Module Code & Module Title

CS5068NI– Cloud Computing & IoT

"IoT-based RFID Door Unlock System"

Assessment Type

50% Group Report

Semester 2024-25 Autumn

Group Members

London Met ID	Student Name
23047371	Achyut Adhikari
22085531	Dipesh Dhital
20049126	Achal Dahal
23047552	Bishesh Aryal
23047358	Rupesh Mahato

Assignment Due Date: Tuesday, May 6, 2025

Assignment Submission Date: Tuesday, May 6, 2025

Submitted To: Sugat Man Shakya

Word Count: 2003

I confirm that I understand my coursework needs to be submitted online via MST under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Plagiarism check in TurnItIn

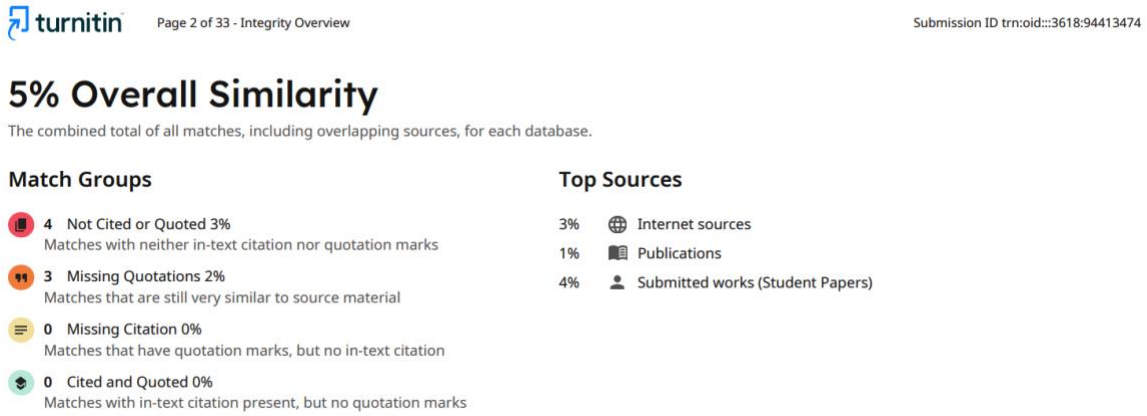

Figure 1: Plagiarism Check.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to all those who contributed to the successful completion of this RFID-Based Door Unlock System project.

First and foremost, we are deeply thankful to our lecturer, **Mr. Sugat Man Shakya**, for his invaluable guidance, insightful feedback, and continuous support throughout the project. His expertise and encouragement helped shape the direction of this work.

We extend our heartfelt appreciation to our tutor, **Mr. Ayush Bhakta Pradhanang**, for his patient mentorship, practical suggestions, and assistance in troubleshooting technical challenges during the implementation phase. His guidance was instrumental in refining the system's functionality.

We would also like to acknowledge our group members for their constructive discussions and motivation, which kept us inspired throughout the project duration.

ABSTRACT

This project presents the design and implementation of an IoT-based RFID Door Unlock System, which replaces traditional mechanical locks with a secure, automated access control solution. The system utilizes RFID technology for contactless authentication, granting access only to authorized users while maintaining a log of entry attempts.

A microcontroller (Arduino) processes data from an RC522 RFID reader to validate registered tags. Upon successful authentication, the system triggers a servo motor to open the door, accompanied by visual (LED) and auditory (buzzer) feedback.

The project demonstrates a cost-effective, scalable, and reliable alternative to conventional locks, addressing key security vulnerabilities such as key duplication and lack of access tracking.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

The Internet of Things (IoT) is a network of interconnected devices embedded with sensors, software, and connectivity to collect, process, and exchange data. These smart devices automate tasks, optimize operations, and improve decision-making with minimal human intervention. IoT enhances efficiency, enables real-time monitoring, and supports applications like smart homes, healthcare, agriculture, and urban infrastructure, driving innovation through data-driven insights and automation (al., 2013).

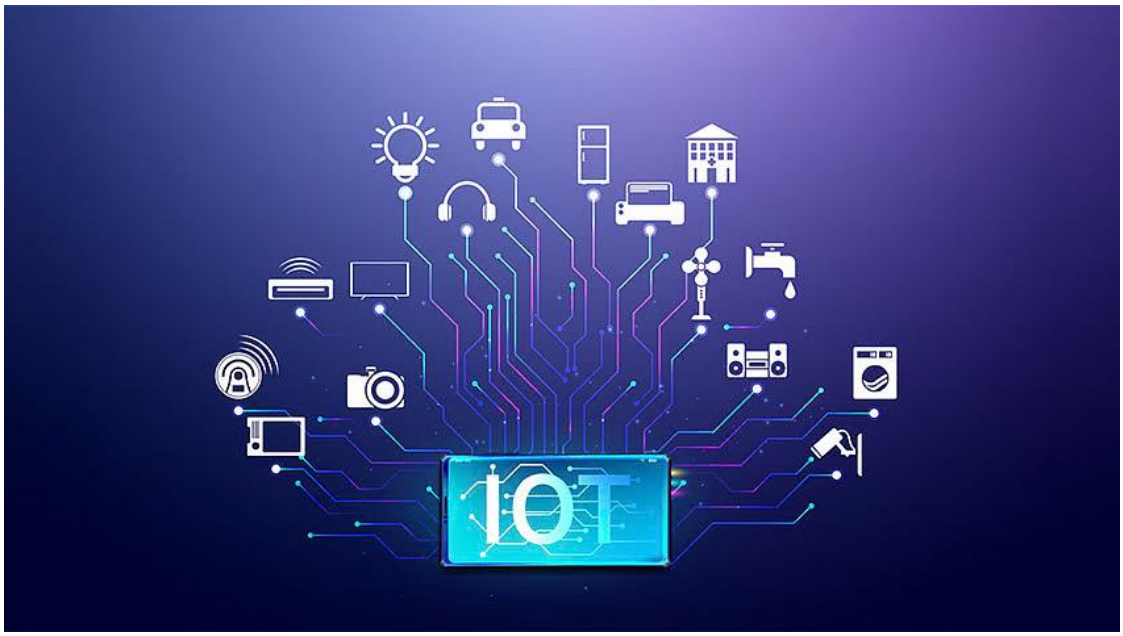

Figure 2: IoT Photo.

In today's rapidly evolving technological landscape, security remains a critical concern for homes, offices, and institutions. Traditional lock-and-key systems, while widely used, suffer from significant vulnerabilities such as key duplication, loss, and lack of access monitoring (Kumar et al., 2019). These weaknesses expose users to unauthorized entry, theft, and security breaches.

Figure 3: RFID Door Unlock Sample.

To address these challenges, modern access control systems such as biometric scanners, keypad locks, and RFID-based solutions are gaining traction. Among these, Radio Frequency Identification (RFID) technology offers a reliable, cost-effective, and scalable alternative (Want, 2006). RFID-based door access systems provide secure authentication, real-time monitoring, and remote management features that traditional locks cannot match.

This project proposes the development of an IoT-enabled RFID door unlock system, leveraging microcontroller technology to create a smart, automated security solution. By integrating an RFID reader (RC522) with an Arduino, and a servo motor the system ensures only authorized users gain access while logging entry attempts for enhanced security (Al-Fuqaha et al., 2015).

1.1 Current Scenario

Traditional lock-and-key mechanisms have been the standard for securing doors for decades. However, they suffer from several vulnerabilities:

- **Key Duplication:** Unauthorized key copying is a major security risk. According to a study by Statista, over 30% of burglaries involve the use of duplicated or stolen keys.
- **Lost Keys:** Misplaced keys lead to security breaches and costly lock replacements.
- **No Access Logs:** Mechanical locks do not track who enters or exits, making it difficult to monitor unauthorized access.

