CS5054NI Advanced Programming and Technologies

50% Group Coursework

Submission: Milestone 1

RFID – Based Door Lock System

Academic Semester: Spring Semester 2025

Credit: 15 credit semester long module

Group Name:			
SN	**Student Name**	**College ID**	**University ID**
1	**Sayam Rai**	**np01nt4a230179**	**23047491**
2	**Stuti Timilsina**	**np01nt4a230154**	**23047477**
3	**Sushant Chaudhary**	**np01nt4a230169**	**23047494**
4	**Chirag K.C.**	**np01nt4a230165**	**23047488**
5	**Siddartha Amatya**	**np01nt4a230113**	**23047409**

Website Link: https://srituhobby.com/how-to-make-a-rfid-door-lock-with-arduino/

Assignment Due Date: 15th May 2025

Assignment Submission Date: 15th May 2025

I confirm that I understand my coursework needs to be submitted online via MST Classroom 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.

23047409_SiddarthaAmatya_L2N7_Team3.docx

Islington College,Nepal

Document Details

Submission ID
trn:oid:::3618:95998766

Submission Date
May 15, 2025, 12:18 PM GMT+5:45

Download Date
May 15, 2025, 12:19 PM GMT+5:45

File Name
23047409_SiddarthaAmatya_L2N7_Team3.docx

File Size
35.6 KB

29 Pages
5,113 Words
29,286 Characters

turnitin Page 1 of 34 - Cover Page Submission ID trn:oid:::3618:95998766

turnitin Page 2 of 34 - Integrity Overview Submission ID trn:oid:::3618:95998766

11% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

51 Not Cited or Quoted 10%
Matches with neither in-text citation nor quotation marks

7 Missing Quotations 2%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

3% Internet sources
1% Publications
10% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

turnitin Page 3 of 34 - Integrity Overview Submission ID trn:oid:::3618:95998766

Match Groups

51 Not Cited or Quoted 10%
Matches with neither in-text citation nor quotation marks

7 Missing Quotations 2%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

3% Internet sources
1% Publications
10% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1 Submitted works
INTI Universal Holdings SDM BHD on 2025-04-20 2%

2 Submitted works
Jabatan Pendidikan Politeknik Dan Kolej Komuniti on 2024-11-10 <1%

3 Submitted works
islingtoncollege on 2025-01-23 <1%

4 Submitted works
islingtoncollege on 2025-01-23 <1%

5 Submitted works
The Manchester College on 2024-05-22 <1%

Acknowledgement

We would like to express our sincere gratitude to our instructor, Mr. Sugat Man Shakya, for his continuous support, valuable insights, and expert guidance throughout the development of this project. His encouragement and constructive feedback have played a vital role in shaping the final outcome of our work.

We are also thankful to London Metropolitan University for providing an excellent academic environment and access to essential resources that enabled us to conduct this project effectively. The academic framework and technical infrastructure have been instrumental in facilitating our research and development process.

Lastly, we extend our heartfelt appreciation to one another as team members for the spirit of collaboration, dedication, and mutual support throughout the project. Each member's contribution and active participation made this group work a successful and enriching experience.

Abstract

This project presents the design and implementation of an RFID-based door lock system that integrates Internet of Things (IoT) technologies to enhance security through contactless access control. The system utilizes the Arduino Uno microcontroller, the RFID-RC522 reader, a micro servo motor, and a 16x2 LCD display to verify user identity and control physical access based on stored RFID credentials. The core functionality involves scanning RFID tags, comparing them against predefined authorized identifiers, and activating a locking mechanism accordingly.

The project was developed in three phases: mechanical assembly, electronic integration, and software programming. Extensive testing was conducted to validate performance across multiple scenarios, including authorized access, unauthorized attempts, and system response accuracy. The system consistently performed as expected, displaying appropriate messages and executing servo movements based on tag verification.

This project not only fulfills the objective of developing a functional, low-cost security system but also contributes to the broader application of IoT in physical access management. Its scalability, affordability, and adaptability make it suitable for educational institutions, offices, and residential buildings. By bridging theoretical knowledge with hands-on implementation, the project demonstrates the practical value of embedded systems and highlights the growing role of IoT in shaping modern, secure infrastructure.

Table of Contents

Table of Figures

Table of Tables

1. Introduction

1.1 Introduction to Internet of Things

The Internet of Things (IoT) allows intelligent devices to automatically connect and exchange data without human intervention, improving quality of life via progress in healthcare, education, transportation, and resource management. Termed by Kevin Ashton in 1999, the IoT has quickly expanded, with the number of connected devices increasing from 12.5 billion in 2010 to over 25 billion by 2020 . These advancements allow systems to become more responsive, adaptive, and capable of functioning with minimal human input, thereby improving safety, convenience, and data accuracy across various domains.

One practical example of IoT in action is the RFID-Based Door Lock system, a dual-layer security mechanism that incorporates both RFID technology and password verification to enhance entry control. Operated by the Arduino Uno microcontroller, this setup exemplifies time-managed automation and secure access through electronic credentials. It not only prevents unauthorized access but also serves as an educational platform for students and developers to engage in real-world applications of programming, circuit design, and security systems. Such IoT-based systems offer valuable hands-on experience, bridging theoretical knowledge with practical implementation, and contributing to the development of future-ready technical skills in automation and cybersecurity. (Jordi Salazar, 2017)

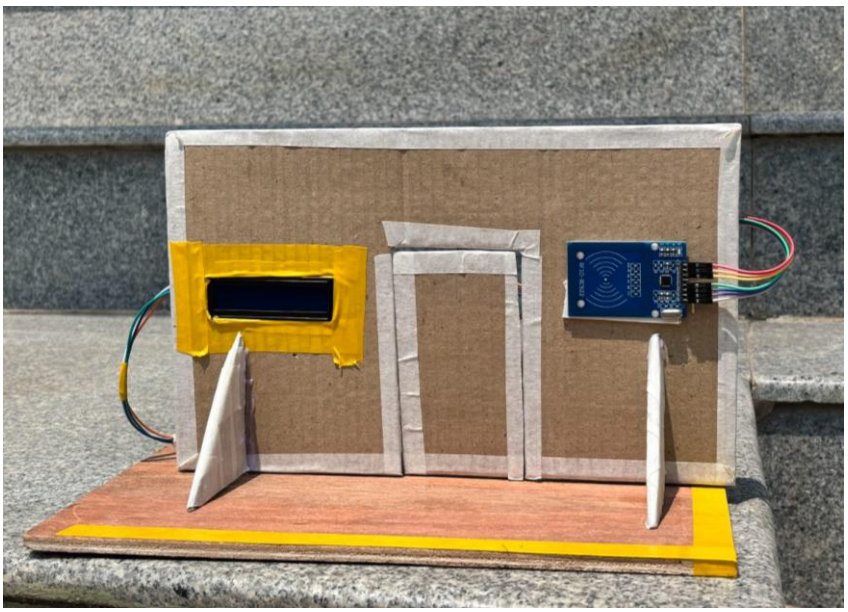

Figure 1 RFID Based door lock system.

