);
    lcd.print("Tag:"+ID);
    delay(2000);

    if (validateRFIDTag(ID))
    {
```

```
      lcd.clear();
      lcd.print("Card Accepted !");
      delay(500);

      digitalWrite(led_Green, HIGH);
      tone(buzzer, 500);
      delay(1000);
      noTone(buzzer);
      digitalWrite(led_Green, LOW);
      lcd.clear();
      lcd.print(" Enter the ");
      lcd.setCursor(0,1);
      lcd.print("Password>>");
      delay(2000);
      return true;

    }else
    {
      lcd.clear();
      lcd.print("Access denied");
      delay(500);
      digitalWrite(led_Red, HIGH);
      tone(buzzer, 300);
      delay(2000);
      digitalWrite(led_Red, LOW);
      noTone(buzzer);
      delay(2000);
      lcd.clear();
      lcd.print(" Access Control ");
      delay(1000);
      lcd.setCursor(0, 1);
      lcd.print("Scan Your Card>>");
      return false;
    }

  }

  return false;
}


//defince RFID tags
bool validateRFIDTag(String ID) {
    if (ID.substring(1) == "73 46 FA 1A")
```

```
    {
      return true;
    }
    if (ID.substring(1) == "68 46 FA 1A")
    {
      return true;
    }
    if (ID.substring(1) == "89 3C 2C C2")
    {
      return true;
    }
    return false;
}


bool checkPasswordAuthentication() {
  // lcd.clear();
  String enteredPassword = "";
  char key = keypad.getKey();

  if (key) {
    lcd.clear();
    lcd.print(key);
    enteredPassword += key;
    delay(100);

    while (key != '#' && enteredPassword.length() <= 3) {
      key = keypad.getKey();
      if (key) {
        lcd.print(key);
        Serial.print("\n");
        enteredPassword += key;
         Serial.print(enteredPassword);
        delay(100);
      }
    }
    Serial.print("\n");
    Serial.print(enteredPassword);
    if(enteredPassword == storedPassword) {
    lcd.clear();
    lcd.print("Password Correct");
    delay(1000);
    digitalWrite(led_Green, HIGH);
    tone(buzzer, 500);
```

```
    delay(2000);
    noTone(buzzer);
    digitalWrite(led_Green, LOW);
    return true;
  }
  else{
    lcd.clear();
    lcd.print("Password Wrong");
    delay(2000);
    lcd.clear();
    lcd.print("Access denied");
    digitalWrite(led_Red, HIGH);
    tone(buzzer, 300);
    delay(2000);
    digitalWrite(led_Red, LOW);
    noTone(buzzer);
    delay(3000);
    lcd.clear();
    lcd.print(" Access Control ");
    delay(1000);
    lcd.setCursor(0, 1);
    lcd.print("Scan Your Card>>");
    isRFIDAuthenticated = false;
    return false;
  }
  }


  return false;
}

void openCloseDoor(){
  if (locked == true)
  {  // If the lock is closed, open it
    for (pos = lockPos; pos <= unlockPos; pos += 1)
    {
      servo.write(pos);
      delay(15);
      locked = false;
    }
    lcd.clear();
    lcd.print("Welcome");
    delay(1000);
    lcd.print("!");
```

```
    delay(1000);
    lcd.print("!");
    delay(1000);
    lcd.print("!");
    lcd.setCursor(0,1);
    lcd.print("DOOR OPENED");


  }else
  {
    for (pos = unlockPos; pos >= lockPos; pos -= 1)
    {

      servo.write(pos);
      delay(15);
      locked = true;
    }
    lcd.clear();
    lcd.print("DOOR CLOSED");
    delay(30000);
    lcd.print(" Access Control ");
    delay(1000);
    lcd.setCursor(0, 1);
    lcd.print("Scan Your Card>>");
  }
}

void resetAuthentication() {
  isRFIDAuthenticated = false;
  isPasswordAuthenticated = false;
  //lcd.clear();
  //lcd.print("Welcome!");
}
```

Minimized version of the poster