Figure 4: Graphical Representation of the data.

In contrast, electronic access control systems (like RFID, biometrics, and smart cards) are becoming increasingly popular due to their enhanced security and convenience. The global smart lock market is projected to grow from 2.3 billion in 2021 to 2.3 billion in 2021 to 6.8 billion by 2028, indicating a strong shift toward automated security solutions (Fortune Business Insights, 2022; MarketsandMarkets, 2021).

1.2 Problem Statement & Project as a Solution

1.1.1 Problem

Conventional locks lack authentication, tracking, and remote control, making them insecure and inefficient. Businesses and homeowners need a cost-effective, scalable, and secure alternative to traditional keys.

1.2.2 Solution

This project proposes an IoT-based RFID door unlock system that:

- Eliminates physical keys by using RFID-based authentication.
- Provides instant feedback (LEDs, buzzer) on access status.

1.3 Aim and Objectives

To design and implement a secure, automated RFID-based door unlock system that enhances access control by replacing traditional keys with contactless authentication, and improving security.

To achieve this aim, the project will fulfill the following measurable objectives:

- **Develop an RFID Authentication System**:
    - Use an RFID reader and tags to authenticate users. The reader scans the tag's unique ID, which is verified against a stored database of authorized IDs to grant or deny access.
- **Implement Door Lock Mechanism**:
    - Integrate an electronic lock (e.g., servo-based) controlled by a microcontroller. When the RFID system authenticates a valid tag, the microcontroller triggers the lock to open, allowing access.
- **Provide User Feedback**:
    - Include visual (LEDs, LCD display) and/or audible (buzzer) feedback to inform users of authentication status (e.g., green LED for success, red LED for failure) and system actions.

- **Ensure System Reliability**:
    - Use robust hardware, secure data storage, and error-handling software. Implement power backups, encryption for RFID communication, and regular maintenance to prevent failures and unauthorized access.

2 Background

An RFID door unlock system uses Radio Frequency Identification (RFID) technology to grant access through doors. It consists of an RFID reader, RFID tags (cards or fobs), and a control system. When an authorized tag is presented to the reader, it transmits a unique ID via radio waves, which the system verifies against a database. If valid, the door unlocks. These systems are widely used for secure, keyless entry in offices, homes, and restricted areas due to their convenience, scalability, and ability to track access. Basic versions emerged in the 1980s, evolving with improved encryption and integration with smart systems.

2.1 System Overview

An RFID Door Unlock System uses an RFID module (with tags), a Arduino, a relay, a solenoid lock, and jumper wires for secure access control. The RFID module scans tags, the arduino processes authentication, and the relay triggers the solenoid lock to unlock the door. A buzzer provides audio feedback (valid/invalid tag), while jumper wires interconnect components.This system eliminates physical keys, enhancing security with automated digital access control.

3 Design Diagrams

3.1 Block Diagram

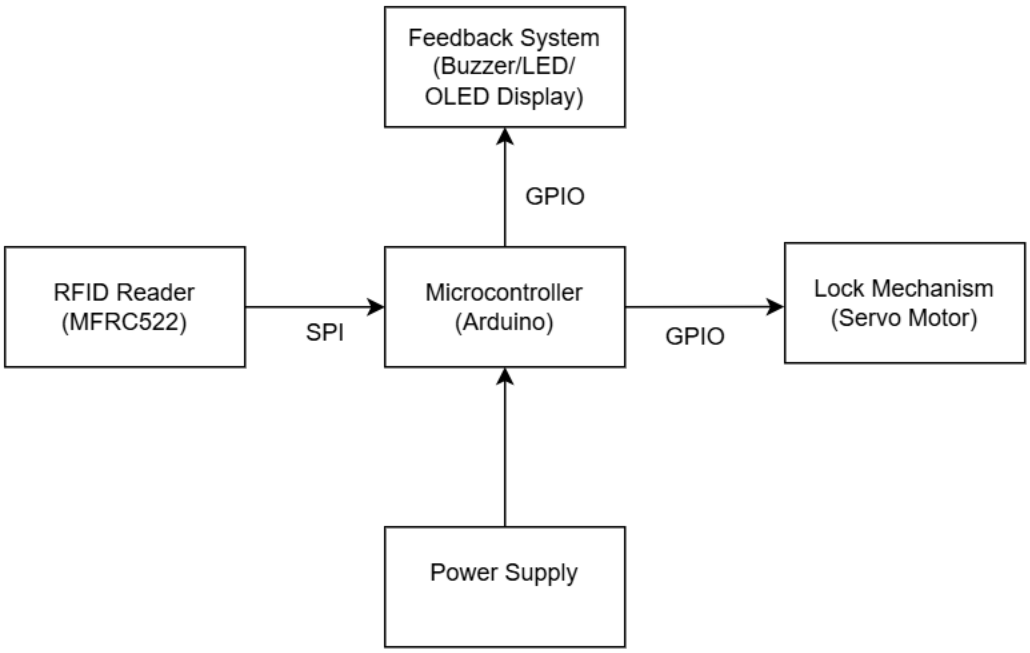

Figure 5: Block Diagram.

3.2 System Architecture

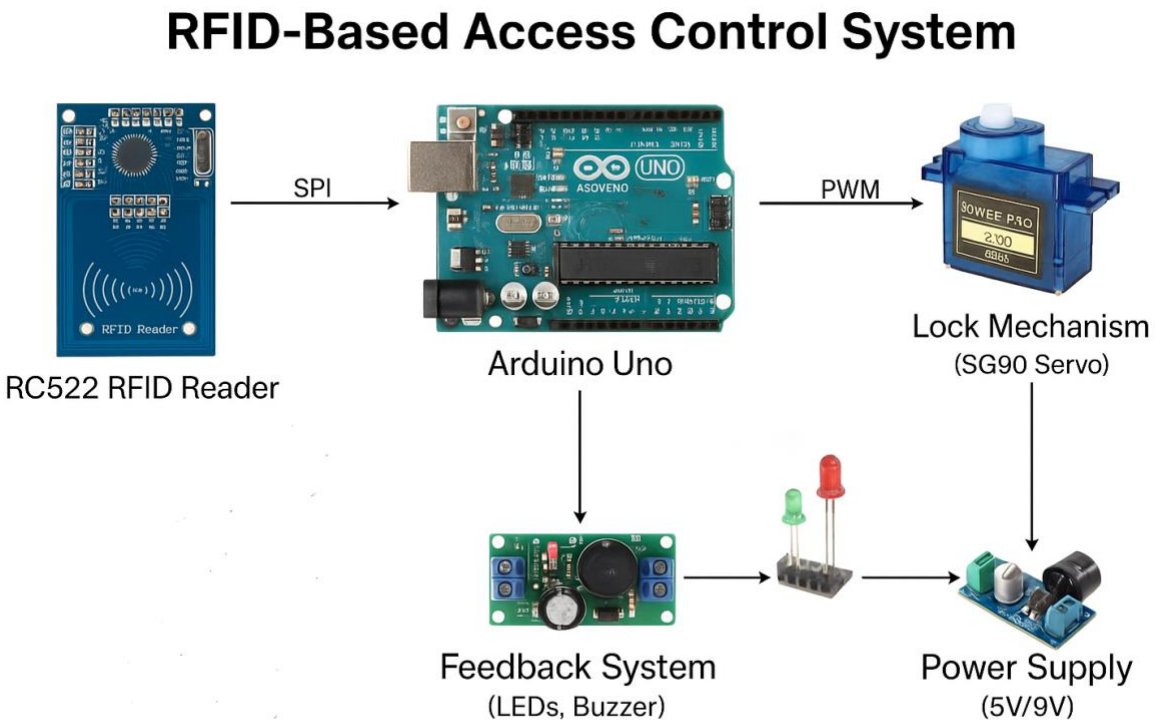

Figure 6: System Architecture.