1.2 Current Scenario

Door locking mechanisms in commercial and industrial settings have evolved from purely mechanical systems to sophisticated electronic access controls. In the 18th–19th centuries, mechanical key-and-tumbler locks became widespread with mass production, securing homes and businesses. With the Industrial Revolution in the late 18th century, home security has always depended on traditional mechanical locks and keys system (Alghamdi, 2020). These conventional methods, although widely used for decades, were often prone to issues such as lost keys, unauthorized duplication, and lock-picking. (Paranagama, 2022)

In Nepal's commercial and industrial sectors, conventional mechanical locks remain the default choice. Most businesses secure doors with padlocks, cylinder locks, or deadbolts operated by physical keys, reflecting broader technology gaps. Industry surveys suggest that nearly half of Nepal's firms face obstacles when adopting new systems (Devkota, 2021). One study bluntly found that Nepali industries "are not ready for I4.0" because they lack even basic enabling technologies (Rajbhandari, 2022). Despite these technologies, adoption of electronic or RFID-based locks in Nepal is extremely limited. High cost is a primary barrier as smart locks can cost on the order of $150–$300 putting them out of reach for most businesses (Market Data Forecast logo, 2024). Infrastructure shortcomings also impede use: erratic power and limited internet in many industrial areas make digital access systems impractical. Indeed, analysts have identified "lack of infrastructure" and related issues as top obstacles to technology adoption in Nepal's factories (Rajbhandari, 2022).

In Nepal, adoption of RFID-based door locks is still very limited. Surveys of Nepalese industry report that most firms are currently "not ready" to implement Industry 4.0 technologies citing a lack of skilled manpower, infrastructure and policy support (Rajbhandari, 2022). Consistent with this, one study found that roughly 97% of Nepali manufacturers were not using RFID at all in their operations (Rajbhandari, 2022). By extension, RFID door access systems remain rare in most commercial and industrial buildings as they continue to rely on mechanical locks or basic electronic keypads. Only selected high-end projects have adopted RFID or smart locking solutions, typically where higher budgets permit. Overall, while RFID locks offer clear global advantages with contactless access, easy management, auditability, their impact in Nepal is currently modest. Wider adoption will depend on improvements in local technical capability, supportive security standards, and cost reductions before such systems become commonplace. (Rajbhandari, 2022)

1.3 Problem Statement and Project as a solution

In many Nepalese industrial and commercial facilities, access is still controlled by conventional mechanical door locks and physical keys. Such key-based systems suffer from well-known security and management problems. Keys are easily lost or stolen which typically forces expensive key duplication or replacement of affected locks. An industry survey reports that over 80% of security professionals view lost keys as a serious risk to facility security as an ordinary key can be illicitly copied without authorization (Bannister, 2016). Moreover, mechanical lock-and-key systems provide no automatic audit trail, and administrators must manually track all issued keys and physically change locks if any key is compromised. Together, these factors make traditional lock systems complex to manage and vulnerable to unauthorized entry in commercial and industrial settings. (CDC, 2020)

An Arduino-based RFID door lock system can address these limitations. In an RFID-access setup, employees carry programmable RFID tokens instead of physical keys, and a microcontroller validates each token before unlocking the door. This means lost or stolen tags can simply be disabled in software without rekeying the door, and new tags can be issued as needed. In practice, such RFID-controlled locks have been shown to be low-cost yet reliable solutions for secure access (Sharma, 2022). Only individuals with authorized RFID cards are granted access, and each scan is recorded by the controller, creating a real-time log of entry activity. Unlike traditional keys, RFID credentials are difficult to duplicate, as each tag carries a unique identifier managed through a centralized system. This setup enables authentication, authorization, and accountability by verifying user identity, granting access based on predefined permissions, and maintaining detailed entry records. By digitizing access and tracking all interactions, the Arduino-based RFID system effectively overcomes the limitations of mechanical locks offering enhanced security, precise credential management, and reliable auditability. (Sharma, 2022)

1.4 Aim and Objectives

The primary aim of this project is to design and implement an RFID-based door lock system using Arduino that enhances physical security through contactless authentication. The system is intended to replace conventional key-based locking mechanisms with a reliable, programmable, and low-cost access control solution suitable for residential, institutional, and commercial applications.

Objectives:

- To develop a functional prototype of an RFID-enabled door locking system using the Arduino Uno microcontroller.
- To integrate RFID authentication for verifying user identity and granting access only to authorized cards.
- To create a secure access control logic that accurately identifies authorized RFID tags, denies unregistered entries, and maintains consistent system performance.
- To conduct systematic testing of the system under multiple scenarios, including valid access, invalid access, and lock re-engagement, in order to validate stability and reliability.
- To evaluate the scalability, affordability, and potential for local adaptation of RFID-based access control systems in the context of Nepal's infrastructure and technological readiness.
- To demonstrate the potential applications of the system in sectors such as security, healthcare, and finance, emphasizing adaptability and scalability.

2. Background

2.1 System Overview

This project is an RFID-based door lock system built using Arduino UNO, designed to allow access only to users with authorized RFID cards. It combines elements of embedded systems and basic IoT to create a simple, effective security solution for doors. When the system is powered on, it initializes all the connected components including the RFID-RC522 reader, a micro servo motor, and a 16x2 LCD display with an I2C interface. The LCD displays a default welcome or instruction message, prompting the user to scan their card. Each component is powered and grounded appropriately using Arduino's power pins, ensuring the system remains compact and energy efficient. This makes the system user-friendly and ideal for applications such as home security, office entry control, or school lab access systems.

When an RFID card is brought close to the reader, the RC522 module captures its UID and sends it to the Arduino via SPI. The Arduino then compares the received UID with a list of authorized UIDs stored in its memory. If a match is found, it sends a signal to the servo motor to rotate from 0° to 90°, simulating the unlocking of a door. Simultaneously, the LCD displays "Access Granted." After a short delay, the servo returns to its locked position and the LCD resets to the welcome message. If the UID does not match, the servo remains in the locked position, and the LCD shows "Access Denied." This feedback loop continues for every scanned card, ensuring the door remains secure and responsive only to approved users.

