VEHICLE ACCESS CONTROL SYSTEM

As a part of the subject

INTRODUCTION TO COMMUNICATION & IOT

22AIE211

Submitted by

S. NAGA KOUSHIK

(CB.EN.U4AIE22046)

SUBASHREE.M

(CB.EN.U4AIE22048)

VISWANATH ADARSH

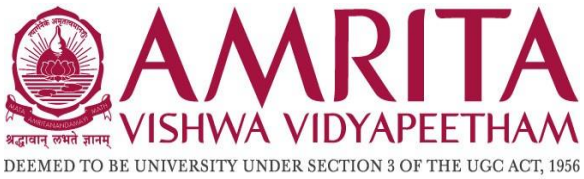
(CB.EN.U4AIE22063)

ABHIRAMARAJU

(CB.EN.U4AIE22066)

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY
IN
CSE(AI)



Centre for Computational Engineering and Networking

AMRITA SCHOOL OF ARTIFICIAL INTELLIGENCE

AMRITA VISHWA VIDYAPEETHAM

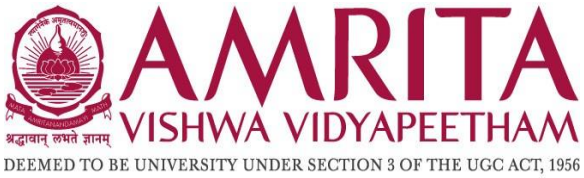
COIMBATORE - 641
112 (INDIA)

June – 2024

AMRITA SCHOOL OF ARTIFICIAL INTELLIGENCE

AMRITA VISHWA VIDYAPEETHAM

COIMBATORE - 641 112



BONAFIDE CERTIFICATE

This is to certify that the thesis entitled "VEHICLE ACCESS CONTROL SYSTEM " submitted by Naga Koushik (CB.EN.U4AIE22046), Subasree (CB.EN.U4AIE22048), Viswanath Adarsh (CB.EN.U4AIE22063), Abhiramaraju (CB.EN.U4AIE22066) for the award of the Degree of Bachelor of Technology in the "CSE(AI) " is a bonafide record of the work carried out by him under our guidance and supervision at Amrita School of Artificial Intelligence, Coimbatore.

Dr.Jaisoorayj

Project Guide

Dr. K.P.Soman

Professor and Head CEN

Submitted for the university examination held on 10/12/2023

AMRITA SCHOOL OF ARTIFICIAL INTELLIGENCE

AMRITA VISHWA VIDYAPEETHAM

COIMBATORE - 641 112

DECLARATION

We, Naga Koushik (CB.EN.U4AIE22046), Subashree.M (CB.EN.U4AIE22048), Viswanath Adarsh (CB.EN.U4AIE22063), Abhiramaraju (CB.EN.U4AIE22066) hereby declare that this is entitled "VEHICLE ACCESS CONTROL SYSTEM", is the record of the original work done by us under the guidance of Dr.Jaisoorayj, Assistant Professor, Centre for Computational Engineering and Networking, Amrita School of Artificial Intelligence, Coimbatore. To, the best of our knowledge this work has not formed the basis for the award of any degree/diploma/ associate ship/fellowship/or a similar award to any candidate in any University.

Name		**Roll Number**	**Signature**
Naga Koushik	-	CB.EN.U4AIE22046	
Subashree.M	-	CB.EN.U4AIE22048	
Viswanath Adarsh	-	CB.EN.U4AIE22063	
Abhiramaraju	-	CB.EN.U4AIE22066	

Place: Coimbatore

Date:10-12-2023

Contents

1. Abstract: 7
2. Introduction: 7
2.1 About the Project: 7
2.2 Project Objectives: 9
2.3 Block Diagram of the proposed project: 10
3. Hardware Components: 10
3.1 RFID Module (RC522): 10
3.2 IR Sensors: 11
3.3 Servo Motor: 11
3.4 LEDs: 12
3.5 Arduino Mega Microcontroller: 13
4 Implementation: 15
4.1 Flow diagram: 15
4.2 Procedure: 16
4.2.2 Entry Processing: 16
4.2.3 Exit Processing: 16
4.3 Circuit Diagram 17
5 Advantages: 17
6 Construction and Working Principle 20
6.1 Construction: 20
6.1.1 Components Used: 20
6.1.2 Connections: 20
6.2 Working Principle: 21
6.2.1 Workflow Summary: 23
7 Code: 23

8 Results: 27
9 Conclusion: 28

Table of Figures

Figure 1 RFID connection with Arduino mega 10
Figure 2 RFID details..... 10
Figure 3 IR Sensor 11
Figure 4 Survo motor 12
Figure 5 LEDs..... 13
Figure 6 Aurdino mega 14
Figure 7 Flow of the Project 15
Figure 8 Circuit Diagram 17

Acknowledgement

We would like to express our special thanks of gratitude to our teacher (Dr. Jaisooraj sir), who gave us the golden opportunity to do this wonderful project, which also helped us in doing a lot of Research and we came to know about so many new things. We are thankful for the opportunity given.

