VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

WINTER SEMESTER 2024-25

Course Code : BECE204L
Course Name : Microcontrollers and Microprocessors.

PROJECT REPORT

DUAL AUTHENTICATION DOOR LOCK MECHANISM

Submitted By :

Ishita Mohanta (23BML0086), Ramani Srinivasan (23BML0008),
Harshitha N (23BML0091), Tarun Eashwar (23BML0094)

SLOT : D1/TD1

Faculty Incharge : Dr. Ragunath G.

ABSTRACT :

This project presents a smart, dual-authentication door lock system that integrates RFID technology, a 4x3 keypads, and an IR sensor for secure access and real-time occupancy tracking. An Arduino Uno serves as the central controller, interfacing with the MFRC522 RFID reader, keypad, servo motor, and LCD display. Users can authenticate using either an RFID tag or a password, providing flexibility and enhanced security. The IR sensor tracks entry and updates a live people count displayed on the LCD. Designed for secure environments like offices or labs, the system ensures reliable access control, unauthorized entry prevention, and improved space monitoring.

LITERATURE REVIEW :

Patents :

Patent Application Number	Patent Title	Country	Description
ES2555675A1	Electronic lock (Machine-translation by Google Translate, not legally binding)	Spain	This patent describes an advanced electronic door lock system with multiple security features. It includes a keypad, electronic circuit, and a locking mechanism controlled by entering a pre-set code. The system has sliding tumblers for automatic door closure and several security bolts for strong locking. It also includes a traditional key-operated cylinder for emergencies. Turning the key anti-clockwise unlocks the door, while turning it clockwise disconnects the inner control. The design allows keyless use and enables locking the inside of the door from outside, adding both convenience and enhanced safety.
Paper Details			
https://patents.google.com/patent/ES2025908A6/en?q=(keypad+based+door+lock+system)&oq=keypad+based+door+lock+system			

Patent Application Number	Patent Title	Country	Description
US4148092A	Electronic combination door lock with deadbolt	United States	This patent describes a door lock system that uses an electronic keypad and magnetic card reader to send coded signals to a central

	sensing means		processor. The processor controls a solenoid latch near the locking bolt. When activated by a valid signal (or an auxiliary switch), the solenoid allows the bolt to move from locked to unlocked. If no valid signal is received, the latch prevents the bolt from moving. This system adds electronic control to enhance security and access flexibility.
Paper Details			
https://patents.google.com/patent/US5775142A/en			

Patent Application Number	Patent Title	Country	Description
CA2929266A1	Systems and methods for authorizing access to a locked enclosure	Canada	This patent describes a battery-less RFID electronic lock system that doesn't need an internal power source. It uses a smart RFID tag and a microcontroller circuit attached to an electric or electromagnetic lock. The system is powered by electromagnetic waves from an RFID reader or smartphone. This energy-harvesting method eliminates the need for batteries. It's suitable for various uses, such as doors, luggage, furniture, and other security applications. The design is efficient, low-maintenance, and eco-friendly.
Paper Details			
https://patents.google.com/patent/CA2929266A1/en			

Patent Application Number	Patent Title	Country	Description
US20090256676A1	Smart-lock system	United States	This patent describes an electronic access control system that includes a lock, card reader, key card, database, and an administrator microprocessor. The lock or key card contains a microprocessor and encrypted memory. The key card allows access and transfers encrypted data between the lock and database through the card reader and administrator unit. The administrator microprocessor manages user access, reviews data, and verifies users with accounts and passwords. This system ensures secure access and keeps a record of activity through encrypted communication.
Paper Details			
https://patents.google.com/patent/US20090256676A1/en			

Patent Application Number	Patent Title	Country	Description
N.A	RFID Door Lock	United States	This patent outlines a simple and user-friendly RFID door lock system. It includes a compact RFID reader/writer, a magnetic door lock, and an LED to indicate lock status. Users only need an RFID tag to lock or unlock the door. The system is easy to install without modifying the door or frame, and it works alongside traditional locks if preferred. It's designed to be a cost-effective and convenient security upgrade for everyday users.
Paper Details			
https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1267&context=eesp			

Reviews :

1. https://ieeexplore.ieee.org/abstract/document/8807588
   This paper presents a dual-security access control system using both a password and RFID technology. The system is designed to allow only authorized users to unlock it by first scanning an RFID tag and then entering a correct password. It uses a passive RFID reader and a keypad, controlled by an Atmega16 microcontroller. If both the RFID tag ID and password match, the lock will open. The goal is to build a reliable and low-cost locker security system that is also error-free.