2.2 Design Diagram

2.2.1 Block Diagram

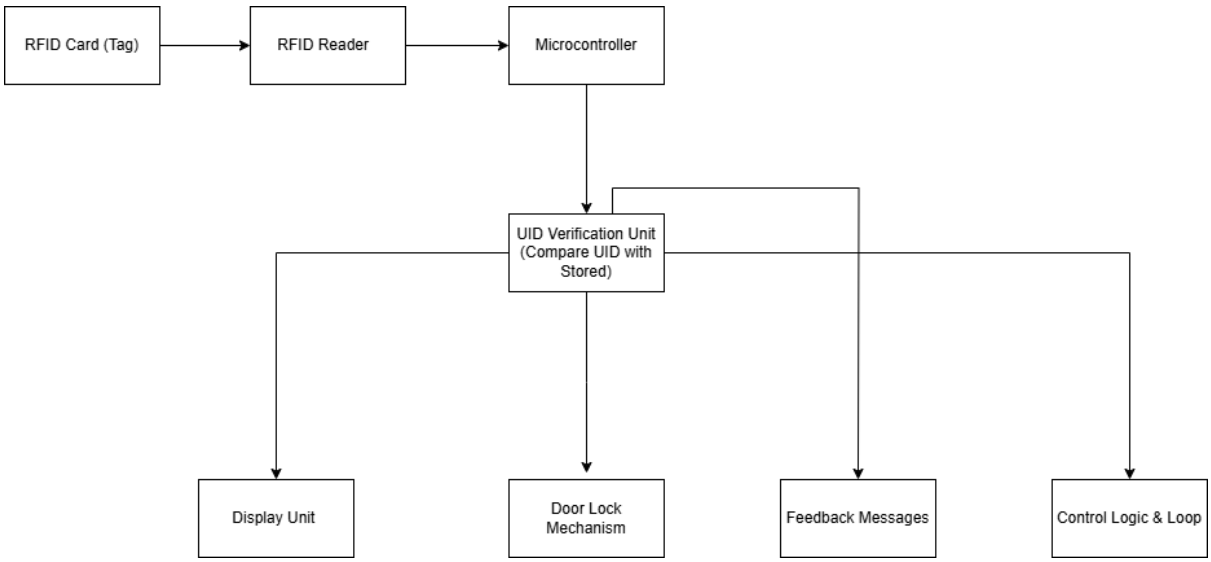

Figure 2: Block Diagram of RFID - Door lock system.

