PROJECT: RFID-Based Solenoid Lock System Using Arduino

---

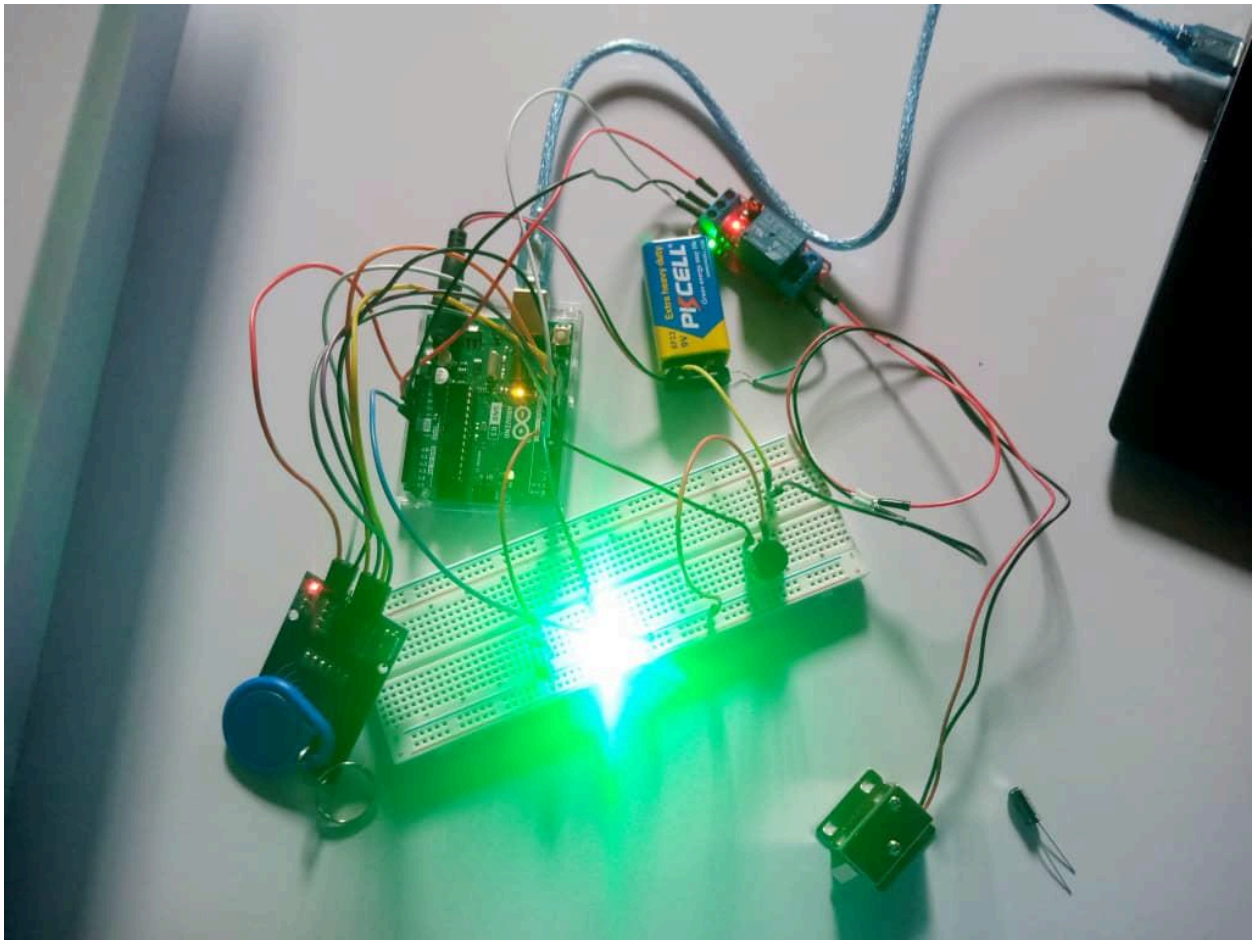
1. Introduction

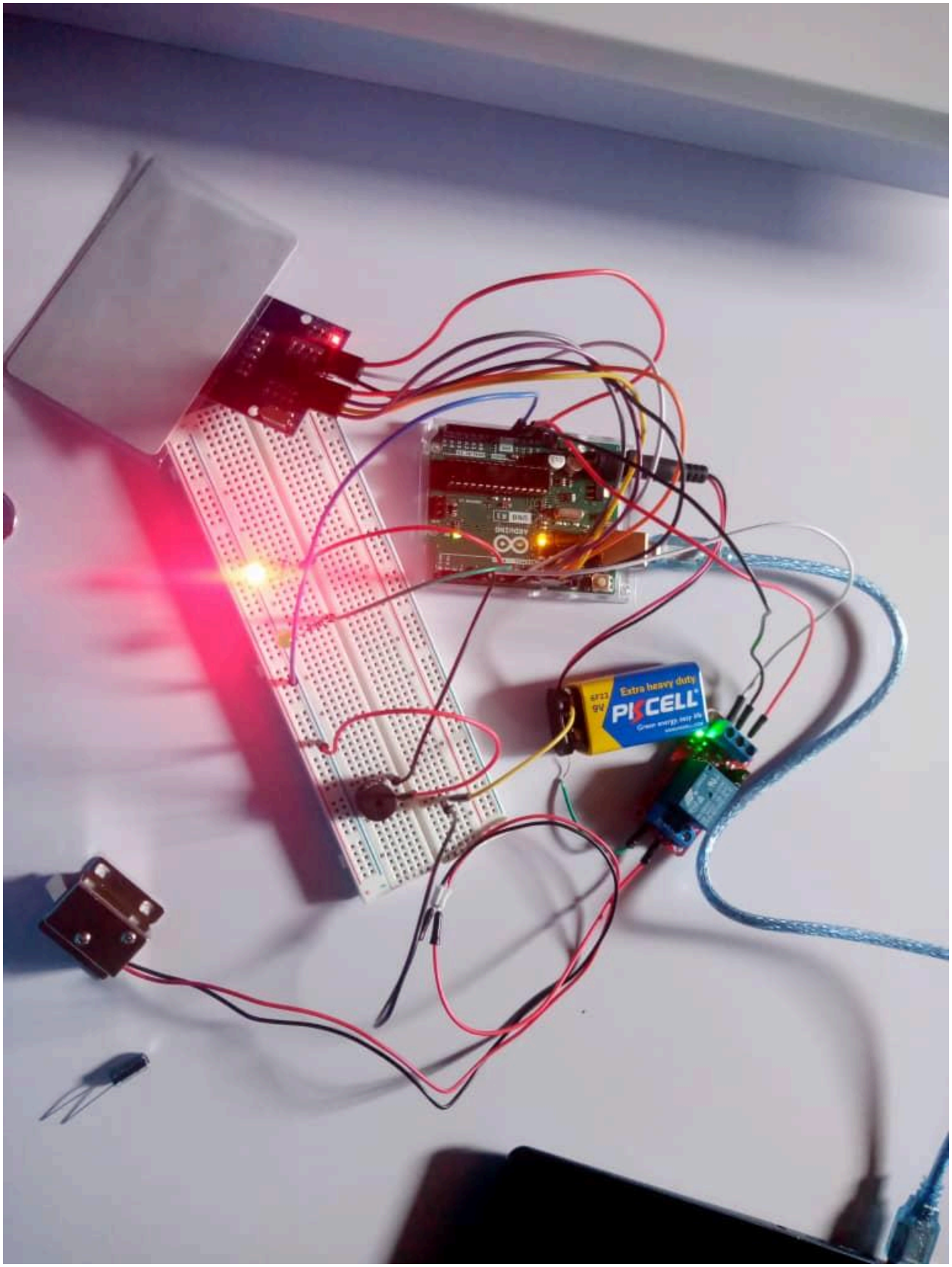
This project focuses on creating a security system using an RFID (Radio Frequency Identification) module and a solenoid lock controlled by an Arduino Uno. The RFID system provides an efficient way to grant or deny access based on card authorization. The project integrates various components such as relays, LEDs, buzzers, and solenoid locks to offer a practical solution for secure access control.

2. Materials Used

- **Arduino Uno**: The microcontroller used to control the entire system.
- **Relay Module**: Acts as a switch to control the solenoid lock.
- **Wires**: Used for connections between components.
- **Solenoid Lock**: An electronic lock controlled by the Arduino to secure access.
- **DC Voltage Source**: Provides power to the solenoid lock and other components.
- **PC**: Used to upload the code to the Arduino Uno.
- **RFID Module (MFRC522)**: Reads the RFID cards to check for authorized access.
- **RFID Card/Tag**: Used for authorization to unlock the solenoid lock.
- **Buzzer**: Provides auditory feedback for access granted or denied.
- **LEDs (Green and Red)**: Indicate the status of access (authorized or denied).