2. https://ieeexplore.ieee.org/abstract/document/10010367
   This paper introduces a home security system using a solenoid door lock controlled by biometric fingerprint, RFID, and keypad authentication. An Arduino Uno manages the system, unlocking the door only after successful verification. The fingerprint sensor scans in about 3.7 seconds, RFID reads E-KTP cards in 2.4 seconds, and the keypad takes around 3.7 seconds. When all three are used together, it takes about 9.8 seconds to unlock the door. While the system enhances security and prevents duplication, it lacks remote monitoring features like SMS or app notifications, which could help homeowners track access in real time.

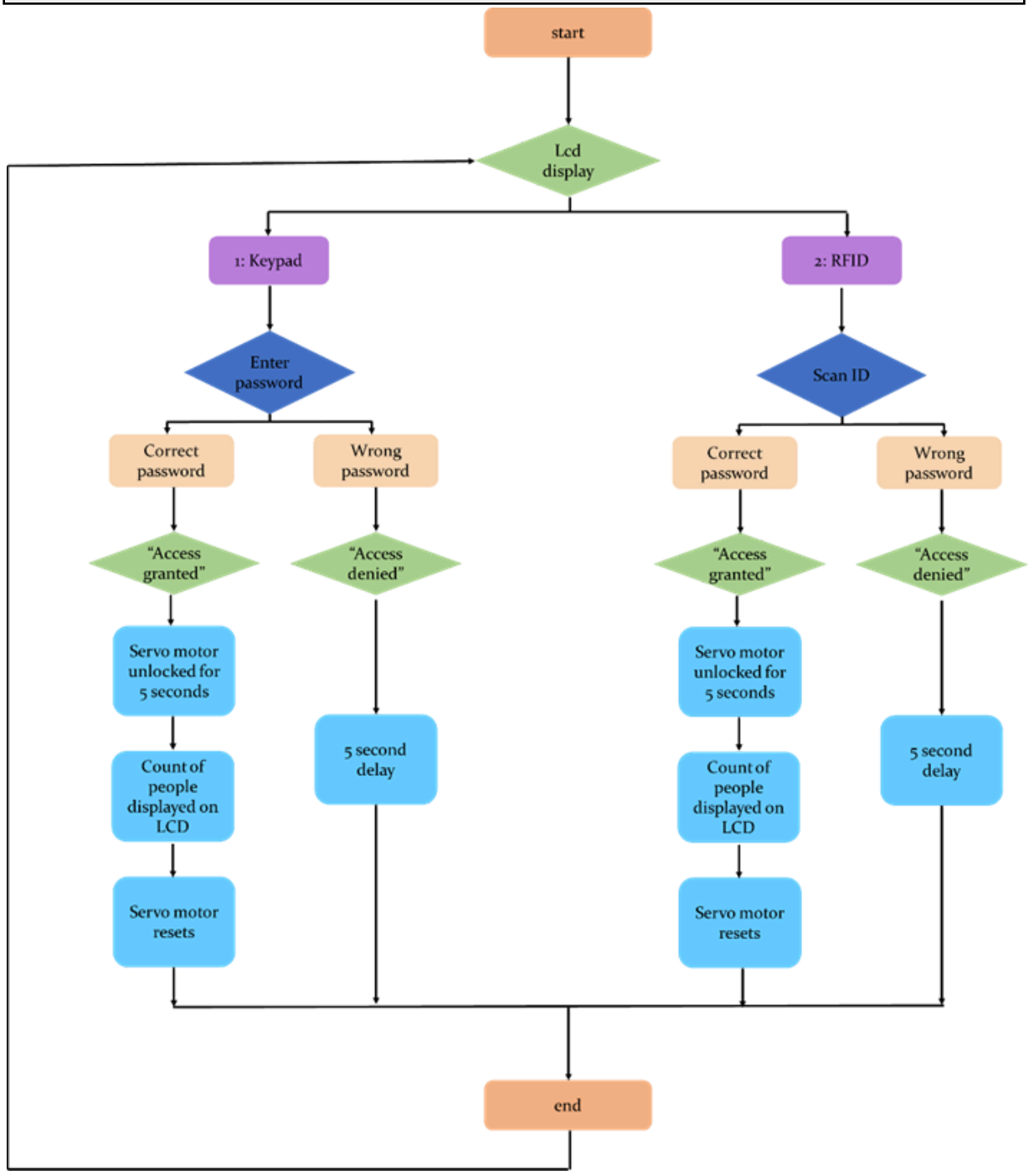
3. https://iopscience.iop.org/article/10.1088/1742-6596/1500/1/012132/pdf
   This paper discusses an automatic door lock system used for classroom security in the Electrical Engineering Department. It uses RFID ID cards as keys, which are scanned and verified through a server. When a valid card is scanned, the server tells the microcontroller to unlock the magnetic door lock. The system is

built using an Arduino Mega. The study involved reviewing related research, designing the device, and testing it. Results showed that the system worked effectively, helping lecturers improve classroom security and convenience.