We would also like to thank our group members, as without their cooperation, we would not have been able to complete the project within the prescribed time.

1. Abstract:

The Automated Vehicle Access Control System seamlessly integrates RFID (Radio-Frequency Identification) technology with IR (Infrared) sensors to manage vehicle access. An Arduino Mega microcontroller orchestrates this efficient system, ideal for parking lots, toll booths, or restricted areas. Upon detecting an approaching vehicle, IR sensors trigger the system to verify the vehicle's RFID tag. If authorized, the servo-controlled gate grants access while simultaneously capturing entry data, including date, time, and vehicle ID (from the RFID tag). LED indicators continue to provide visual feedback on access status. This enhanced system offers streamlined and secure vehicle access management, facilitating analysis and reporting. This improves operational efficiency and security across various applications.

2. Introduction:

2.1 About the Project:

In today's dynamic and fast-paced world, efficient management of vehicle access at controlled points such as parking facilities, toll booths, and restricted areas is essential for ensuring smooth traffic flow and enhancing security. Traditional manual methods of vehicle access control are often labor-intensive, error-prone, and lack real-time monitoring capabilities. To address these challenges, there is a growing demand for automated solutions that can streamline the access control process, improve efficiency, and enhance security.

The integration of RFID (Radio-Frequency Identification) technology with IR (Infrared) sensors and servo-controlled gates presents a promising opportunity to develop automated vehicle access control systems that are both efficient and secure. RFID technology allows for seamless and contactless identification and authentication of vehicles, while IR sensors enable accurate detection of vehicle presence at entry and exit points. The servo-controlled gate mechanism facilitates automated entry and exit of authorized vehicles, providing a seamless and efficient access experience.

This project aims to design and implement an Automated Vehicle Access Control System that leverages the capabilities of RFID, IR sensors, and servo motors to manage vehicle access at controlled points effectively. The system will authenticate vehicles based on pre-programmed RFID tags, automatically open and close gates upon vehicle detection, and provide visual feedback to users through LED indicators. By automating the access control process, the system will enhance operational efficiency, improve security, and provide a seamless access experience for authorized vehicles.

In this project, we will explore the design, development, and implementation of the Automated Vehicle Access Control System, focusing on system architecture, hardware integration, software development, and system testing. Through practical experimentation and evaluation, we aim to demonstrate the system's effectiveness, reliability, and scalability in managing vehicle access in various environments. Ultimately, the project seeks to contribute to the

advancement of automated vehicle access control technologies and their practical applications in real-world settings.

2.2 Project Objectives:

1. **Enhanced Security:** Develop an automated vehicle access control system to bolster security by permitting only authorized vehicles at entry and exit points.
2. **Efficient Authentication:** Utilize RFID technology for swift and efficient vehicle authentication, ensuring seamless access for authorized vehicles.
3. **Optimized Traffic Flow:** Automate access control to improve traffic flow, minimizing wait times for vehicle entry and exit and enhancing overall efficiency.
4. **Reliable Gate Operation:** Implement a servo motor-controlled gate mechanism for smooth and prompt gate operation based on authentication status, enhancing user experience and system reliability.

2.3 Block Diagram of the proposed project:

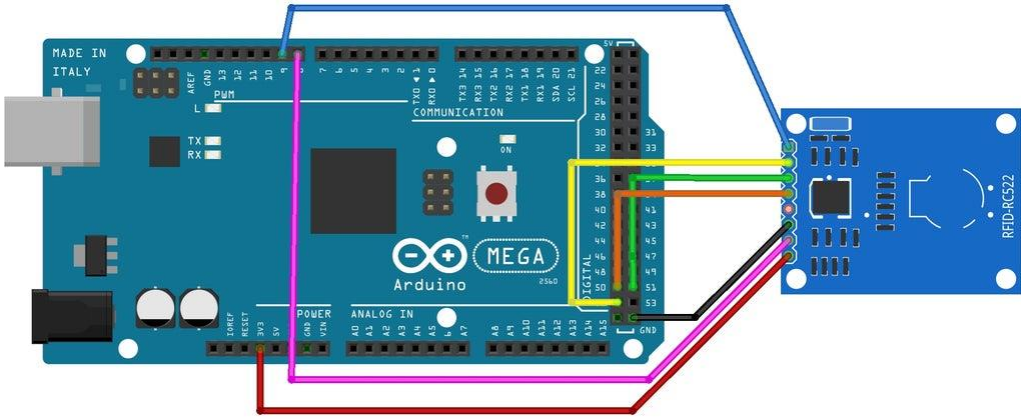


Figure 1 RFID connection with Arduino mega

3. Hardware Components:

3.1 RFID Module (RC522):

The RFID module serves as the primary means of vehicle identification and authentication. It consists of an RFID reader and antenna, capable of reading RFID tags attached to vehicles. The module communicates with the Arduino Mega microcontroller using