3. Circuit Diagram


PICELL


Extra heavy duty
PKCELL

4. Code Explanation

The code provided below is responsible for controlling the RFID-based solenoid lock system. The Arduino reads the RFID tag, compares it with a predefined authorized UID, and takes action based on whether the UID matches or not.

```
#include <SPI.h>
#include <MFRC522.h>

#define SS_PIN 10
#define RST_PIN 9
#define LED_G 7 // define green LED pin
#define LED_R 6 // define red LED
#define RELAY 5 // relay pin
#define BUZZER 2 // buzzer pin
#define ACCESS_DELAY 2000
#define DENIED_DELAY 1000

MFRC522 mfrc522(SS_PIN, RST_PIN); // Create MFRC522 instance.

void setup()
{
  Serial.begin(9600);   // Initiate a serial communication
  SPI.begin();          // Initiate SPI bus
  mfrc522.PCD_Init();   // Initiate MFRC522
  pinMode(LED_G, OUTPUT);
  pinMode(LED_R, OUTPUT);
  pinMode(RELAY, OUTPUT);
  pinMode(BUZZER, OUTPUT);
  noTone(BUZZER);
  digitalWrite(RELAY, LOW);
  Serial.println("Put your card to the reader...");
  Serial.println();
}
```

```
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) == "63 10 A8 E4") // change here the UID of
the card/cards that you want to give access
  {
    Serial.println("Authorized access");
    Serial.println();
    delay(500);
    digitalWrite(RELAY, HIGH);
    digitalWrite(LED_G, HIGH);
```

```
    delay(ACCESS_DELAY);
    digitalWrite(RELAY, LOW);
    digitalWrite(LED_G, LOW);
  }
  else
  {
    Serial.println("Access denied");
    digitalWrite(LED_R, HIGH);
    tone(BUZZER, 300);
    delay(DENIED_DELAY);
    digitalWrite(LED_R, LOW);
    noTone(BUZZER);
  }
}
```

5. How It Works

System Workflow Development

1. Initialization

During the initialization phase, the Arduino Uno sets up the necessary configurations for the various hardware components in the system. Here's a breakdown of what happens:

- **RFID Module Setup**: The RFID module (MFRC522) is initialized to start communicating with the Arduino via the SPI bus. This involves activating the chip select (SS) and reset (RST) pins, ensuring the RFID reader is ready to detect cards.
- **Pin Modes Configuration**: The Arduino configures the pins connected to the LEDs, relay, and buzzer as outputs. This allows the Arduino to control these components by sending high or low signals to the respective pins.
    - **Green LED (LED_G)**: Indicates successful authorization.
    - **Red LED (LED_R)**: Indicates failed authorization.
    - **Relay**: Controls the solenoid lock, enabling or disabling the lock mechanism.
    - **Buzzer**: Provides auditory feedback when access is denied.
- **Serial Communication**: The Arduino starts serial communication at a baud rate of 9600. This allows monitoring of the system's status through the serial monitor, providing real-time feedback on card detection and access decisions.

The system also outputs a message on the serial monitor indicating that it's ready for card scanning.

2. Card Detection

Once the initialization is complete, the system enters a continuous loop where it monitors for the presence of an RFID card. The RFID reader checks for a new card using the following steps:

- **Checking for Card Presence**: The RFID module checks if a card is near the reader. If no card is detected, the system continues to loop without taking any action.
- **Card Selection**: If a card is detected, the system attempts to read its data. This involves retrieving the card's unique identifier (UID), which is then processed by the Arduino.

3. UID Verification

After detecting and selecting a card, the system performs the following steps:

- **UID Retrieval**: The Arduino reads the UID of the card and displays it on the serial monitor for verification purposes.
- **UID Comparison**: The system converts the UID to a string and compares it with a predefined authorized UID stored in the code. This predefined UID represents the card(s) that are allowed to unlock the solenoid lock.
    - **Authorized UID**: If the UID of the card matches the authorized UID, the system proceeds to grant access.
    - **Unauthorized UID**: If the UID does not match, the system denies access.

4. Access Control

Based on the result of the UID verification, the system controls the solenoid lock and the LEDs:

- **Authorized Access**:
    - **Relay Activation**: The relay is activated, which in turn powers the solenoid lock, unlocking it. The green LED is also turned on to indicate successful authorization.
    - **Access Delay**: The relay and green LED remain active for a specified period (2 seconds in this case), allowing time for the door to be opened.
    - **Reset**: After the delay, the relay is deactivated, and the solenoid lock returns to its locked state. The green LED is also turned off.
- **Denied Access**:
    - **Red LED and Buzzer Activation**: If the card is unauthorized, the red LED lights up, and the buzzer sounds to indicate that access has been denied.
    - **Denied Delay**: The red LED and buzzer remain active for a short period (1 second) before being turned off, signaling the end of the denial response.