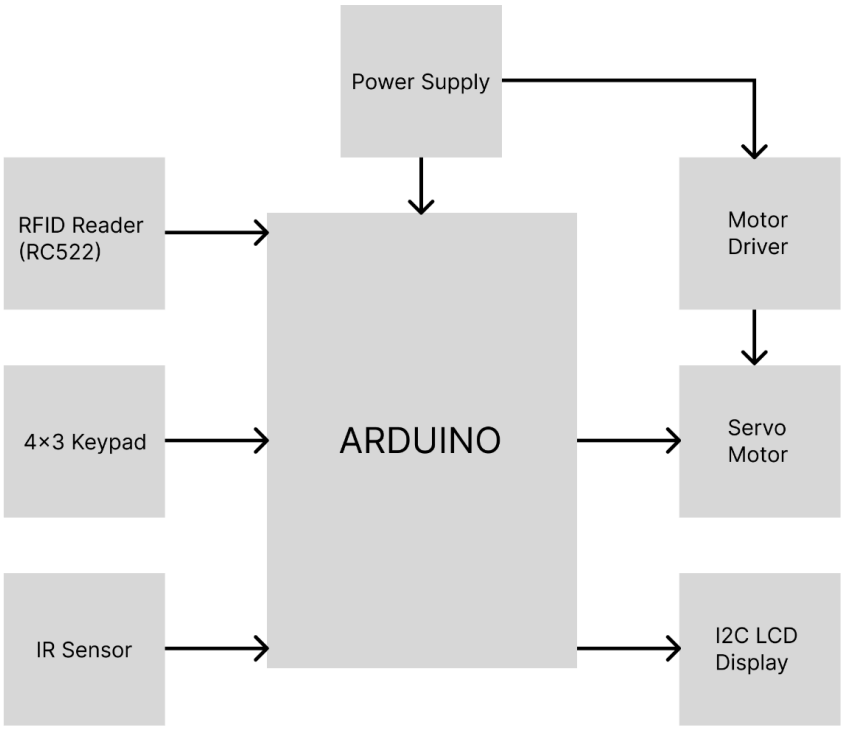
4. https://www.researchgate.net/profile/Akhilesh-Waoo-2/publication/354508883_RFID-Based_Digital_Door_Locking_System/links/61be184ffd2cbd7200ad0dd7/RFID-Based-Digital-Door-Locking-System.pdf
   This paper describes an IoT-based door locking system using RFID technology. Only registered users with authorized RFID cards can unlock the door. The system is controlled by an Arduino and uses a servo motor to open and close the door. It also keeps track of how long the door stays open. LED lights indicate the door status: green for open, yellow for locked, and red for an invalid card. A buzzer provides audio alerts. This setup enhances security and allows owners to monitor access to specific places like offices.

5. https://www.iarjournals.com/upload/43162168.pdf
   This paper focuses on improving home security using an RFID-based door lock system. Traditional locks like chains or deadbolts have drawbacks, such as being heavy, fragile, or inconvenient. The proposed system uses RFID technology to offer a more secure and user-friendly solution. RFID allows wireless, flexible, and scalable control over access. The aim is to combine better security with ease of use, all while keeping the cost low. This system addresses common issues found in traditional locking methods.