2.2.2 Hardware Architecture

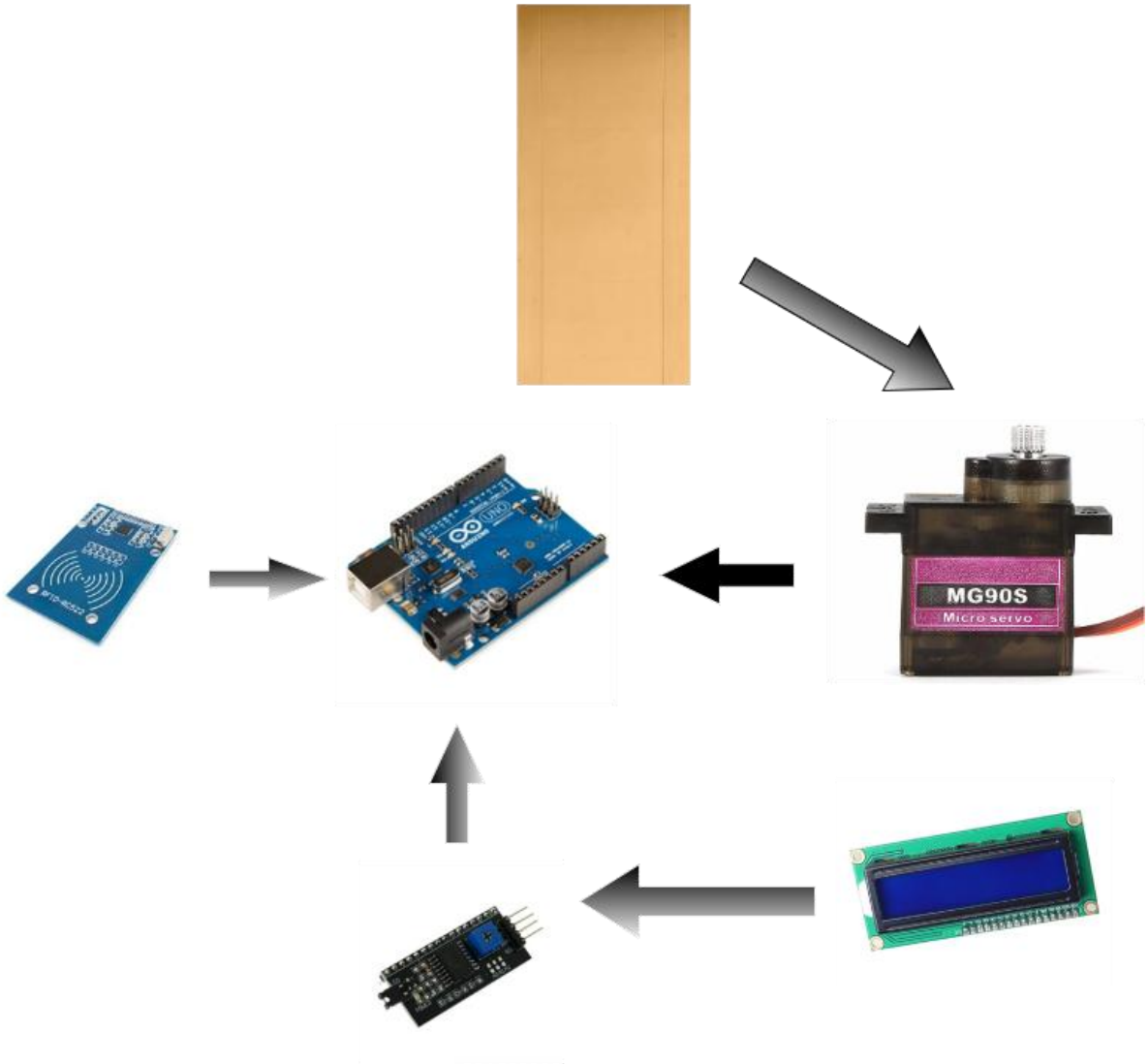

Figure 3: Hardware Architecture of RFID - Door lock system

2.2.3 Circuit Diagram

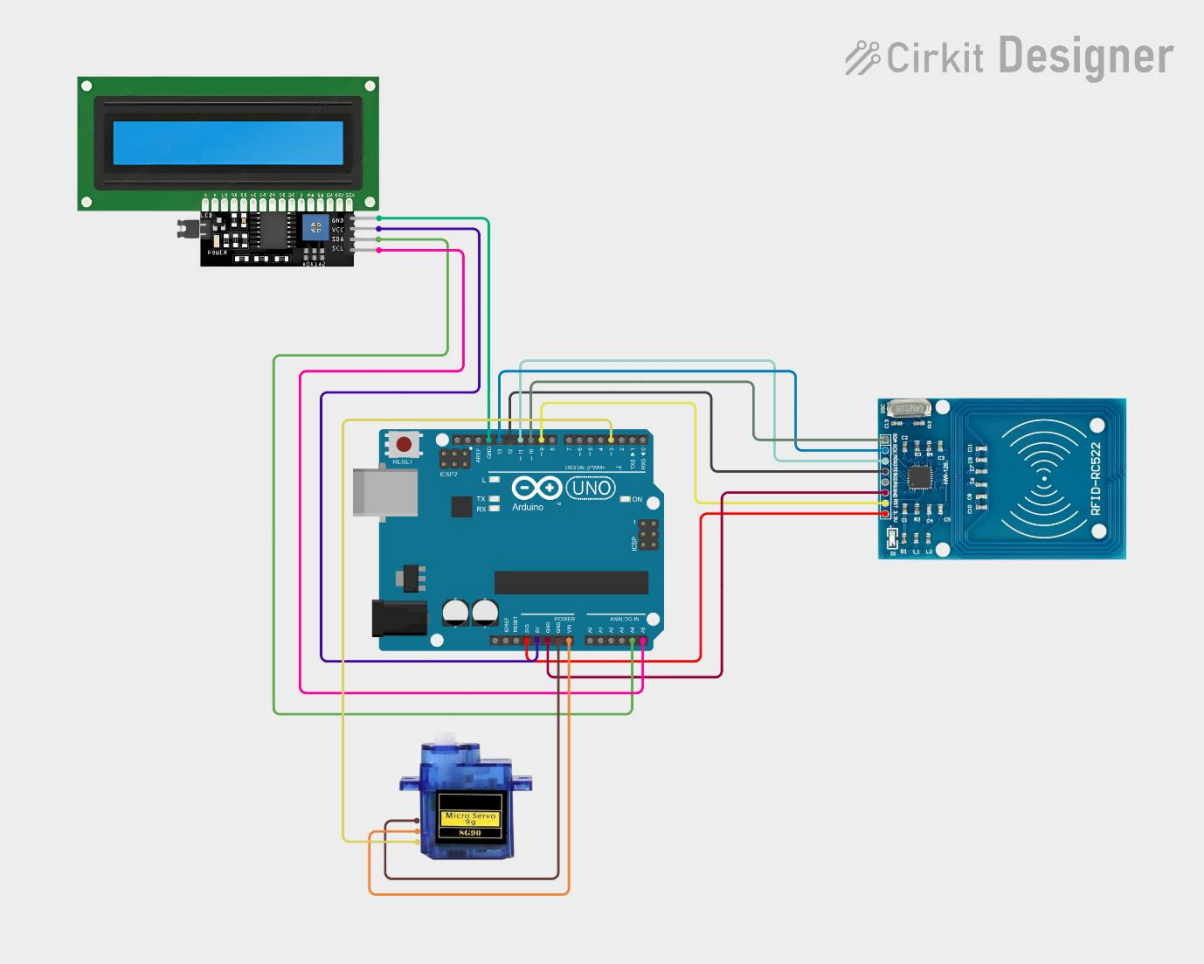

Figure 4: Circuit Diagram of RFID - Door lock system.