3.3 Circuit Diagram

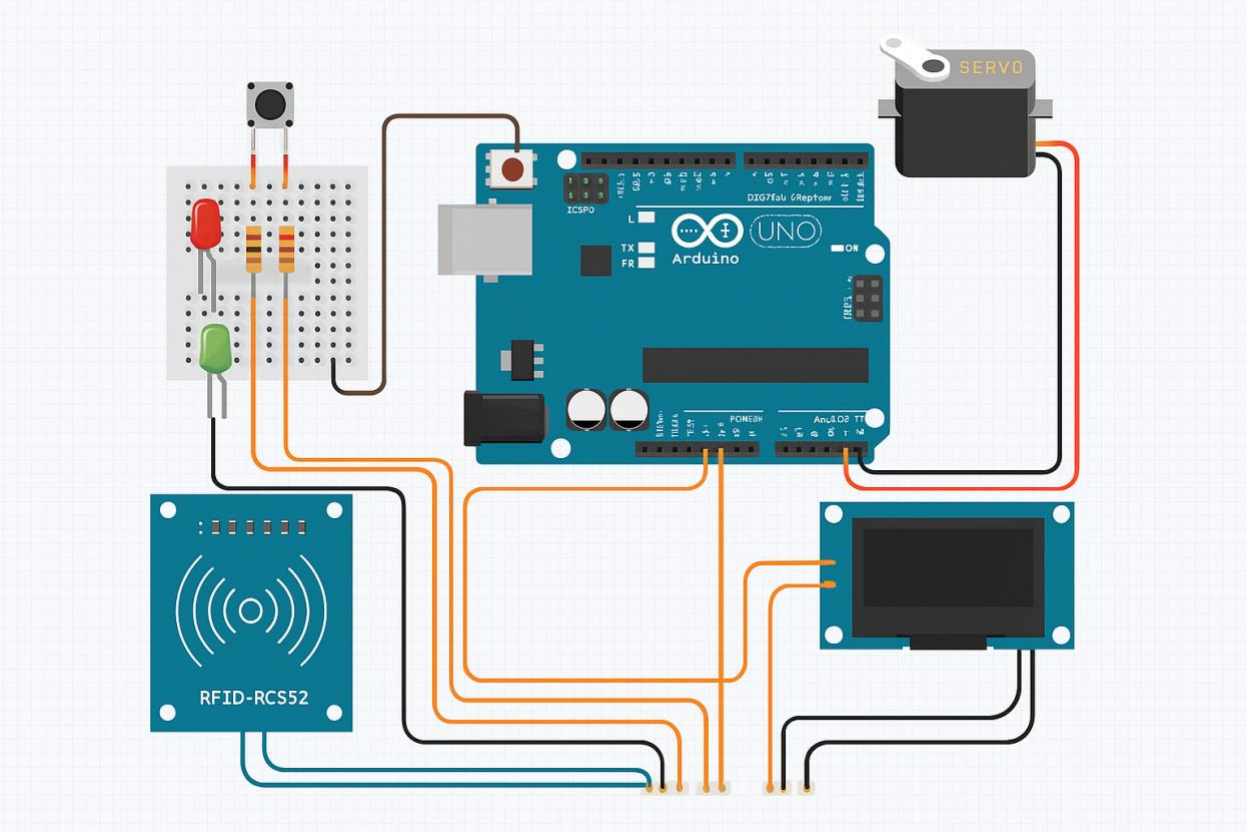

Figure 7: Circuit Diagram.

3.4 Flow Chart

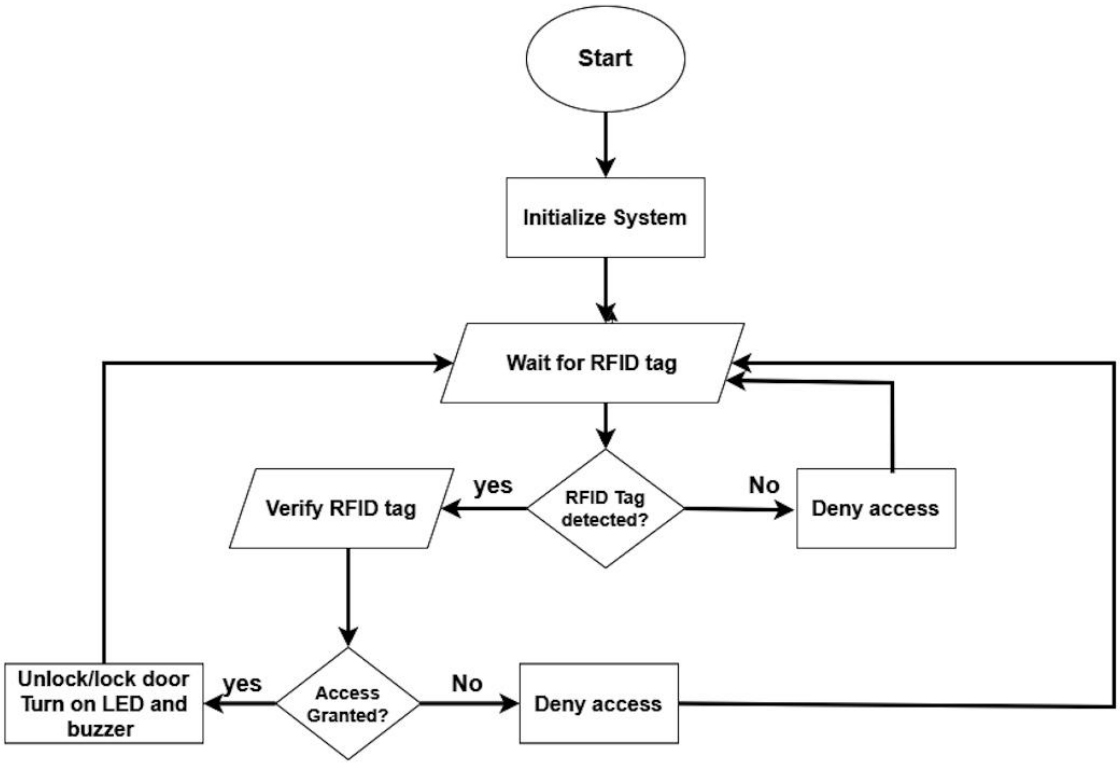

Figure 8: Flowchart diagram.