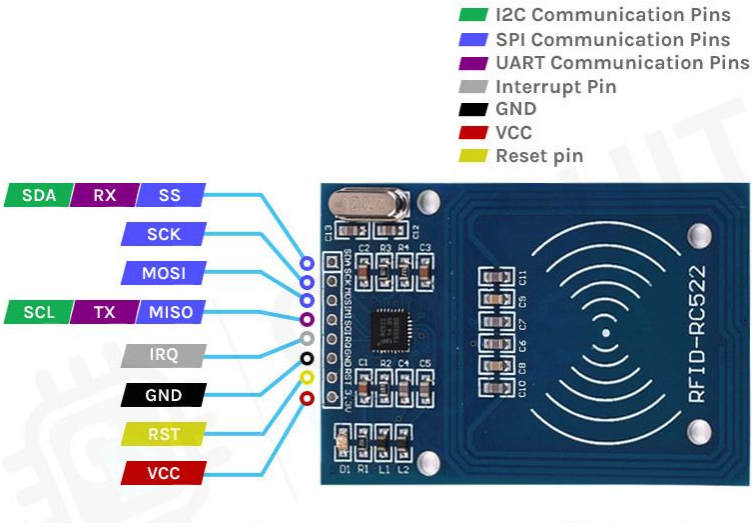


Figure 2 RFID details

the Serial Peripheral Interface (SPI) protocol. Key features include fast reading speed, low power consumption, and support for various RFID tag types.

3.2 IR Sensors:

Infrared (IR) sensors are used for vehicle detection at entry and exit points. Each sensor comprises an IR emitter and receiver pair, capable of detecting the presence of vehicles based on reflected infrared light. They are connected to digital input pins of the Arduino Mega for interfacing and data acquisition. IR sensors offer reliable detection capabilities and are suitable for various environmental conditions.

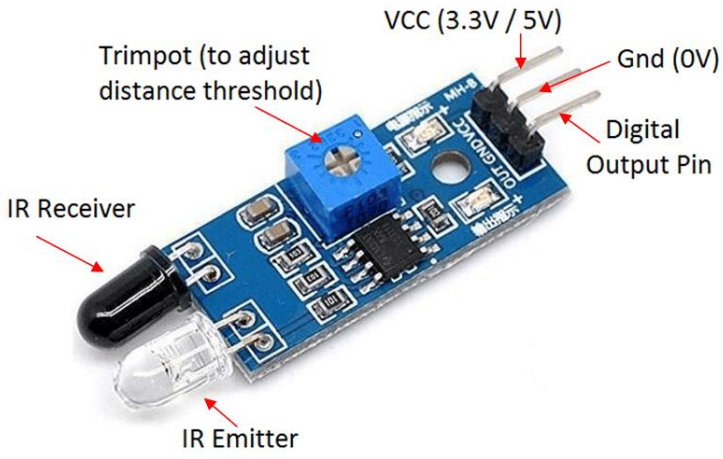


Figure 3 IR Sensor

3.3 Servo Motor:

The servo motor controls the gate mechanism, facilitating its opening and closing based on authentication status. It provides precise angular control over the gate's movement, ensuring smooth operation and positional accuracy. The servo motor is connected to a digital output

pin of the Arduino Mega for control signals.Features include high torque, low noise, and a compact form factor, ideal for gate automation applications.

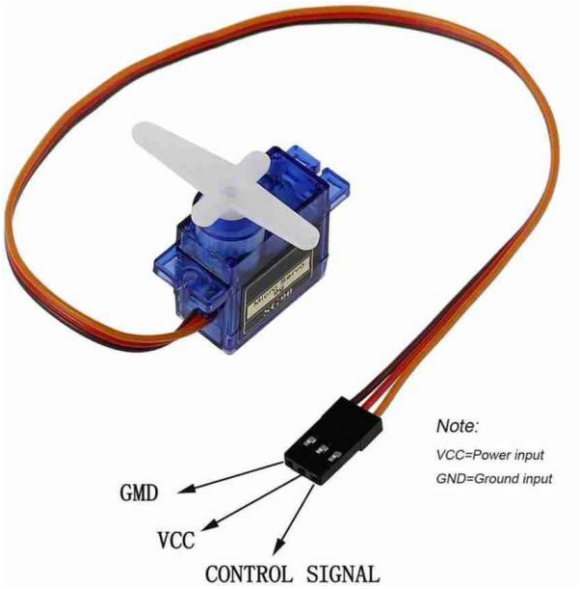


Figure 4 Survo motor

3.4 LEDs:

Light Emitting Diodes (LEDs) are used to provide visual feedback on access status to drivers and system administrators. Two LEDs are employed: a green LED indicates authorized access, while a red LED signifies denied access. They are connected to digital output pins of the Arduino Mega for control signals.LEDs offer low power consumption, long lifespan, and high visibility, making them suitable for indicating access status in various lighting conditions.