2.2.4 Schematic Diagram

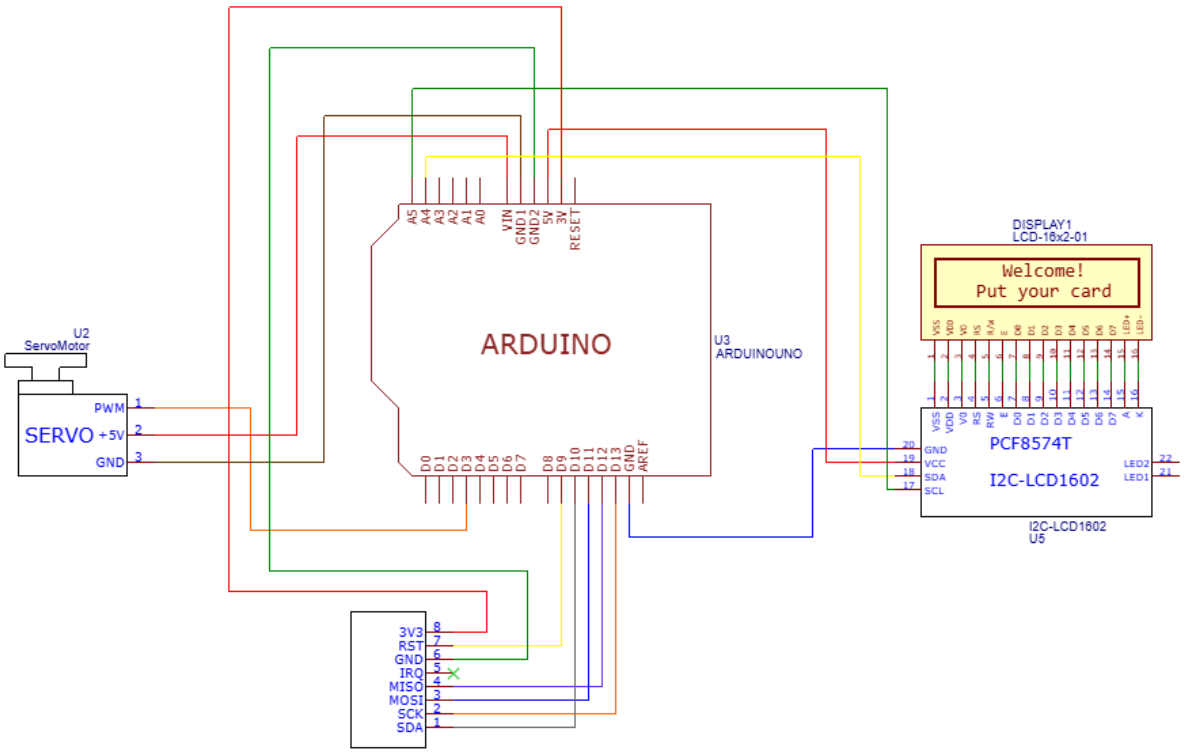

Figure 5: Schematic Diagram of RFID - Door lock system

2.2.5 Flowchart

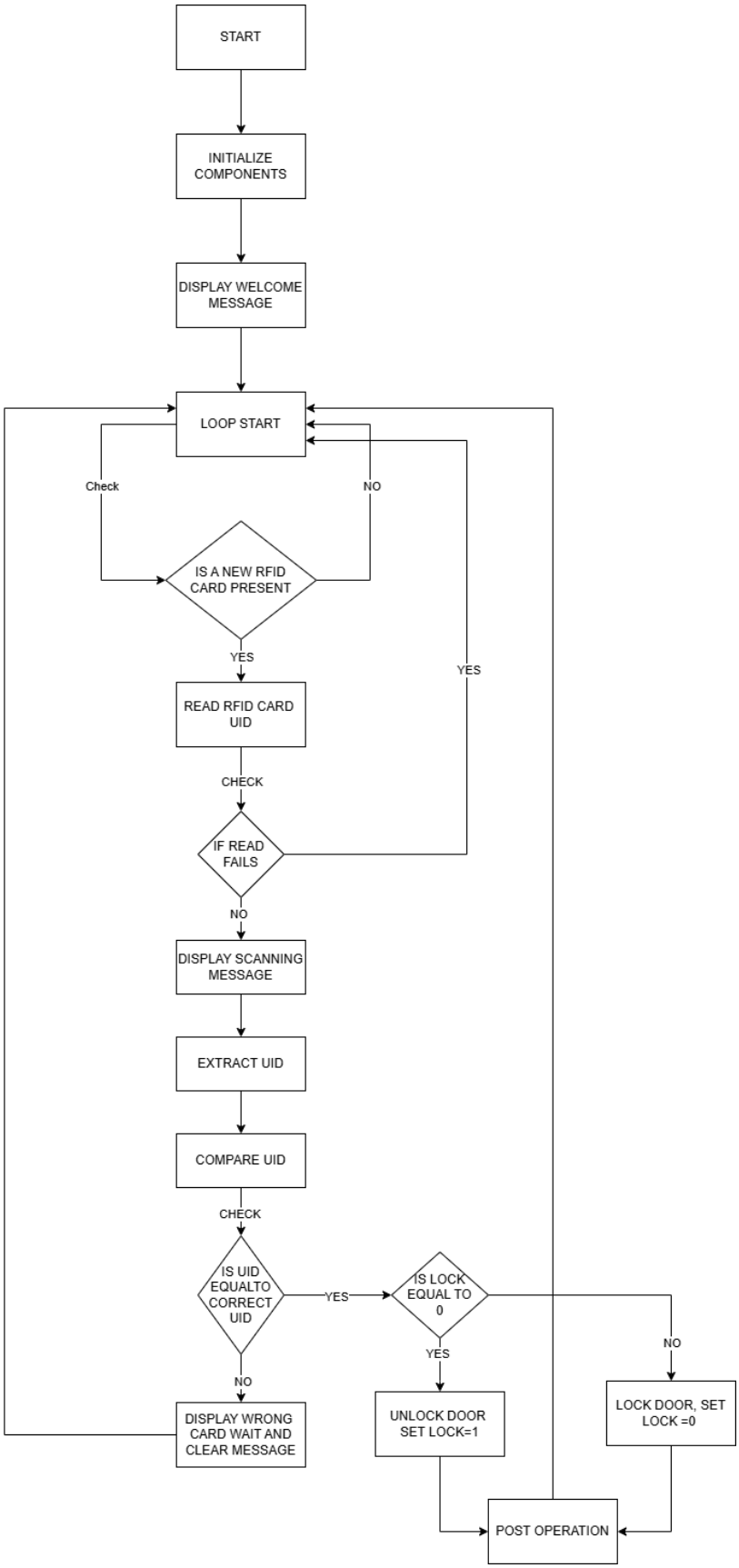

Figure 6: Flow chart of RFID - Door lock system

2.3 Requirement Analysis

This section provides a comprehensive and detailed analysis of both hardware and software components essential to ensure the effective design, seamless integration, and successful implementation of the dual-authentication door lock system.

2.3.1 Hardware Requirement

Arduino Uno

Arduino UNO is a microcontroller board based on ATmega328P Microcontroller, an 8-bit AVR Architecture based MCU from ATMEL. It has two variants, one has 28-pin DIP Microcontroller and the other has 32 lead Quad Flat Package Microcontroller. (Adruino, 2020)

Figure 7: Picture of Arduino Uno

Jumper Wires

A jumper wire is an electrical wire with connector pins at each end, used to connect two points in a circuit without soldering.

Figure 8: Picture Jumper Wires

RFID Reader (RC522)

RFID is short for Radio Frequency Identification that uses electromagnetic waves in radio frequency to transfer data. RC522 RFID model is based on MFRC522 IC that is one of the most inexpensive options that comes with a RFID card tag and key fob tag having 1KB memory. (microdigisoft, 2022)

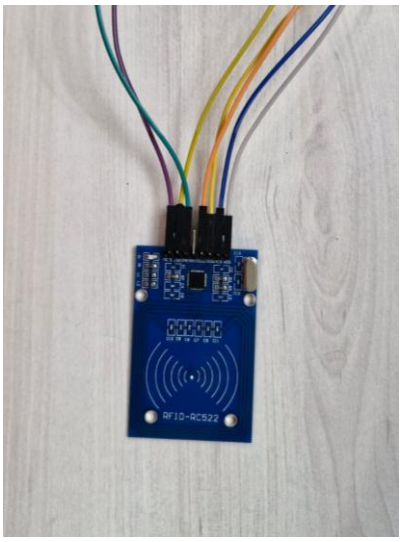

Figure 9: Picture RFID Reader

RFID Cards and Tags

An RFID card is a contactless smart card embedded with a microchip and antenna, used for wireless data transmission in applications like access control and contactless payments. An RFID tag is a small device containing a microchip and antenna, attached to objects or living beings for identification and tracking via radio waves. (TsangJean, 2024).

Figure 10: Picture RFID Card and Tag

LCD Display (16x2)

The l2c display module is a Liquid Crystal Display (LCD) screen which interacts using inter-integrated circuit (l2c) protocol. It enables simple communication between microcontrollers and peripheral devices. (Poly Notes Hub, 2024)

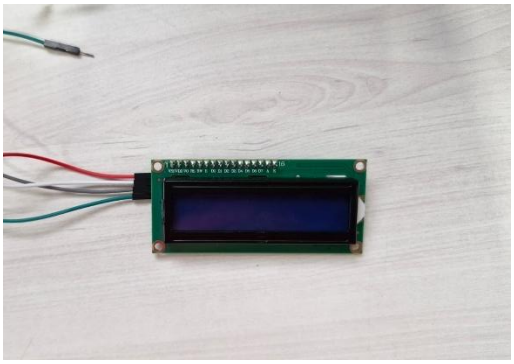

Figure 11: Picture LCD Display (16x2)

Servo Motor

A servo motor is a highly specialized motor that is designed for precise control of rotary or linear motion. It employs a feedback mechanism to ensure the positioning using a signal that dictates the motor's movement to wanted position. (Advanced Motion Controls, 2024)

Figure 12: Picture Servo Motor

2.3.2 Software Requirements

Arduino IDE

The Arduino IDE serves as the primary interface for writing programs which can be transmitted to an Arduino Mega. The Arduino IDE features four essential components for users such as code editor, compiler, uploader and serial monitor for debugging processes.

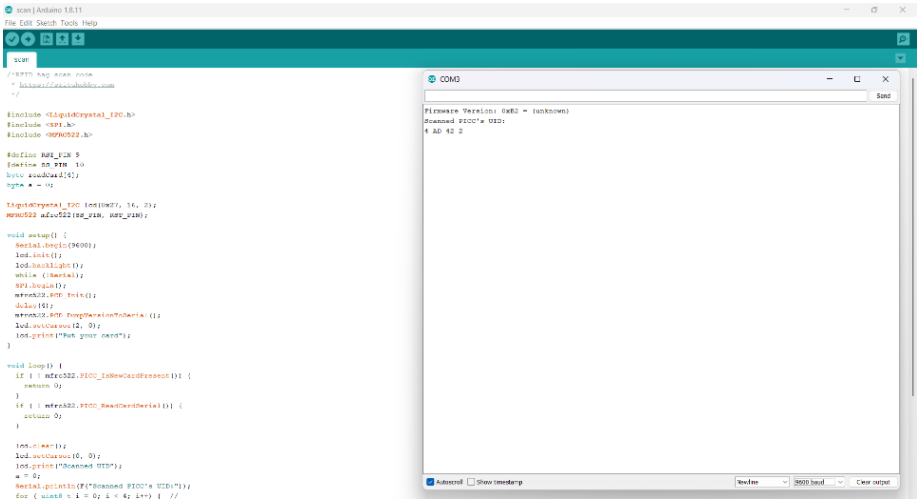

Figure 13: Programming in the Arduino IDE

Programming Language (C/C++)

Development of Arduino firmware primarily uses C/C++ which provides microcontroller-level access through which users can control memory functions and I/O devices and time-dependent operations efficiently.