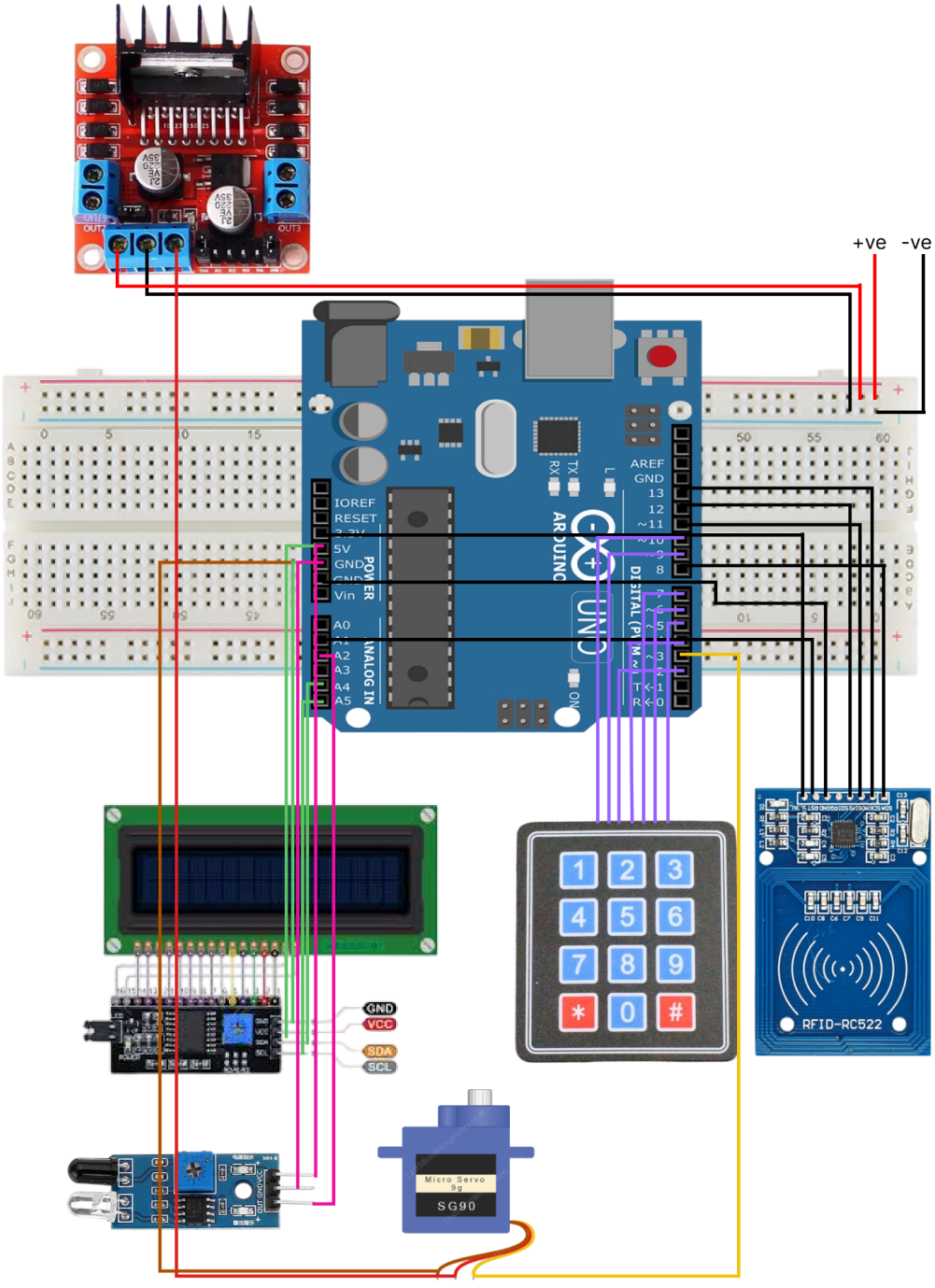
FLOW CHART :


start
Lcd display
1: Keypad
2: RFID
Enter password
Scan ID
Correct password
Wrong password
Correct password
Wrong password
"Access granted"
"Access denied"
"Access granted"
"Access denied"
Servo motor unlocked for 5 seconds
5 second delay
Servo motor unlocked for 5 seconds
5 second delay
Count of people displayed on LCD
Count of people displayed on LCD
Servo motor resets
Servo motor resets
end

BLOCK DIAGRAM :



CIRCUIT DIAGRAM :



PIN CONFIGURATIONS :

MODULE PIN	ARDUINO PIN
RFID Module :	
SDA	D8
SCK	D13
MOSI	D11
MISO	D12
GND	GND
RST	A1
3.3V	3.3V
Keypad :	
R1	D5
R2	D6
R3	D7
R4	D4
C1	D2
C2	D9
C3	D10
LCD :	
GND	GND
VCC	5V
SDA	A4
SCL	A5
SERVOMOTOR :	
PWM (Orange)	D3

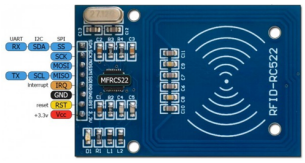
VCC (Red)	5V of motor driver
GND (Brown)	GND
IR Sensor :	
OUT	A2
GND	GND
VCC	5V
Motor Driver :	
+12 V	Positive of the battery
GND	Negative of the battery and GND of arduino
+5 V	VCC of the servo motor

COMPONENTS LIST :

Component 1– Arduino Uno :
The Arduino Uno is a popular open-source microcontroller board based on the ATmega328P. It features 14 digital I/O pins, 6 analog inputs, a 16 MHz quartz crystal, and onboard USB-to-serial communication, making it ideal for prototyping and embedded system development. The board supports various communication protocols (UART, SPI, I2C) and is programmable via the Arduino IDE using C/C++-based libraries. With its plug-and-play simplicity, robust community support, and extensive compatibility with sensors, actuators, and shields, the Arduino Uno is widely used in automation, robotics, IoT, and interactive projects.