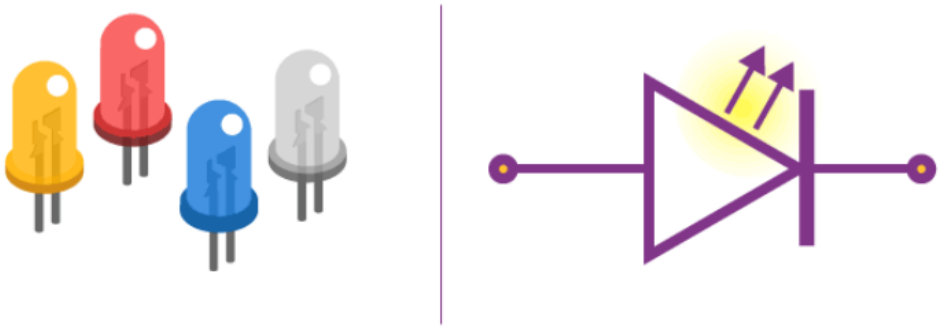


Figure 5 LEDs

3.5 Arduino Mega Microcontroller:

The Arduino Mega serves as the central processing unit for the access control system, orchestrating the operation of all hardware components. It features a powerful microcontroller with multiple digital and analog input/output pins, suitable for interfacing with various sensors and actuators. The Arduino Mega is programmed using the Arduino Integrated Development Environment (IDE), allowing for easy code development and uploading. Key capabilities include real-time data processing, sensor interfacing, and motor control, making it an ideal choice for embedded systems applications like access control.