Figure 14: Logo of Programming Language (C/C++)

Cirkit Designer

Cirkit Designer is a user-friendly application for designing and simulating electronic circuits. This application includes drag-and-drop tools that enable users to create breadboard circuits and automatically produce schematics together with bill of materials for educational applications. (cirkitstudio, 2023).

Figure 15: Logo Cirkit Designer

Easy EDA

Easy EDA is a cloud-based platform to develop schematic diagrams and Printed circuit board layouts which includes circuit simulation tools within its platform. Users can collaborate in real-time with this platform and find numerous efficient hardware design components within its system. (easyeda, 2023)

Figure 16: Logo Easy EDA

Draw.io

Draw.io function is an open-source drawing software that lets users build flowcharts along with network diagrams and UML models without any cost. The tool enables users to utilize Google Drive or OneDrive for cloud storage features which simplify file saving and sharing capabilities. The tool plays a role in producing the flowchart which describes the door lock system operations. (Elena, 2022)

Figure 17: Logo Draw.io

Microsoft Word

Microsoft Word functions is a word processing application where users prepare documents through formatting and editing stages. Users can benefit from numerous functionalities offered by Microsoft Word including text formatting options and functionality for table and image addition as well as page designing instruments which come with multiple templates for diverse documentation requirements. (Byju's.com, 2019)

Figure 18: Logo Microsoft Word

3. Development

3.1 Planning and Design

The development of the RFID-based door lock system began with identifying the core problem of limited access control in traditional locking mechanisms, especially in commercial and institutional environments. The goal was to create a secure, scalable, and cost-effective solution that would eliminate the risks of lost keys, unauthorized duplication, and physical lock tampering. The planning phase involved analyzing existing electronic lock technologies, selecting the appropriate components (Arduino UNO, RFID-RC522, SG90 micro servo, and I2C LCD), and defining system requirements such as low power consumption, user-friendly feedback, and reliable real-time performance.

During the design phase, the system architecture was sketched to outline all major functional blocks: RFID card scanning, microcontroller-based decision-making, motor-driven lock actuation, and display output. The team selected the Arduino UNO due to its simplicity, community support, and sufficient GPIO for SPI and I2C communication. The RFID-RC522 module was integrated for tag-based authentication, while the servo motor was used to physically simulate the locking mechanism. The 16x2 I2C LCD was chosen to reduce pin usage and provide real-time system feedback. Circuit connections were carefully mapped to ensure non-conflicting pin usage, allowing seamless integration of all modules without additional hardware.

To ensure reliability, the team prepared a logical flow chart of the program logic before beginning implementation. This included defining conditions for access approval, error handling for unrecognized tags, and timing delays for lock actuation. Safety considerations like proper grounding, voltage compatibility (3.3V for the RFID module), and power stability were also part of the design checklist. The planning and design phase concluded with a working schematic and block diagram, forming the basis for successful implementation and testing. This structured approach ensured the project met its goals both in functionality and usability.

3.2 Resource Collection

Through market research and institutional support, the keypad and RFID-based door lock system were developed, and its necessary components were acquired. In order to choose materials that met requirements for interconnection and were able to stand failure and security threats, the team compared available options before making their purchases. Together with the locking mechanism, which showed remarkable strength in integrating with electronic control, the RFID sensor was selected as the best option based on accuracy and responsiveness. The Arduino Mega microcontroller, an I2C 16x2 LCD display module, and a servo motor were the three crucial parts that the college provided. These essential parts compose the system, and their primary functions include using the Arduino Uno to control the system, the LCD to provide user feedback, and the servo motor to operate the locking mechanism. The project's balanced resource purchase plan allowed it to achieve both operational success and economic efficiency.

3.3 System Development

The development of the RFID-Based Door Lock System was executed in four distinct phases, ensuring a structured integration of hardware and software components.

3.3.1 Phase 1: Laptop–Arduino Connection

In this initial phase, the Arduino Uno microcontroller was connected to a laptop via USB to facilitate program upload and serial communication. This setup enabled direct interaction with the Arduino IDE for code compilation, debugging, and real-time monitoring. The system was powered through this connection, forming the base for subsequent configuration and testing activities.

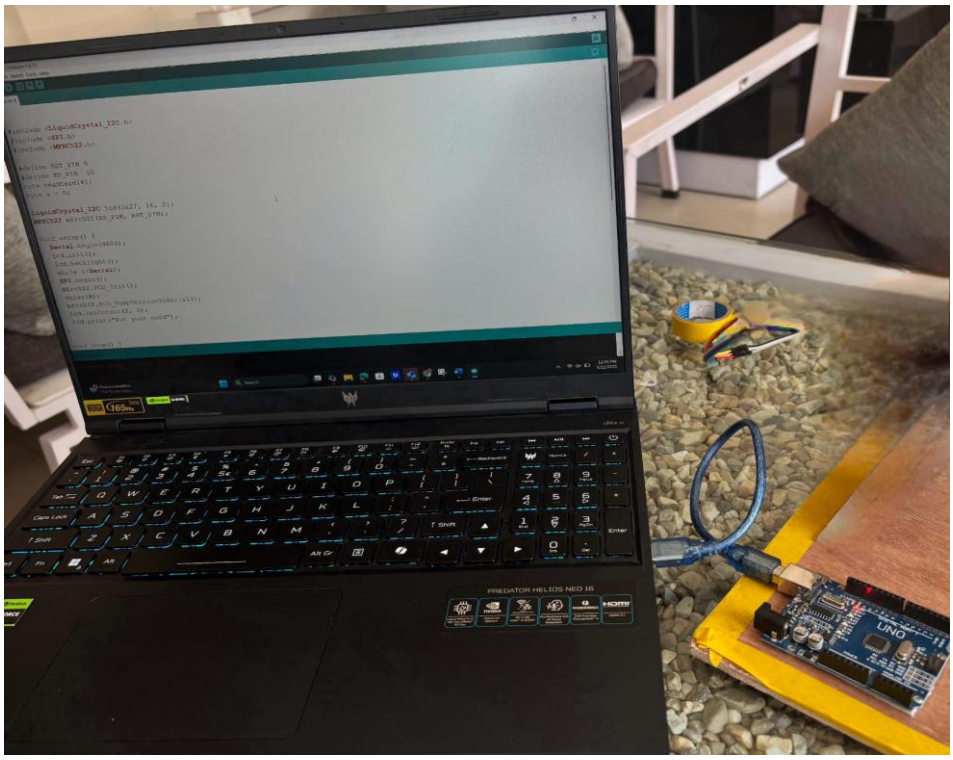

Figure 19: Programming the Arduino Board

3.3.2 Phase 2: Input Device Connection

The RFID-RC522 module was first positioned onto the system frame as part of the structural layout. It was securely fixed on the right side of the cardboard panel near the mock door, ensuring convenient card tapping access.