3.5 Schematic Diagram

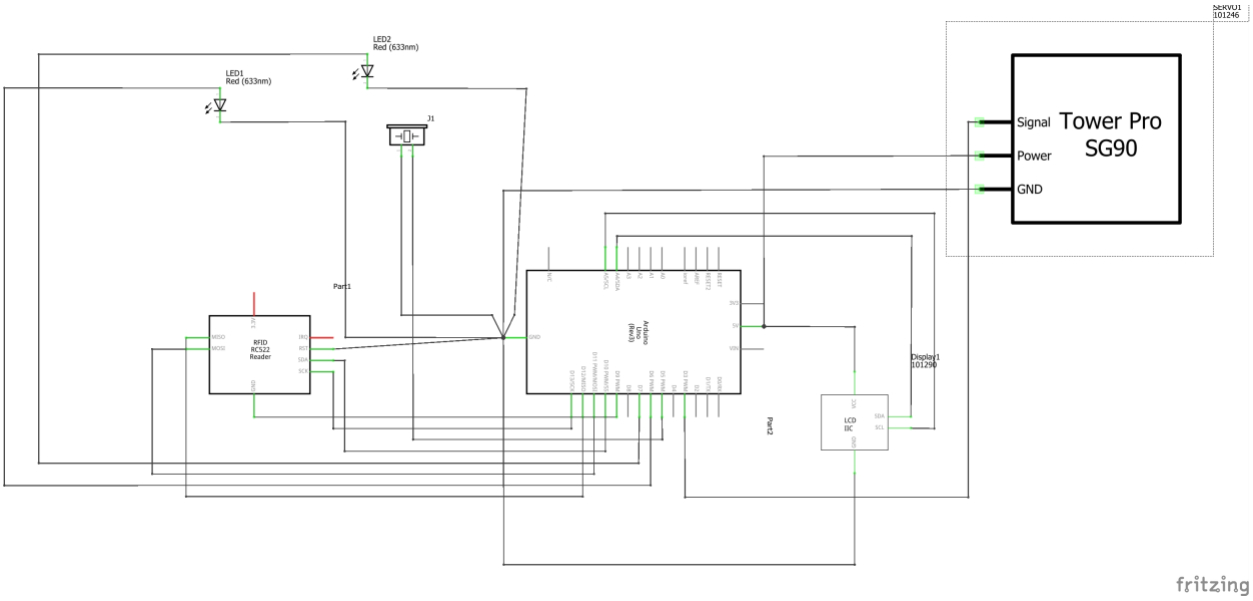

Figure 9: Schematic Diagram.

4 Requirement Analysis

4.1 Hardware Requirements

Component	Specification	Purpose
Microcontroller	Arduino Uno	Brain of the system, processes RFID data
RFID Reader	RC522 Module	Scans and verifies RFID tags
Lock Mechanism	SG90 Servo Motor	Physically unlocks the door
Feedback System	LEDs (Red/Green), Buzzer	Indicates access status
Power Supply	5V DC Adapter / 9V Battery	Powers the circuit

Table 1: Hardware Requirements.

6.1 IoT-Based RFID Door Unlock System

4.2 Software Requirements

Tools	Purpose
Arduino IDE	Programming the microcontroller

Table 2: Software Requirements.

4 Development

4.1 Wiring Details

RFID Module (MFRC522)

RFID Pin	Connect To Arduino
SDA	D10
SCK	D13
MOSI	D11
MISO	D12
GND	GND
RST	D9

OLED Display

OLED Pin	Connect To Arduino
VCC	5V
GND	GND
SCL	A5 (on UNO/Nano)
SDA	A4 (on UNO/Nano)

Servo Motor

Servo Wire	Connect To Arduino
Signal	D3
VCC	5V
GND	GND (same as Arduino GND)

Main Access Indicator LED

LED Leg	Connect To
Anode (+)	D7
Cathode (-)	GND

Invalid Access LED

LED Leg	Connect To
Anode (+)	D6
Cathode (-)	GND

Buzzer Wiring (Active Buzzer)

Buzzer Pin	Connect To Arduino
+ (VCC)	D5
– (GND)	GND

4.2 Phase 1: Planning and Analysis

Step 1: Initial Planning and Problem Identification

- Team brainstorming to identify a real-world, budget-friendly project.
- Chose the problem of physical door access security and inefficiency.
- Decided to develop an RFID-based access control system using Arduino UNO.

Step 2: Feasibility and Goal Setting

- Project goals: offline functionality, real-time feedback, cost-efficiency.
- Outlined required functionality: card detection, user identification, feedback through display, lights, and sound.

4.3 Phase 2: System Design

Step 3: System Architecture and Component Selection

- Designed the functional components:
    - RFID Module (MFRC522) for reading cards.
    - OLED Display for user messages.
    - Servo Motor to simulate door lock/unlock.
    - LEDs & Buzzer for visual and audible feedback.

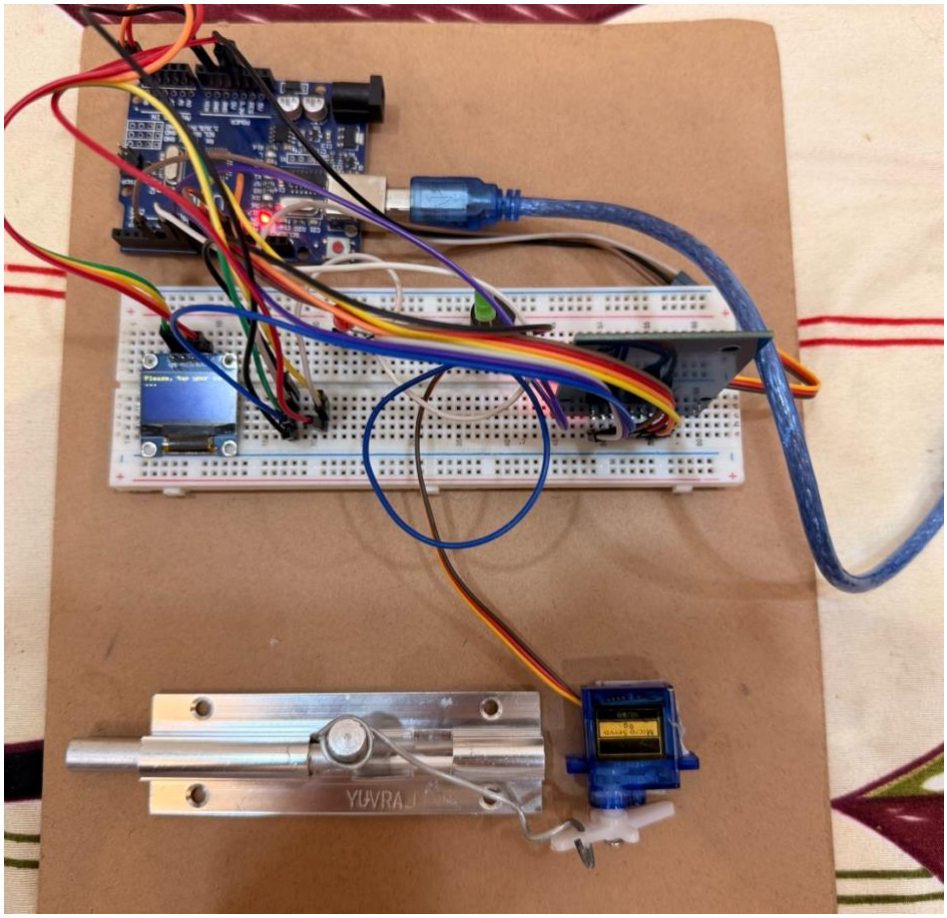

Figure 10: Prototype Design.

Step 4: Task Distribution and Role Assignment

- Team assigned roles for procurement, wiring, coding, and testing.
- Identified required hardware and libraries.

Step 5: Circuit Design and Wiring Plan

- Designed the circuit:
  - RFID via SPI
  - OLED via I2C (A4/A5)
  - Servo on PWM pin
  - LEDs and Buzzer on digital pins

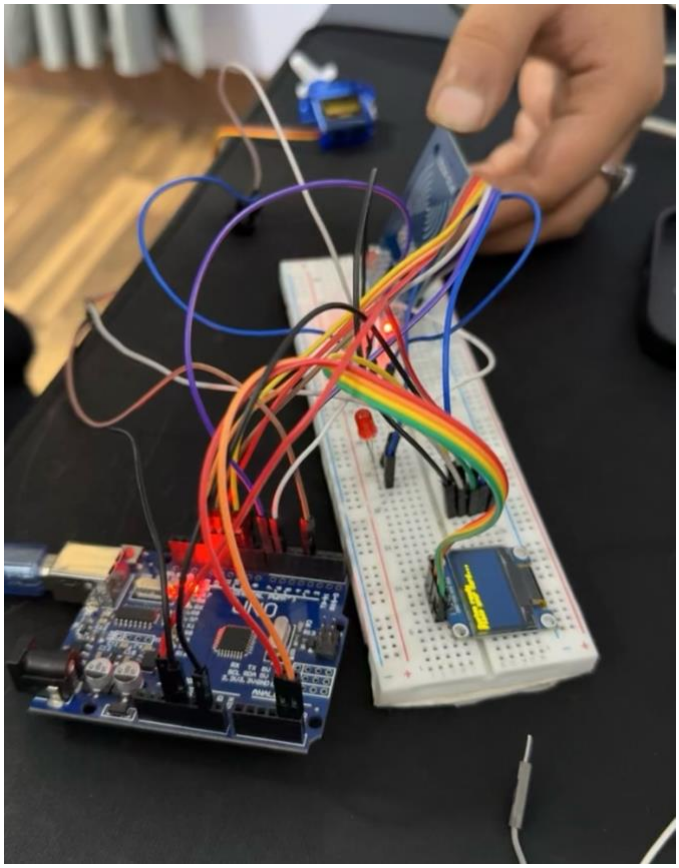

Figure 11: Wiring Plan.