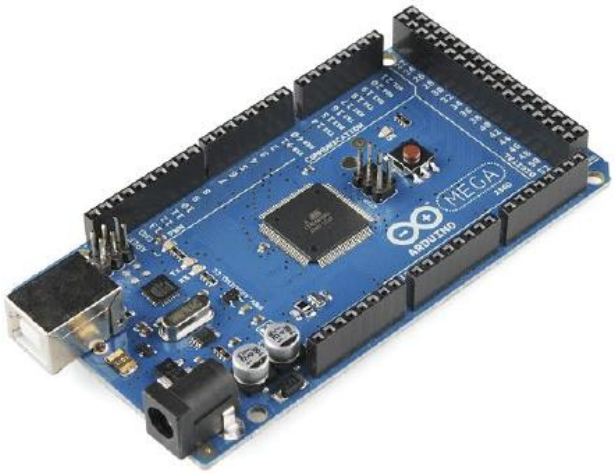


Figure 6 Aurdino mega

4 Implementation:

4.1 Flow diagram:

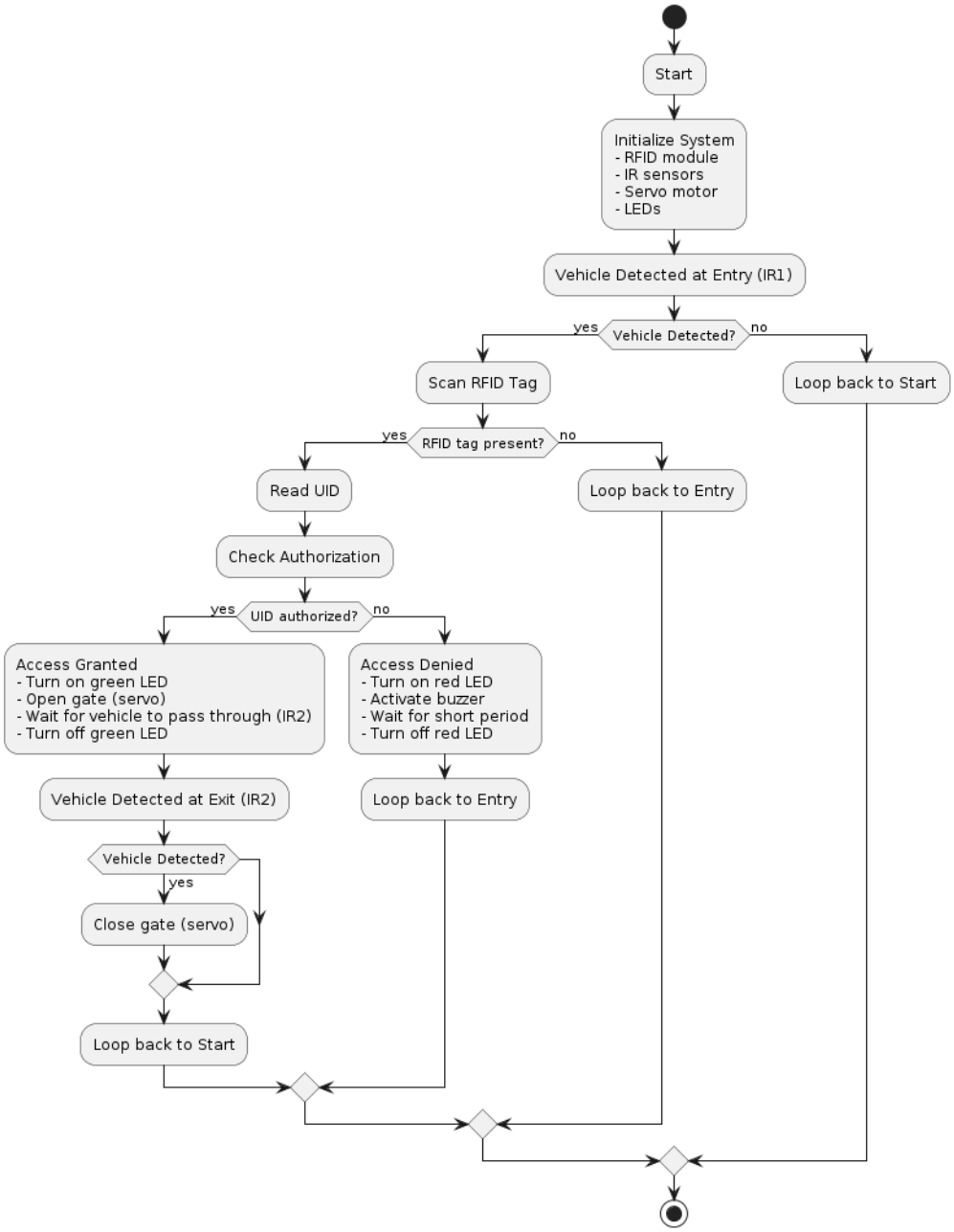


Figure 7 Flow of the Project

4.2 Procedure:

There are mainly three part in this project they are

4.2.1 Initialization:

In the initialization phase, the system components are set up and made ready for operation. This includes initializing the RFID module, IR sensors, servo motor, and LEDs. This step ensures that all hardware components are properly configured before the system starts monitoring for vehicles and processing RFID tags.

4.2.2 Entry Processing:

The entry processing phase involves detecting a vehicle at the entry IR sensor and then scanning for an RFID tag to check authorization. If a vehicle is detected at the entry point, the system scans for an RFID tag. If a tag is present, its UID is read and checked against a list of authorized UIDs. If the UID is authorized, the system grants access by turning on the green LED, opening the gate using the servo motor, and waiting for the vehicle to pass through the second IR sensor. If the UID is not authorized, the system denies access by turning on the red LED and activating a buzzer, then waiting for a short period before resetting to monitor for the next vehicle.

4.2.3 Exit Processing:

The exit processing phase deals with detecting a vehicle at the exit IR sensor and subsequently closing the gate. After the vehicle has passed through the exit point, the system closes the gate by adjusting the servo motor to its initial position. This phase ensures that the gate

remains open until the vehicle has fully exited the monitored area, preventing any potential collisions or misreadings.

4.3 Circuit Diagram

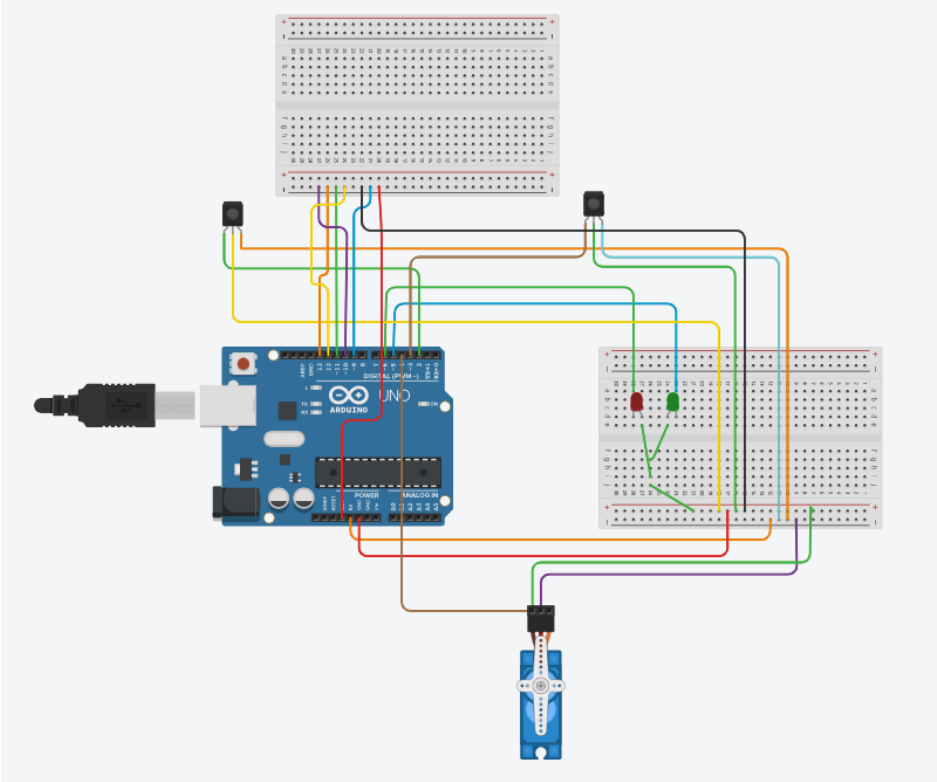


Figure 8 Circuit Diagram

5 Advantages:

Advantages and Benefits of the RFID-Based Vehicle Access System

Enhanced Security:

The use of RFID technology provides a high level of security by ensuring that only authorized vehicles can gain access. Unauthorized vehicles without the correct RFID tags are denied entry, reducing the risk of theft or unauthorized access to the premises.