Component 2 – RFID Reader/Writer Module :
The 13.56MHz RFID Reader/Writer Module based on the RC522 IC is a compact and efficient device for contactless data communication. Operating at 13.56MHz, it can read and write data to compatible RFID tags and cards, making it ideal for authentication,

access control, and automation applications. The module communicates via the SPI, I2C, or UART interface, allowing seamless integration with microcontrollers like Arduino and Raspberry Pi. With its low power consumption, fast response time, and anti-collision features, the RC522 module is widely used in secure identification systems, payment terminals, and smart inventory management.

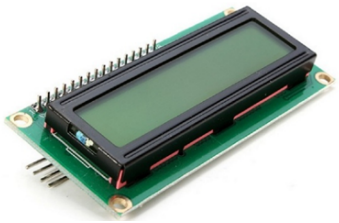


Component 3 – 4x4 Membrane Keypad :
The 4x4 Membrane Keypad is a compact and lightweight input device designed for user authentication and data entry in embedded systems. It features 16 tactile keys, including numbers (0-9) and function keys (*, #, A, B, C, D), arranged in a matrix configuration. The keypad communicates with microcontrollers like Arduino via a row-column scanning method, requiring minimal I/O pins. With its thin, flexible design, easy integration, and durable membrane switches, the keypad is widely used in security systems, access control, automation, and interactive projects.

Component 4 – RFID Smart Card :
The 13.56MHz RFID Smart Card, often referred to as an RFID ISO Card or MIFARE Classic Card, is a contactless identification card embedded with an RF chip and antenna. Operating at 13.56MHz, it communicates with RFID readers using technologies like ISO/IEC 14443A for secure data transmission. These cards are commonly used for access control, attendance systems, public transport, and cashless transactions. With unique identifier (UID) storage and optional writable memory, they provide a reliable, reusable, and tamper-resistant solution for authentication and automation applications.

Component 5 – LCD Display :

The 16x2 LCD Display is a widely used alphanumeric display module designed for embedded systems and microcontroller-based projects. It features two rows with 16 characters each, supporting ASCII and custom characters. Based on the Hitachi HD44780 controller, it communicates via parallel (4-bit or 8-bit mode) or I2C interface, making it compatible with microcontrollers like Arduino and Raspberry Pi. With its low power consumption, backlight for visibility, and ease of integration, the 16x2 LCD is ideal for displaying sensor data, system status, and user prompts in automation, IoT, and security applications.



Component 6 – Servo Motor :

A servo motor is a rotary actuator that enables precise control of angular position, velocity, and acceleration. It typically consists of a DC motor, gearbox, potentiometer, and control circuitry. The motor receives a PWM signal that determines its rotational angle, usually within a range of 0° to 180°. Servo motors are commonly used in robotics, automation, and control systems where accurate positioning is required. Due to their compact design and ease of interfacing, they are widely used in embedded applications.

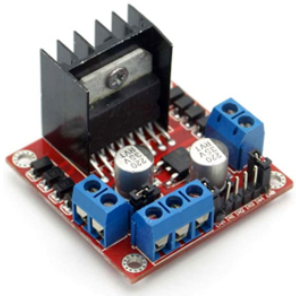
Component 7 – 9V Battery :

A 9V battery is a compact and portable power source commonly used in low-power electronic devices. It provides a nominal voltage of 9 volts and is available in both non-rechargeable (alkaline) and rechargeable (NiMH, Li-ion) variants. The battery

typically features a rectangular form factor with snap connectors for easy integration. Due to its convenience and moderate energy capacity, the 9V battery is suitable for powering microcontrollers, sensors, and small actuators in prototyping and standalone circuits.

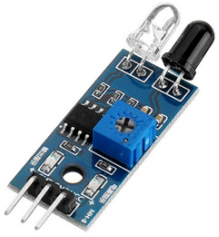
Component 8 – L298N Motor Driver :

The L298N is a dual full-bridge motor driver integrated circuit designed to control the direction and speed of two DC motors or one stepper motor. It supports motor voltages from 5V to 46V and current up to 2A per channel. The module includes heat sinks, terminal blocks, and logic-level input pins compatible with microcontrollers. It allows bidirectional control and features built-in diodes for back EMF protection, making it suitable for a variety of motor control applications in robotics and automation.