The system then loops back to the card detection phase, ready to process the next card. This continuous cycle ensures the system remains responsive and secure, providing real-time access control based on the presence and verification of RFID cards.

6. Practical Applications

potential applications for the RFID-based solenoid lock system:

1. Securing Doors in Residential and Commercial Buildings

- **Home Security**: Use the system to secure entry points like front doors, garages, and gates in residential settings.
- **Office Buildings**: Control access to offices, meeting rooms, and storage areas in commercial spaces.

2. Controlling Access to Restricted Areas

- **Server Rooms**: Protect sensitive IT infrastructure by limiting access to server rooms.
- **Laboratories**: Secure laboratories where hazardous materials or confidential research is conducted.
- **Data Centers**: Restrict entry to data centers to authorized personnel only.

3. Integrating with Other Security Systems

- **Alarm Systems**: Pair the RFID lock with an alarm system to trigger alerts if unauthorized access is attempted.
- **Surveillance Systems**: Integrate with CCTV cameras to monitor access points in real-time.

4. Educational Institutions

- **Classrooms and Labs**: Secure classrooms, labs, and administrative offices to ensure only authorized students and staff can enter.
- **Dormitories**: Control access to student dormitories for enhanced security.

5. Healthcare Facilities

- **Medicine Cabinets**: Secure medicine cabinets and storage rooms where controlled substances are kept.
- **Patient Rooms**: Restrict access to certain patient rooms or medical records areas.

6. Parking Facilities

- **Vehicle Access Control**: Use the system to control access to parking garages or lots, allowing only vehicles with RFID tags to enter.
- **Gated Communities**: Secure the entry points of gated communities by issuing RFID cards to residents and approved visitors.

7. Industrial and Manufacturing Sites

- **Machinery Access**: Limit access to heavy machinery or equipment to trained personnel only.
- **Warehouse Security**: Secure warehouses to prevent unauthorized access to inventory and supplies.

8. Hospitality Industry

- **Hotel Rooms**: Replace traditional key cards with RFID-based locks for hotel rooms.
- **VIP Areas**: Control access to VIP lounges, conference rooms, or exclusive events within hotels or resorts.

9. Retail Security

- **Stock Rooms**: Secure stock rooms and storage areas to prevent theft or unauthorized access by employees.
- **Point-of-Sale Systems**: Integrate the RFID lock with POS systems to restrict access to cash drawers or safe rooms.

10. Transportation Hubs

- **Airport Security**: Control access to secure areas within airports, such as baggage handling areas or restricted terminals.
- **Public Transit Stations**: Secure staff-only areas within bus or train stations, limiting access to authorized personnel.

11. Event Management

- **Concerts and Festivals**: Use RFID wristbands or cards to control access to different areas within an event venue, such as backstage or VIP sections.
- **Conference Rooms**: Secure conference rooms or exhibition areas during large-scale events or trade shows.

12. Banking and Finance

- **Vault Security**: Use RFID locks to control access to bank vaults and safe deposit boxes.
- **ATM Maintenance**: Restrict access to ATMs for maintenance and restocking by authorized personnel only.

13. Government and Military

- **Sensitive Documents**: Secure areas where classified or sensitive documents are stored.

- **Military Bases**: Control access to various facilities within a military base, ensuring only authorized personnel can enter.

14. Libraries and Archives

- **Rare Collections**: Protect rare books, documents, or artifacts in libraries and archives from unauthorized access.
- **Private Study Rooms**: Secure private study rooms or research areas in academic institutions.

15. Sports and Recreation Facilities

- **Gym Membership**: Use RFID cards as gym memberships to control access to fitness facilities.
- **Locker Rooms**: Secure locker rooms and equipment storage areas in sports facilities or recreational centers.

7. Conclusion

This project demonstrates the practical use of an RFID system for access control. By using an Arduino Uno, RFID reader, and solenoid lock, a secure and efficient locking mechanism can be implemented. This project can be expanded further by integrating a database for storing multiple authorized UIDs or adding a display for user feedback.

8. References

- Viral Science https://www.youtube.com/watch?v=RtxIklx94L8