Automated Access Control:

The system automates the process of vehicle entry and exit, minimizing the need for human intervention. This reduces the need for manual checks by security personnel, thereby lowering labor costs and improving operational efficiency.

Efficient Traffic Management:

By automating the entry and exit process, the system helps in managing traffic flow more efficiently. Vehicles can move in and out without delays, which is particularly beneficial during peak hours. This leads to smoother traffic operations and reduced congestion at entry and exit points.

Data Logging and Tracking:

The system can be integrated with a data logging mechanism to keep track of all vehicles that enter and exit the premises. This data can be used for various purposes, such as auditing, tracking vehicle movements, and identifying patterns or potential security threats.

Convenience for Users:

The automated nature of the system offers convenience for vehicle owners. They can enter and exit the premises without having to stop for manual checks, which saves time and provides a seamless access experience.

Scalability:

The system can be easily scaled to accommodate more entry and exit points or to manage a larger volume of vehicles. Additional RFID

readers, sensors, and gates can be integrated into the existing setup without significant changes to the infrastructure.

Reduced Human Error:

By automating the vehicle access process, the likelihood of human errors, such as misidentifying vehicles or failing to record entries and exits, is minimized. This leads to more accurate and reliable access control.

Cost-Effective:

Over time, the system can lead to cost savings by reducing the need for security personnel and minimizing the costs associated with manual access control methods. The initial investment in RFID technology and sensors is offset by the long-term operational efficiencies gained.

Environmentally Friendly:

By reducing idle times and vehicle queues, the system can contribute to lower emissions from vehicles. Efficient traffic management means less fuel consumption and reduced environmental impact, supporting sustainability goals.

Integration with Other Systems:

The RFID-based vehicle access system can be integrated with other security and management systems, such as surveillance cameras, parking management systems, and building access control. This creates a comprehensive security network that enhances overall safety and operational effectiveness.

6 Construction and Working Principle

6.1 Construction:

6.1.1 Components Used:

- **Arduino Mega:** Acts as the main controller, processing signals and controlling all connected components.
- **RFID Module (MFRC522):** Used to read RFID tags.
- **IR Sensors:** Two sensors (one for entry and one for exit) to detect the presence of a vehicle.
- **Servo Motor:** Controls the gate mechanism, opening and closing it based on access validation.
- **LEDs:** Green and red LEDs to indicate access status (granted or denied).
- **Buzzer:** Provides audible feedback for denied access.

6.1.2 Connections:

- **RFID Module:**
  - SDA -> D9
  - SCK -> D52
  - MOSI -> D51
  - MISO -> D50
  - GND -> GND
  - RST -> D8
  - 3.3V -> 3.3V
- **IR Sensors:**
  - **Entrance IR Sensor:** VCC -> 5V, GND -> GND, OUT -> D2

        - **Exit IR Sensor:** VCC -> 5V, GND -> GND, OUT -> D3
    - **Servo Motor:** Signal -> D4, VCC -> 5V, GND -> GND
    - **LEDs:**
        - **Green LED:** Anode -> 220Ω resistor -> D5, Cathode -> GND
        - **Red LED:** Anode -> 220Ω resistor -> D6, Cathode -> GND

6.2 Working Principle:

The RFID-based vehicle access control system operates on a straightforward principle of identification and authorization using RFID technology, coupled with IR sensors for vehicle detection and a servo motor for gate control. Here's how the system works step-by-step:

1. **System Initialization:**
    - When powered on, the Arduino Mega initializes all components, including the RFID module, IR sensors, servo motor, LEDs, and the buzzer.
2. **Vehicle Detection at Entry:**
    - The entrance IR sensor continuously monitors for the presence of a vehicle. When a vehicle is detected, it signals the Arduino to start the RFID scanning process.
3. **RFID Tag Scanning:**
    - The RFID module scans for an RFID tag. If a tag is present, it reads the unique identifier (UID) from the tag.
4. **Authorization Check:**

- The UID read from the RFID tag is compared against a pre-defined list of authorized UIDs stored in the Arduino's memory.
- If the UID matches an authorized entry, access is granted. If not, access is denied.

5. **Access Granted:**
    - The green LED lights up to indicate that access is granted.
    - The servo motor is activated to open the gate by rotating to a designated angle.
    - The system waits for the vehicle to pass through the entrance, detected by the exit IR sensor.
6. **Access Denied:**
    - The red LED lights up and the buzzer sounds to indicate that access is denied.
    - After a short delay, the red LED and buzzer turn off, and the system resets to detect another vehicle.
7. **Vehicle Detection at Exit:**
    - The exit IR sensor monitors the vehicle as it passes through.
    - Once the vehicle is detected at the exit, the servo motor is activated to close the gate by rotating back to the initial position.
    - The system then resets to its initial state, ready for the next vehicle.