4.4 Phase 3: System Development

Step 6: Assembly and Hardware Integration

- Procured components from college, local and online sources.
- Assembled all hardware on a breadboard based on the circuit design.

Step 7: Coding and Logic Implementation

- Programmed the Arduino to:
  - Detect RFID cards and read UID.
  - Validate UID against predefined authorized user.
  - Trigger servo motor, LEDs, and buzzer based on card status.
  - Display relevant messages on the OLED screen.

```
// Servo and LED
Servo servo;
const int ledPin = 7;  // LED connected to digital pin 7

// Allowed UID
String UID = "33 F6 23 10";
byte lock = 0;

void setup() {
  Serial.begin(9600);
  servo.attach(3);
  servo.write(70);
  pinMode(ledPin, OUTPUT);      // Set LED pin as output
  digitalWrite(ledPin, LOW);    // Turn LED OFF initially

  SPI.begin();
  rfid.PCD_Init();
\
  // Initialize OLED
  if (!display.begin(SSD1306_SWITCHCAPVCC, 0x3C)) {
    Serial.println(F("OLED failed"));
    for (;;);
  }
```

Figure 12: Program for validating the correct user.

4.5 Phase 4: Testing and Debugging

Step 8: System Testing and Validation

- Programmed valid UID (e.g., **33 F6 23 10** for Achyut Adhikari).
- Performed tests with:
    - Valid cards: unlocked with green LED and welcome message.
    - Invalid cards: remained locked, red LED lit, “Invalid Card” displayed.
- Used Serial Monitor for debugging and real-time UID verification.

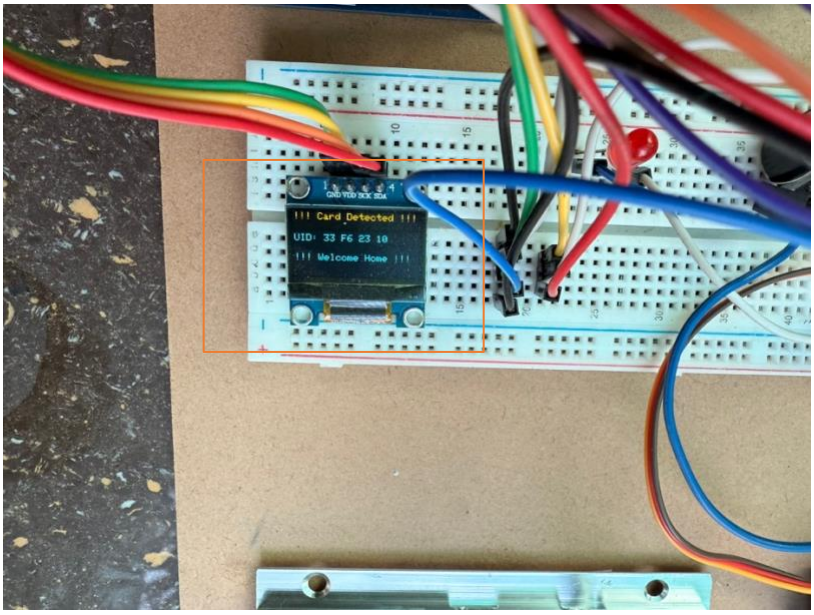

Figure 13: Programmed Valid UID.

Step 9: Code Refinement and Stability Checks

- Tested with multiple scans to ensure:
  - No response delays
  - Stable servo operation
  - Accurate feedback on OLED and through LEDs/buzzer

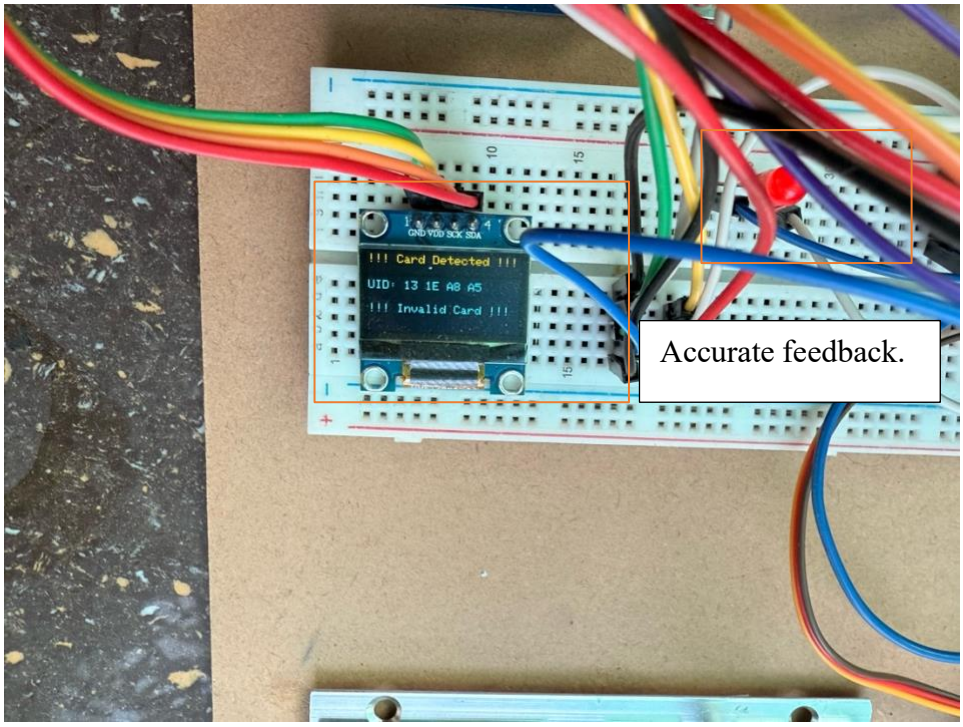

Figure 14: Stability Check.

4.6 Phase 5: Results and Evaluation

Step 10: Final Results and Observations

- System operated reliably offline.
- Accurately handled user identification.
- Delivered immediate, clear feedback.
- Met the project's goal of a low-cost, effective access control system.

5 Testing

5.1 Test 1: Authorized card test

Objective	To verify that the door unlocks when an authorized RFID card is scanned.
Action	Scan a registered RFID card on the reader.
Expected Result	OLED displays “Welcome Home”, servo unlocks the door, green LED along with buzzer lights up.
Actual Result	OLED displayed “Welcome Home”, servo unlocked, and green LED along with buzzer turned on.
Conclusion	The test was performed successfully.

Table 3: Authorized Card Test.