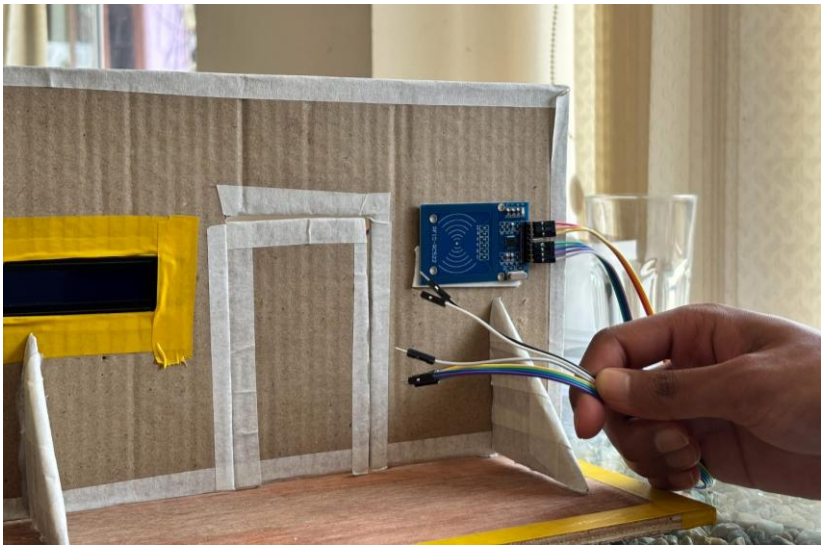

Figure 20: Fixing the RFID reader to the right side of the structure

Once the RFID module was in place, it was interfaced with the Arduino Uno using the SPI communication protocol. The jumper wires were connected to specific digital pins on the Arduino board, enabling proper data transmission and power supply. The table below summarizes the exact pin-to-pin mapping used for integration.

Figure 21: RFID module fully wired to the Arduino Uno using jumper cables.

Connection: Arduino to RFID Reader (RC522 – SPI Interface)

Arduino Pin	RFID Pin	Function Description
D10	SDA	Enables SPI communication.
D13	SCK	Clock line for SPI communication.
D11	MOSI	Sends data from Arduino to RFID module.
D12	MISO	Send data from RFID module to Arduino.
D9	RST	Resets the RFID module.
GND	GND	Common ground for stable operation.
3.3V	3.3V	Powers the RFID module.

Table 1: Connection between Arduino and RFID reader

3.3.3 Phase 3: Output Device Connection

Initially, the SG90 servo motor was physically mounted inside the prototype structure, aligned to control the mock door's bolt mechanism. A sturdy iron rod was attached between the servo horn and the door latch, enabling mechanical movement when the servo rotates. The placement allowed precise push-and-pull control of the lock mechanism, simulating real-world door locking and unlocking behavior. After mounting, the servo motor was connected to the Arduino Uno.

Figure 22 Servo motor fixed to the side panel with the rod connected to the locking latch.

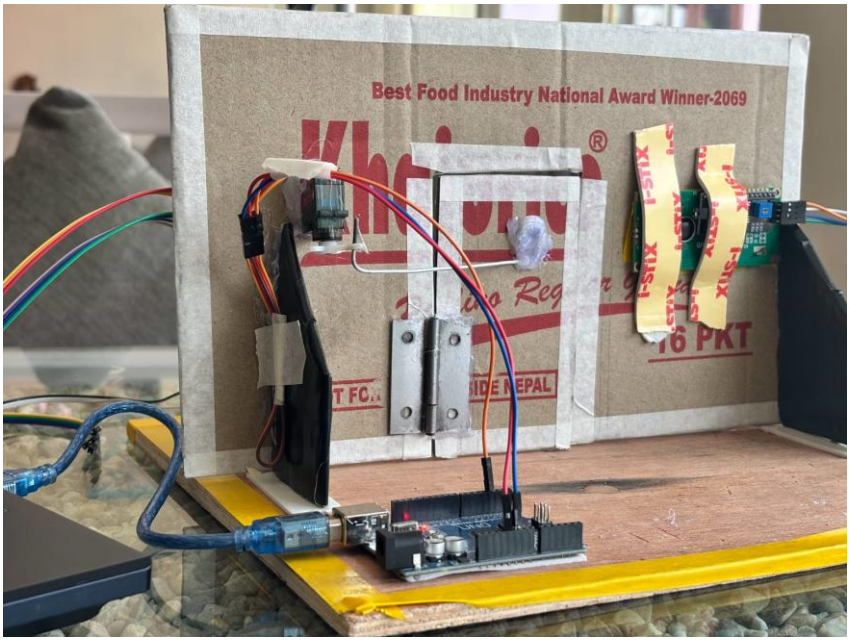

Figure 23: Servo motor fully connected to Arduino Uno

Connection: Arduino to Micro Servo (SG90)

Arduino Pin	Servo Pin	Description
D3	Signal	Sends control signal to rotate servo.
5V	VCC	Provides 5V power to the servo motor.
GND	GND	Completes the circuit with ground.

Table 2: Connection between Arduino and RFID reader

Additionally, the 16x2 I2C LCD display was embedded on the left side of the prototype structure, visibly placed for user interaction. Its position was selected to clearly display system messages such as access status and UID scans during operation, enhancing the system's usability and feedback clarity.

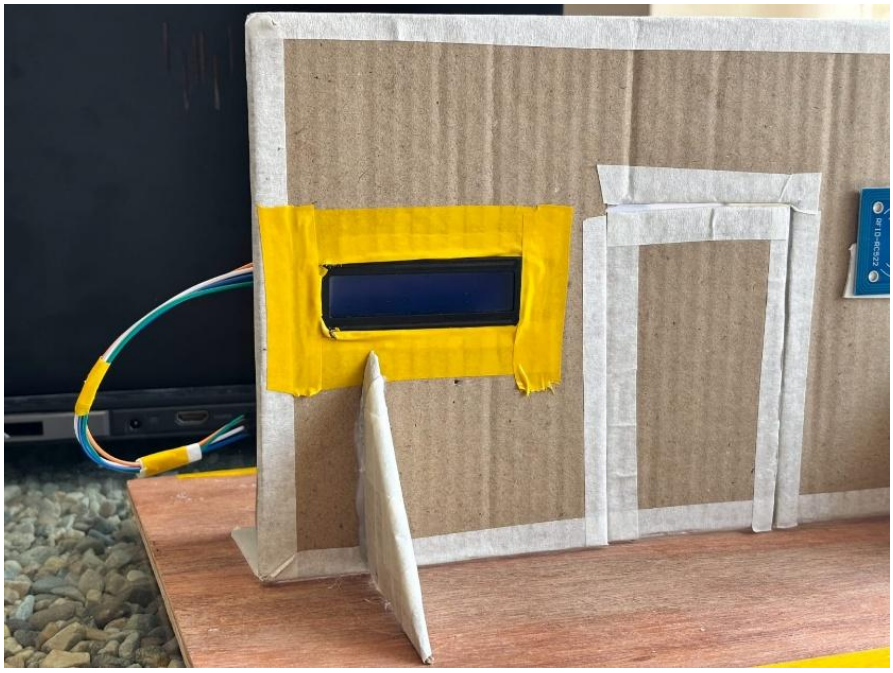

Figure 24: LCD display fixed to the left panel for real-time system feedback.