6.2.1 Workflow Summary:

- **Step 1:** System initializes all components.
- **Step 2:** Entrance IR sensor detects a vehicle.
- **Step 3:** RFID module scans for a tag.
- **Step 4:** UID is checked for authorization.
- **Step 5:** If authorized, green LED lights up, gate opens, and vehicle passes through. If not, red LED and buzzer activate, denying access.
- **Step 6:** Exit IR sensor detects the vehicle's departure, and the gate closes.
- **Step 8:** System resets for the next cycle.

This combination of RFID technology and IR sensors provides a secure, automated method for controlling vehicle access, ensuring that only authorized vehicles can enter and exit the controlled area.

7 Code:

Arduino IDE code

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

// Pin Definitions
#define SS_PIN 9
#define RST_PIN 8
#define ENTRANCE_SENSOR_PIN 2
#define EXIT_SENSOR_PIN 3
#define SERVO_PIN 4
#define GREEN_LED_PIN 5
#define RED_LED_PIN 6
```

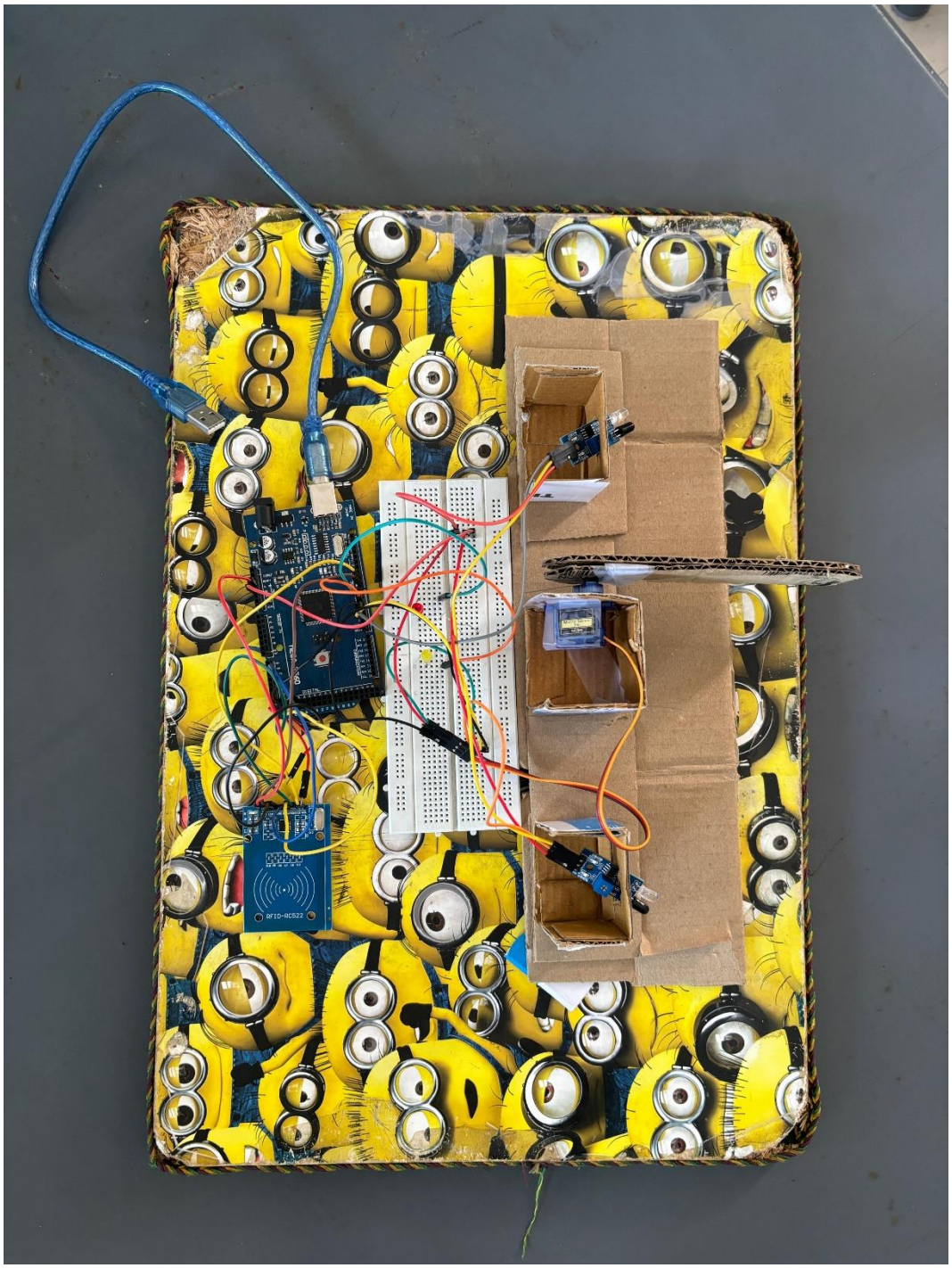
```
// RFID Module
MFRC522 mfrc522(SS_PIN, RST_PIN);