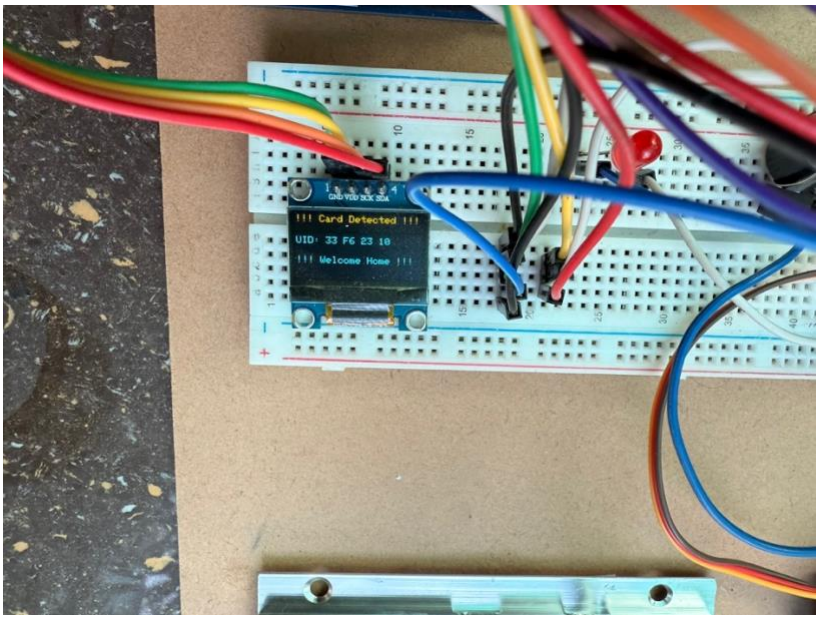

Figure 15: Authorized Card Test.

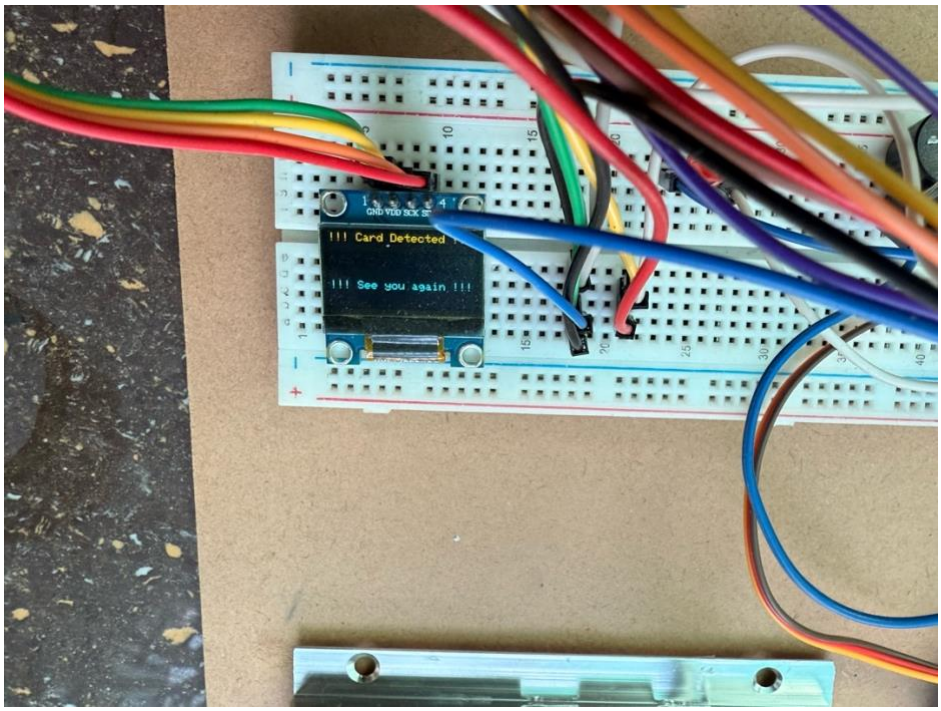

Figure 16: Authorized Card Test.

5.2 Test 2: Unauthorized card test

Objective	To verify that the system give access to unregistered RFID cards.
Action	Scan an unregistered RFID card.
Expected Result	OLED displays **"Welcome Home",** servo unlocks the door, green LED along with buzzer lights up.
Actual Result	OLED displayed **"Invalid Card",** door stayed locked, red LED turned on.
Conclusion	The test was performed **unsuccessfully**.

Table 4: Unauthorized Card Test.

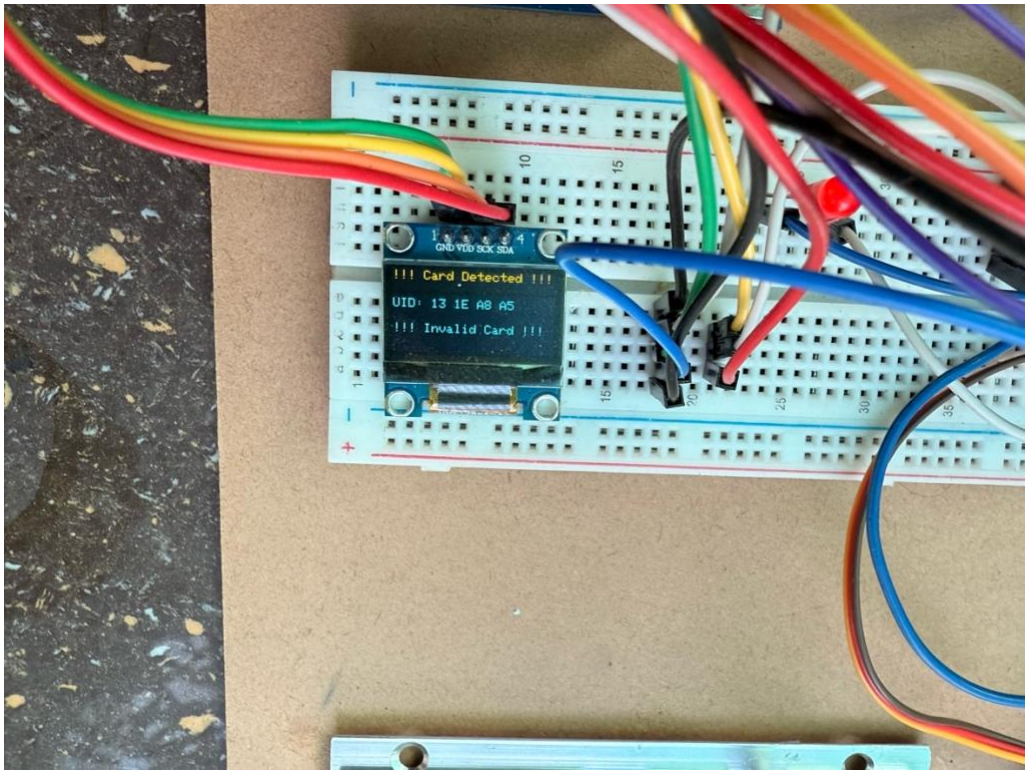

Figure 17: Unauthorized Card Test.

5.3 Test 3: Distance and Orientation Sensitivity

Objective	To determine the effective scanning range and angle for the RFID reader.
Action	Scan a valid card at varying distances and angles.
Expected Result	Reader detects card within 3–5 cm and at direct or slight tilt angles.
Actual Result	Card was detected up to 4 cm at several angles; worked best when aligned.
Conclusion	The test was performed successfully.

Table 5: Distance and Orientation Sensitivity.