Component 9 – IR Sensor :

An infrared (IR) sensor is an electronic device that detects infrared radiation to identify proximity, motion, or object presence. It typically consists of an IR LED that emits infrared light and a photodiode or phototransistor that senses reflected light. When an object passes in front of the sensor, the reflected IR light is detected and converted into an electrical signal. IR sensors are widely used in obstacle detection, motion sensing, and line-following systems due to their simplicity, low cost, and fast response time.



WORKING OPERATION :

The primary objective of this system is to allow secure access control using two independent methods: an RFID-based authentication and a keypad-based password entry. The circuit integrates an Arduino Uno as the central controller, interfacing with multiple modules—RFID reader, 4x3 keypad, IR sensor, servo motor, I2C LCD, and a motor driver (L298N)—to create a functional and interactive security system.

The system begins with the LCD displaying a prompt for the user to either scan an RFID card or enter a password through the keypad. The user can choose either of the two modes:

Keypad Mode :
When the keypad is used, the user is prompted to enter a password. The Arduino checks this input against a predefined password stored in the code. If the password matches, the system displays “Access Granted” on the LCD, triggers the servo motor to unlock for 5 seconds using the L298N motor driver, and simultaneously increases the people count shown on the display. After the delay, the servo resets, relocking the door. If the password is incorrect, “Access Denied” is shown and no access is granted.

RFID Mode :
In the RFID-based path, the user scans their RFID tag using the RC522 reader. The tag's UID is read by the Arduino and checked against stored IDs. Upon a successful match, “Access Granted” is displayed, and the same unlocking mechanism is triggered as in the keypad mode. Again, the people count is incremented and shown on the LCD. If the scanned ID is unrecognized, the LCD displays “Access Denied.”

An IR sensor is used to detect actual presence or movement through the doorway, which can help in cross-verifying the people counter logic or for added automation.

The servo motor (SG90) is powered via the L298N motor driver module, with a separate power supply ensuring sufficient torque. The use of the I2C LCD reduces pin consumption, keeping the system compact and efficient.

This dual-authentication system is ideal for controlled access environments like offices, labs, or homes, where multiple users can use either RFID cards or passcodes. The project enhances security, ensures logging of entries, and demonstrates an integration of multiple input-output devices using a single microcontroller.

FEATURES AND ADVANTAGES :

The positive features of this project include :

- Dual Authentication : The system supports two modes of authentication—RFID card scanning and password input through a keypad. This dual method enhances security by making it harder for unauthorized individuals to gain access.

- LCD User Interface : A 16x2 LCD screen provides a clear and user-friendly interface, guiding users through the process and displaying messages such as "Enter Password" or "Access Granted/Denied."

- Automated Locking with Servo Motor : A servo motor is used to control the door lock. It unlocks for a brief period (rotates 90°) after valid access and resets automatically after a short delay, ensuring the door is always secured.

- Entry Count with IR Sensor : An IR sensor tracks how many people enter when the door is unlocked, providing basic monitoring functionality not commonly available in standard lock systems.

- Auto-Reset Loop : After completing a cycle—regardless of whether access was granted or denied—the system returns to the initial state, allowing continuous use without manual reset.

- Battery-Powered : Powered by a 9V battery, the system can operate in locations without direct power supply, making it ideal for remote or temporary installations.

DRAWBACKS AND LIMITATIONS :

Despite its effectiveness, the system has certain drawbacks and limitations :

- Limited Security Features : The system relies on pre-registered RFID cards and static passwords, which may be susceptible to cloning, theft, or unauthorized sharing. No encryption in RFID data transmission makes it vulnerable to hacking.

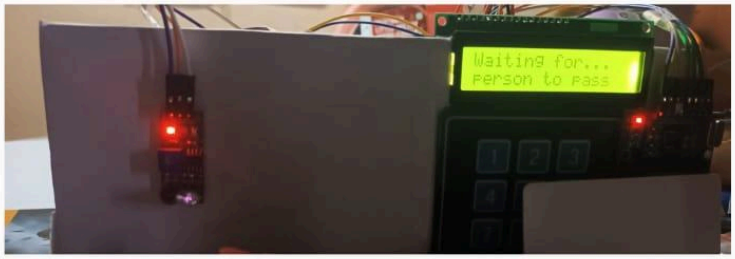
- Dependency on RFID Tags : Lost or stolen RFID cards can grant unauthorized access unless immediately deactivated. Users must carry their cards at all times, which may be inconvenient.