// Servo Motor
Servo gateServo;

// Create a dictionary to store authorized UIDs and their respective
names
struct AuthorizedCard {
  String uid;
  String name;
};

AuthorizedCard authorizedCards[] = {
  { "0E43257D", "Alice" },
  { "35227", "Bob" }
};
const int numAuthorizedCards = sizeof(authorizedCards) /
sizeof(AuthorizedCard);

// Variables
bool vehicleDetected = false;
bool gateOpen = false;
unsigned long lastEntranceSensorTriggerTime = 0;
unsigned long lastExitSensorTriggerTime = 0;

void setup() {
  Serial.begin(9600);
  SPI.begin();
  mfrc522.PCD_Init();

  pinMode(ENTRANCE_SENSOR_PIN, INPUT);
  pinMode(EXIT_SENSOR_PIN, INPUT);
  pinMode(GREEN_LED_PIN, OUTPUT);
  pinMode(RED_LED_PIN, OUTPUT);

  gateServo.attach(SERVO_PIN);
  gateServo.write(90); // Initial position (gate closed)

  Serial.println("System Initialized. Waiting for vehicle...");
}

void loop() {
  unsigned long currentMillis = millis();

  // Check the entrance sensor with debounce
```

```
  if (digitalRead(ENTRANCE_SENSOR_PIN) == HIGH &&
digitalRead(EXIT_SENSOR_PIN) == LOW) {
    lastEntranceSensorTriggerTime = currentMillis;
    if (vehicleDetected == false) {
      vehicleDetected = true;
      closeGate()
      Serial.println("Vehicle detected at the entrance");
    }
  }

  int scanResult = scanRFID();
  if (scanResult == 1) {
    openGate();
  } else if (scanResult == 0) {
    denyAccess();
  }
  // Check the exit sensor with debounce
  if (digitalRead(EXIT_SENSOR_PIN) == HIGH &&
digitalRead(ENTRANCE_SENSOR_PIN) == LOW) {
    lastExitSensorTriggerTime = currentMillis;
    if (vehicleDetected == true) {
      vehicleDetected = false;
      Serial.println("Vehicle detected at the exit");
      closeGate(); // Close gate when vehicle reaches exit sensor
    }
  }
}

int scanRFID() {
  if (!mfrc522.PICC_IsNewCardPresent() ||
!mfrc522.PICC_ReadCardSerial()) {
    return -1; // No card present
  }
  String uid = "";
  for (byte i = 0; i < mfrc522.uid.size; i++) {
    uid += String(mfrc522.uid.uidByte[i], HEX);
  }
  uid.toUpperCase();
  Serial.print("Card UID: ");
  Serial.println(uid);
  mfrc522.PICC_HaltA();

  return isAuthorized(uid) ? 1 : 0;
}

bool isAuthorized(String uid) {
```

```
  for (int i = 0; i < numAuthorizedCards; i++) {
    if (uid == authorizedCards[i].uid) {
      Serial.print("Welcome ");
      Serial.println(authorizedCards[i].name);
      return true;
    }
  }
  return false;
}

void openGate() {
  Serial.println("Access granted. Opening gate...");
  digitalWrite(GREEN_LED_PIN, HIGH);
  digitalWrite(RED_LED_PIN, LOW);
  gateServo.write(0); // Open gate
  gateOpen = true;

  delay(2000); // Keep the red LED on for 2 seconds

  digitalWrite(GREEN_LED_PIN, LOW);
}

void denyAccess() {
  Serial.println("Access denied.");
  digitalWrite(RED_LED_PIN, HIGH);
  digitalWrite(GREEN_LED_PIN, LOW);
  delay(2000); // Keep the red LED on for 2 seconds
  digitalWrite(RED_LED_PIN, LOW);
}

void closeGate() {
  if (gateOpen) {
    Serial.println("Closing gate...");
    gateServo.write(90); // Close gate
    gateOpen = false;
  }
}
```

8 Results:

Hardware Setup:



9 Conclusion:

The RFID-Based Vehicle Access Control System exemplifies a comprehensive, secure, and automated solution for managing vehicle entry and exit in restricted areas. By integrating RFID technology with IR sensors and a servo motor, the system ensures that only authorized vehicles gain access, significantly enhancing both security and operational efficiency. The use of Arduino Mega as the central controller simplifies the implementation and offers substantial flexibility for customization, making the system easily adaptable to various access control requirements. Throughout its development, the project has undergone rigorous testing and validation, proving its feasibility and effectiveness in real-world applications such as parking lots, gated communities, and secure facilities. Furthermore, this system reduces the need for manual supervision, minimizes human errors, and provides a reliable way to control access in secure environments. Looking ahead, potential enhancements could include real-time data logging for monitoring access patterns, remote control capabilities for administrators, integration with biometric verification for an added layer of security, and scalability to accommodate multiple entry and exit points, further extending its utility and reliability in diverse scenarios.