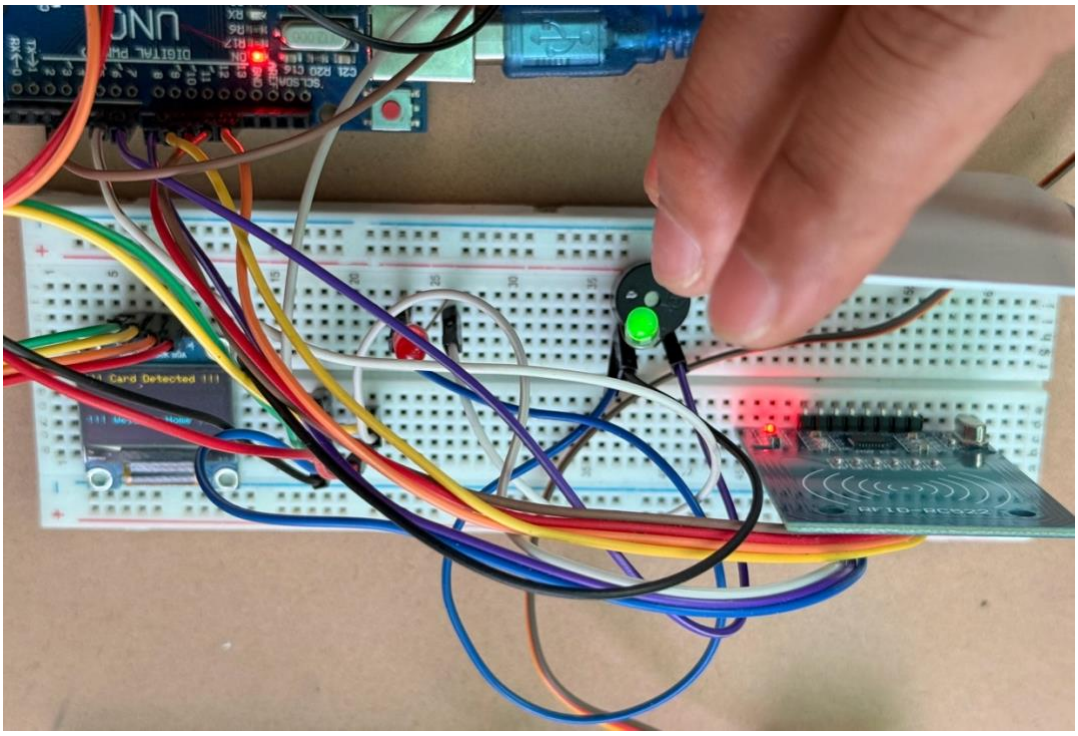

Figure 18: Distance Sensitivity Test.

5.4 Test 4: Power Failure and Recovery

Objective	To check system behavior after power loss and restoration.
Action	Power off the Arduino, then power it back on and scan a valid card.
Expected Result	System should reboot normally and recognize valid cards.
Actual Result	System restarted correctly and recognized authorized card.
Conclusion	The test was performed successfully.

Table 6: Power Failure and Recovery.

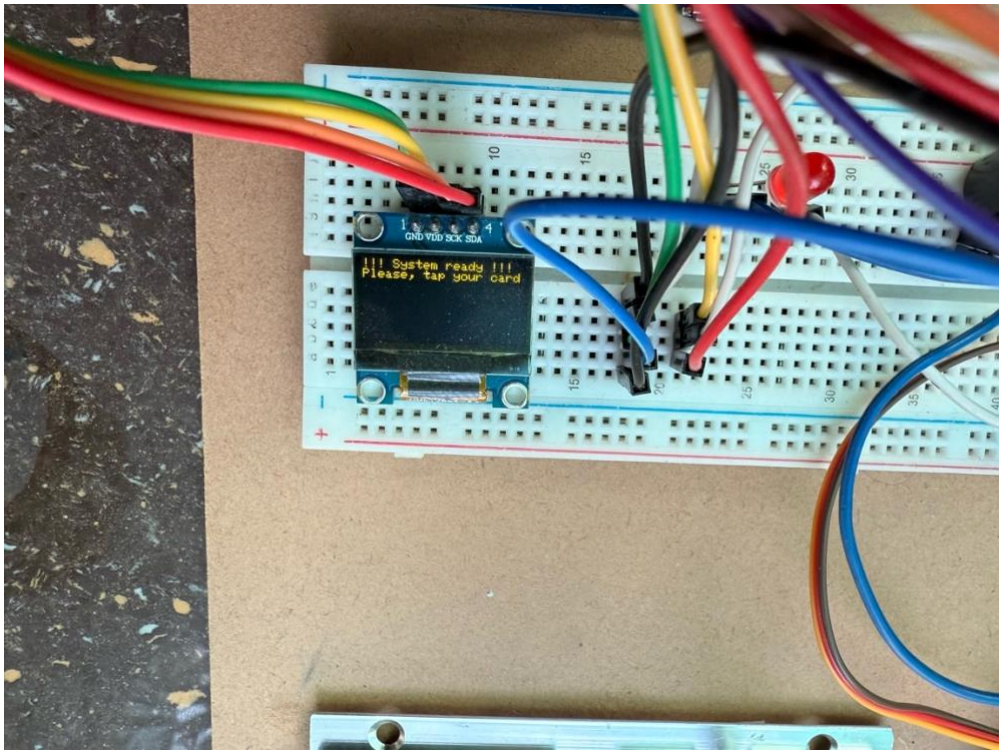

Figure 19: Power Failure and Recovery Test.

5.5 Test 5: Multiple Card Reads / Rapid Scanning

Objective	To ensure the system handles multiple rapid scans correctly.
Action	Scan several RFID cards (authorized and unauthorized) rapidly.
Expected Result	System should correctly process each card without freezing or misbehaving.
Actual Result	All scans processed correctly, with accurate messages for each case.
Conclusion	The test was performed successfully.

Table 7: Multiple Card Reads / Rapid Scanning.

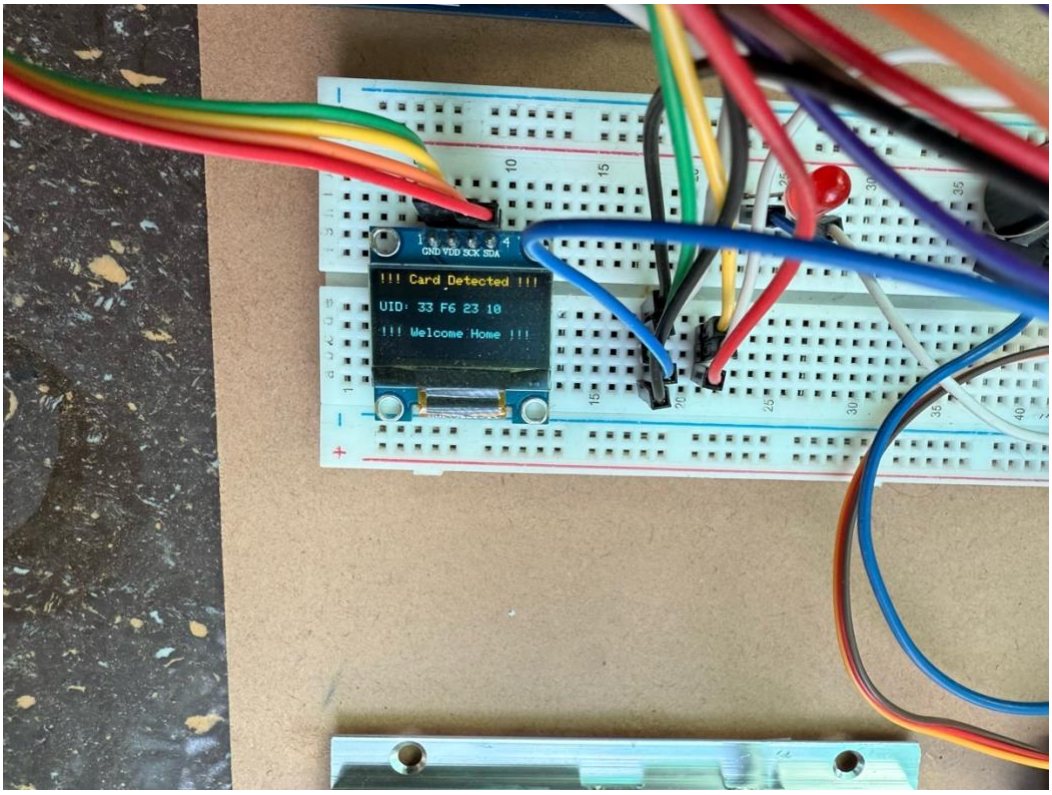

Figure 20: Rapid Card Test.