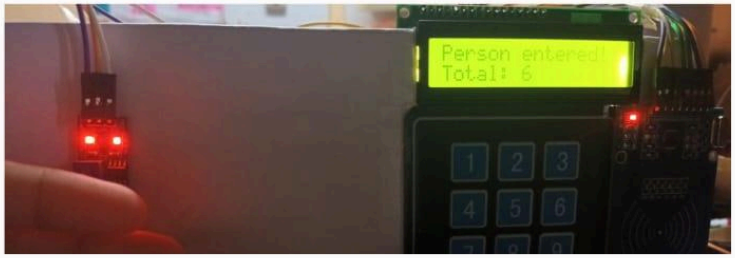
- People Counter Accuracy : The IR sensor can miscount due to multiple people entering simultaneously or small objects triggering false detections. It does not differentiate between entry and exit, leading to possible incorrect counts.

- Limited Scalability : The system is designed for small-scale use and may not handle high-traffic areas efficiently. Adding cloud integration, real-time database management, or biometric authentication would improve scalability.

- Power Dependency : The system requires continuous power to function, making it ineffective during power failures without a backup power source. Also, for the purpose of the project prototype we have used a 9V battery as our power supply which is not enough to power the servo motors mechanical movement.

DEMO :





Working Video and Code Run-Through have been shared on this drive folder : https://drive.google.com/drive/folders/1MFW3hhIm7Zp0vnbZk9iugKtJWiBqNEis?usp=drive_link