6 Conclusion

The IoT-based RFID Door Unlock System presents a functional and secure replacement for conventional mechanical locks. By combining RFID technology with microcontroller processing, the system provides contactless authentication. The implementation offers several key benefits: elimination of physical key vulnerabilities through digital authentication, automated door control via servo mechanism with status indicator. The solution demonstrates cost-efficiency through its use of affordable components while remaining scalable for broader applications.

This project successfully establishes a practical foundation for smart access control systems, suitable for residential, commercial, and institutional use. The design approach provides a template for future developments in IoT security systems, with potential for integration of additional features like biometric verification or remote access management. The system represents a meaningful step forward in modernizing physical security infrastructure.

7 Bibliography

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M., 2015. *Internet of Things: A survey on enabling technologies, protocols, and applications*. IEEE Communications Surveys & Tutorials, 17(4), pp.2347–2376.

Want, R., 2006. *An introduction to RFID technology*. IEEE Pervasive Computing, 5(1), pp.25–33.

Kumar, S., Tiwari, P. and Zymbler, M., 2019. *Internet of Things is a revolutionary approach for future technology enhancement: A review*. Journal of Big Data, 6(1), pp.1–21.

Fortune Business Insights, 2022. *Smart lock market size, share & COVID-19 impact analysis, by type (deadbolts, lever handles, padlocks, and others), by technology (Wi-Fi, Bluetooth, and others), by end-user (residential, hospitality, commercial, and others), and regional forecast, 2021–2028*. [online] Report No. 101725. Available at: https://www.fortunebusinessinsights.com [Accessed 4 May 2025].

8 Appendix

8.1 IoT-Based RFID Door Unlock System

8.1.1 Component Details

Microcontroller (Arduino Uno)

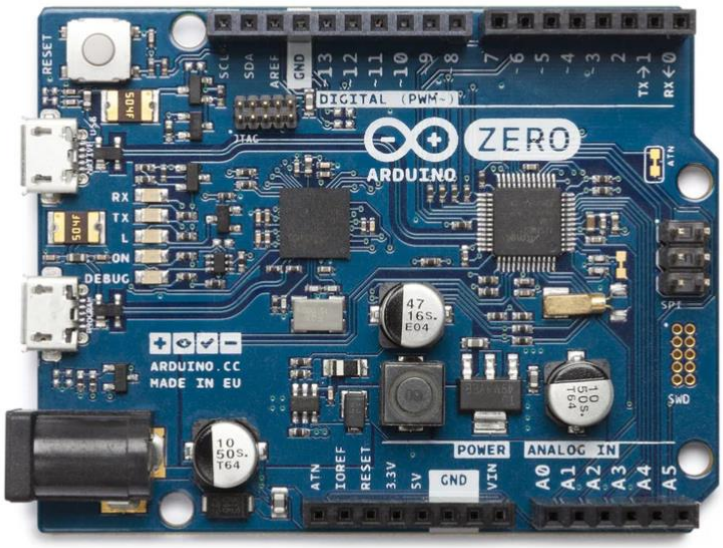

Figure 21: Arduino Uno.

Function: The Arduino acts as the central processing unit of the system. It reads data from the RFID reader, processes the tag information, checks it against the authorized list, and sends commands to actuators (like servo motors) to lock or unlock the door. It also handles outputs to the OLED display and LED indicators.

RFID Reader (RC522 Module)

Figure 22: RFID Reader.

Function: Scans and verifies RFID tags/cards for authentication.

Key Features:

Works at 13.56 MHz frequency.

Range: ~5 cm (contactless).

Lock Mechanism (SG90 Servo)

Figure 23: Lock Mechanism.

Function: Physically locks/unlocks the door.

Key Features:

Silent, precise movement (best for lightweight doors).

Feedback System (LEDs + Buzzer)

Figure 24: LED Buzzer.

Function: Provides visual/audio feedback on access status.

Indicators:

Green LED + Beep: Access granted.

Red LED + Long Beep*:* Access denied.

Power Supply (5V Adapter / 9V Battery)

Figure 25: Power Supply.

Function: Powers the circuit.

Options:

5V DC Adapter*:* Stable for continuous use.

9V Battery: Portable but less durable.

8.2 Code for Programming Adruino

```
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>
#include <Wire.h>
#include <Adafruit_GFX.h>
#include <Adafruit_SSD1306.h>

// RFID Pins
#define SS_PIN 10
#define RST_PIN 9
MFRC522 rfid(SS_PIN, RST_PIN);

// OLED Display Settings
#define SCREEN_WIDTH 128
#define SCREEN_HEIGHT 64
#define OLED_RESET -1
Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, OLED_RESET);

// Servo and LED
Servo servo;
const int ledPin = 7;  // LED connected to digital pin 7

// Allowed UID
String UID = "33 F6 23 10";
byte lock = 0;

void setup() {
  Serial.begin(9600);
  servo.attach(3);
  servo.write(70);
  pinMode(ledPin, OUTPUT);      // Set LED pin as output
  digitalWrite(ledPin, LOW);    // Turn LED OFF initially

  SPI.begin();
  rfid.PCD_Init();
\
  // Initialize OLED
  if (!display.begin(SSD1306_SWITCHCAPVCC, 0x3C)) {
    Serial.println(F("OLED failed"));
    for (;;);
  }

  display.clearDisplay();
  display.setTextSize(1);
  display.setTextColor(WHITE);
```

```
  display.setCursor(0, 0);
  display.println("!!! System ready !!!");
  display.println("Please, tap your card...");
  display.display();
}

void loop() {
  if (!rfid.PICC_IsNewCardPresent()) return;
  if (!rfid.PICC_ReadCardSerial()) return;

  display.clearDisplay();
  display.setCursor(0, 0);
  display.println("!!! Card Detected !!!");
  display.display();

  String ID = "";
  for (byte i = 0; i < rfid.uid.size; i++) {
    if (i > 0) ID.concat(" ");
    ID.concat(String(rfid.uid.uidByte[i], HEX));
    delay(100);
  }
  ID.toUpperCase();

  Serial.print("Scanned UID: ");
  Serial.println(ID);

  display.setCursor(0, 20);
  display.print("UID: ");
  display.println(ID);
  display.display();

  if (ID == UID && lock == 0) {
    digitalWrite(ledPin, HIGH);   // 🔘 Turn ON LED
    servo.write(70);              // Lock door
    display.setCursor(0, 40);
    display.println("!!! See you again !!!");
    display.display();
    delay(1500);
    digitalWrite(ledPin, LOW);    // 🔘 Turn OFF LED
    lock = 1;
  }
  else if (ID == UID && lock == 1) {
    digitalWrite(ledPin, HIGH);   // 🔘 Turn ON LED
    servo.write(160);             // Unlock door
    display.setCursor(0, 40);
    display.println("!!! Welcome Home !!!");
    display.display();
    delay(1500);
```

```
  digitalWrite(ledPin, LOW);   // 🔘 Turn OFF LED
  lock = 0;
 }
 else {
 digitalWrite(6, HIGH);   // 🔘 Turn ON Red LED
 display.setCursor(0, 40);
 display.println("!!! Invalid Card !!!");
 display.display();
 delay(1500);
 digitalWrite(6, LOW);
 }

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

 display.clearDisplay();
 display.setCursor(0, 0);
 display.println("Please, tap your card...");
 display.display();
}
```