CODE :

```
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <Keypad.h>
#include <Servo.h>
#include <SPI.h>
#include <MFRC522.h>

// LCD Setup
LiquidCrystal_I2C lcd(0x27, 16, 2);

// Servo Motor (Pin D3) - Updated with better control
Servo doorLockServo;
#define SERVO_PIN 3
#define SERVO_LOCKED_POS 20    // Adjusted locked position (experiment with values)
#define SERVO_UNLOCKED_POS 80  // Adjusted unlocked position
bool isDoorLocked = true;

// Keypad Setup
const byte ROWS = 4;
const byte COLS = 3;
char keys[ROWS][COLS] = {
  {'1','2','3'},
  {'4','5','6'},
  {'7','8','9'},
  {'*','0','#'}
};
byte rowPins[ROWS] = {5, 6, 7, 4};
byte colPins[COLS] = {2, 9, 10};
Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS, COLS);

// Password
String correctPassword = "1234";
String enteredPassword = "";

// RFID Setup
#define SS_PIN 8
#define RST_PIN 9
MFRC522 rfid(SS_PIN, RST_PIN);
byte registeredUIDs[][4] = {{0x7B, 0xFD, 0xF7, 0x03}};
int numRegisteredUIDs = sizeof(registeredUIDs)/sizeof(registeredUIDs[0]);

// IR Sensor (Pin A2)
#define IR_SENSOR_PIN A2
int peopleCount = 0;
bool objectDetected = false;
#define DETECTION_TIMEOUT 10000  // 10 seconds
```

```
// Auth Mode
char authMode = '#';

void setup() {
  Serial.begin(9600);

  // Initialize Servo - Added servo test sequence
  doorLockServo.attach(SERVO_PIN);
  testServo(); // Test servo movement on startup

  // Initialize other components
  lcd.init();
  lcd.backlight();
  SPI.begin();
  rfid.PCD_Init();
  pinMode(IR_SENSOR_PIN, INPUT_PULLUP);

  selectAuthMode();
}

void loop() {
  if (authMode == '1') handleRFID();
  else if (authMode == '2') handleKeypad();
}

// ====== Servo Test Sequence ======
void testServo() {
  Serial.println("Testing servo...");
  doorLockServo.write(SERVO_LOCKED_POS);
  delay(4000);
  doorLockServo.write(SERVO_UNLOCKED_POS);
  delay(4000);
  doorLockServo.write(SERVO_LOCKED_POS);
  Serial.println("Servo test complete");
}

// ====== Door Control Functions ======
void lockDoor() {
  doorLockServo.write(SERVO_LOCKED_POS);
  isDoorLocked = true;
  Serial.println("Door locked");
}

void unlockDoor() {
  doorLockServo.write(SERVO_UNLOCKED_POS);
  isDoorLocked = false;
  Serial.println("Door unlocked");
}

// ====== Authentication Mode Selection ======
void selectAuthMode() {
```

```
  lcd.clear();
  lcd.print("Select Mode:");
  lcd.setCursor(0, 1);
  lcd.print("1:RFID 2:Keypad");

  authMode = '0';
  while (authMode != '1' && authMode != '2') {
    authMode = keypad.getKey();
    delay(10);
  }

  lcd.clear();
  if (authMode == '1') {
    lcd.print("Scan your ID");
    Serial.println("RFID mode activated");
  } else {
    lcd.print("Enter Password");
    Serial.println("Keypad mode activated");
  }
}

// ====== Keypad Handling ======
void handleKeypad() {
  char key = keypad.getKey();
  if (!key) return;

  Serial.print("Key pressed: "); Serial.println(key);

  if (key == '#') { // Submit password
    if (enteredPassword == correctPassword) {
      grantAccess();
    } else {
      denyAccess();
    }
    enteredPassword = "";
  }
  else if (key == '*') { // Clear input
    enteredPassword = "";
    lcd.clear();
    lcd.print("Enter Password");
  }
  else { // Password entry
    enteredPassword += key;
    lcd.setCursor(enteredPassword.length()-1, 1);
    lcd.print('*');
  }
}

// ====== RFID Handling ======
void handleRFID() {
  if (!rfid.PICC_IsNewCardPresent() || !rfid.PICC_ReadCardSerial()) return;
```

```
  Serial.print("Scanned UID:");
  bool accessGranted = false;
  for (byte i = 0; i < rfid.uid.size; i++) {
    Serial.print(rfid.uid.uidByte[i] < 0x10 ? " 0" : " ");
    Serial.print(rfid.uid.uidByte[i], HEX);

    // Check against registered UIDs
    for (int j = 0; j < numRegisteredUIDs; j++) {
      if (memcmp(rfid.uid.uidByte, registeredUIDs[j], 4) == 0) {
        accessGranted = true;
        break;
      }
    }
  }
  Serial.println();

  if (accessGranted) {
    grantAccess();
  } else {
    denyAccess();
  }

  rfid.PICC_HaltA();
  rfid.PCD_StopCrypto1();
}

// ====== IR Sensor People Counting ======
bool waitForPerson() {
  lcd.clear();
  lcd.print("Waiting for...");
  lcd.setCursor(0, 1);
  lcd.print("person to pass");

  unsigned long startTime = millis();
  while (millis() - startTime < DETECTION_TIMEOUT) {
    int irState = digitalRead(IR_SENSOR_PIN);

    if (irState == LOW && !objectDetected) {
      // Person detected
      objectDetected = true;
      peopleCount++;
      Serial.print("Person detected! Total: ");
      Serial.println(peopleCount);

      lcd.clear();
      lcd.print("Person entered!");
      lcd.setCursor(0, 1);
      lcd.print("Total: ");
      lcd.print(peopleCount);
```

```
      delay(1000); // Debounce
      return true;
    }
    else if (irState == HIGH && objectDetected) {
      objectDetected = false;
    }
    delay(50);
  }

  lcd.clear();
  lcd.print("Timeout!");
  delay(1000);
  return false;
}

// ====== Access Control ======
void grantAccess() {
  unlockDoor();
  lcd.clear();
  lcd.print("Access granted!");
  Serial.println("Access granted - door unlocked");

  // Wait for person to pass
  waitForPerson();

  lockDoor();
  selectAuthMode();
}

void denyAccess() {
  lcd.clear();
  lcd.print("Access denied!");
  Serial.println("Access denied");
  delay(2000);
  selectAuthMode();
}
```

FINAL PRESENTATION :

A number of changes were done to the initial idea to fit it into the resources and objectives of the project. The prototype was created based on an Arduino Uno, which has fewer input/output pins than the Arduino Mega. This presented challenges in finalizing an optimal pin arrangement to facilitate proper functioning. Additionally, the whole system runs on a 9V battery, making the device capable of functioning as a fully operational and portable remote prototype.

CONCLUSION :

The RFID and keypad-based door lock system with an integrated people counter offers a cost-effective and practical solution for secure access control in restricted environments. By combining dual authentication—RFID scanning and password entry—with real-time monitoring via an IR sensor, the system enhances both security and situational awareness. Despite its effectiveness, limitations such as RFID card cloning, password predictability, and IR-based counting inaccuracies must be

acknowledged. Future upgrades could include biometric authentication, cloud-based activity logs, encrypted data handling, and AI-powered intrusion detection. Overall, the project successfully demonstrates a smart, scalable access control system with strong potential for real-world deployment and continued innovation.