Following the physical setup, the LCD display was interfaced with the Arduino Uno using the Inter-Integrated Circuit (I2C) communication protocol. This protocol is widely used in embedded systems due to its efficiency and minimal wiring requirements.

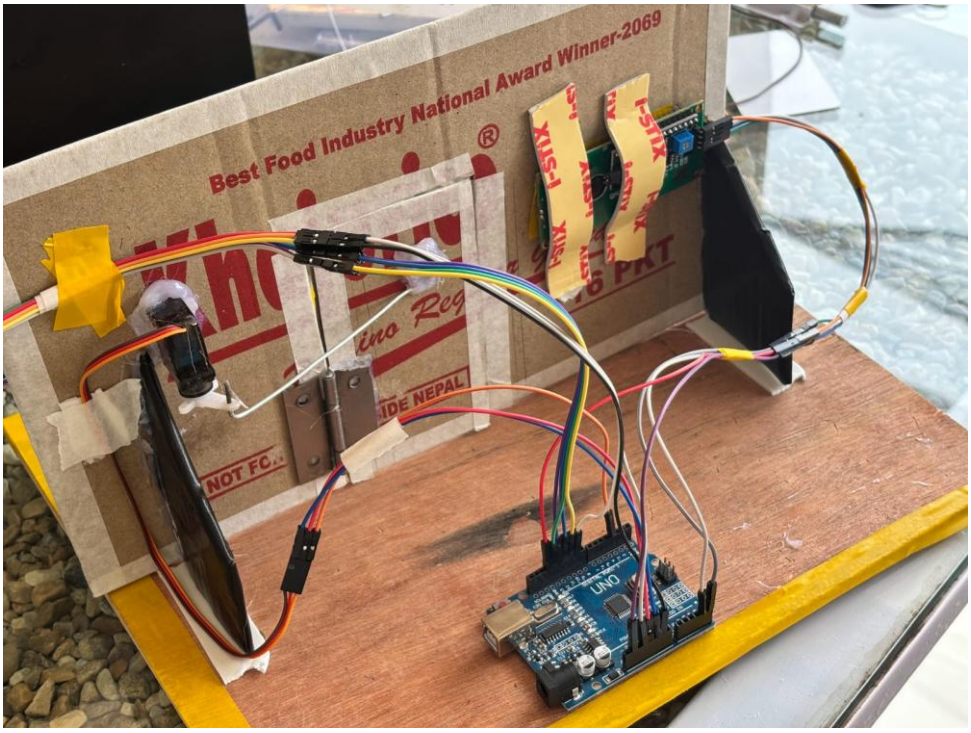

Figure 25: LCD display wired and connected to Arduino Uno using the I2C protocol.

Connection: Arduino to 16x2 LCD Display (via I2C Module)

Arduino Pin	LCD I2C Pin	Description
A4	SDA	It sends data to the LCD via I2C protocol.
A5	SCL	It sends clock signals for I2C timing.
5V	VCC	Powers the LCD module with 5V.
GND	GND	Connects LCD to ground.

Table 3: Connection between Arduino and LCD display

3.3.4 Phase 4 : Programming and Final Prototype Display

Once all components were structurally and electrically integrated, the final phase involved uploading the complete program to the Arduino Uno via the Arduino IDE. Libraries such as MFRC522, Servo, and LiquidCrystal_I2C are included to enable RFID tag reading, control the servo motor, and display messages on the LCD. The code is uploaded to the Arduino with predefined UID values for authorized RFID cards.

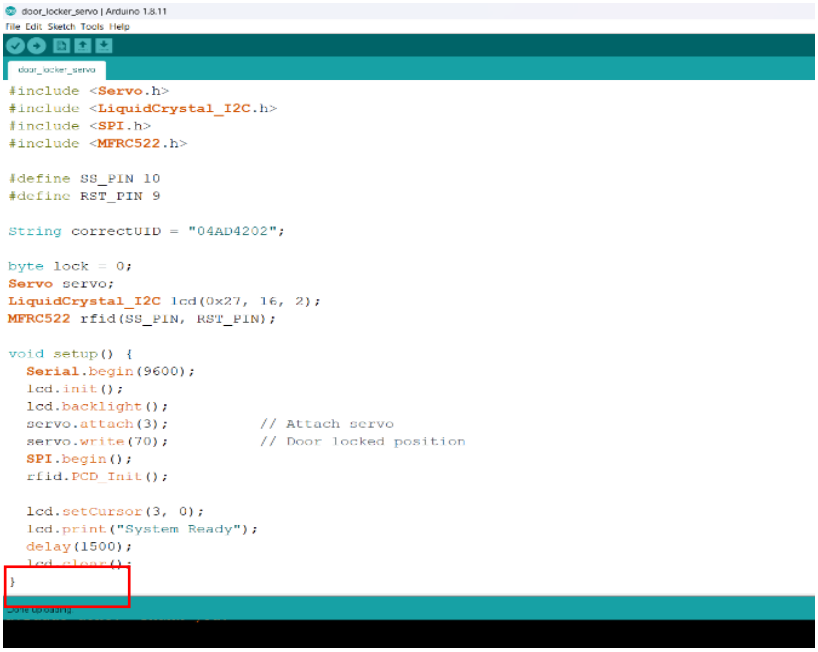

Figure 26: Code successfully uploaded to the microcontroller.

After successfully uploading the code, the system was powered on, initiating the boot process. The LCD display showed the startup message, confirming readiness. When an RFID card was tapped, the reader captured its unique identifier (UID) and passed it to the microcontroller for verification. If the UID matched a registered value, the servo motor triggered the door to unlock, and the LCD displayed an "Access Granted" message. If the UID was not recognized, the door remained locked, and the LCD displayed "Access Denied."

Figure 27: Access Granted

The program also handled automatic re-locking functionality. Upon successful access, the servo returned to the locked position after a short delay, enhancing system security. This phase demonstrated the full functionality of the prototype, confirming that all modules operated in synchrony as intended.

Figure 28: Door Unlocked

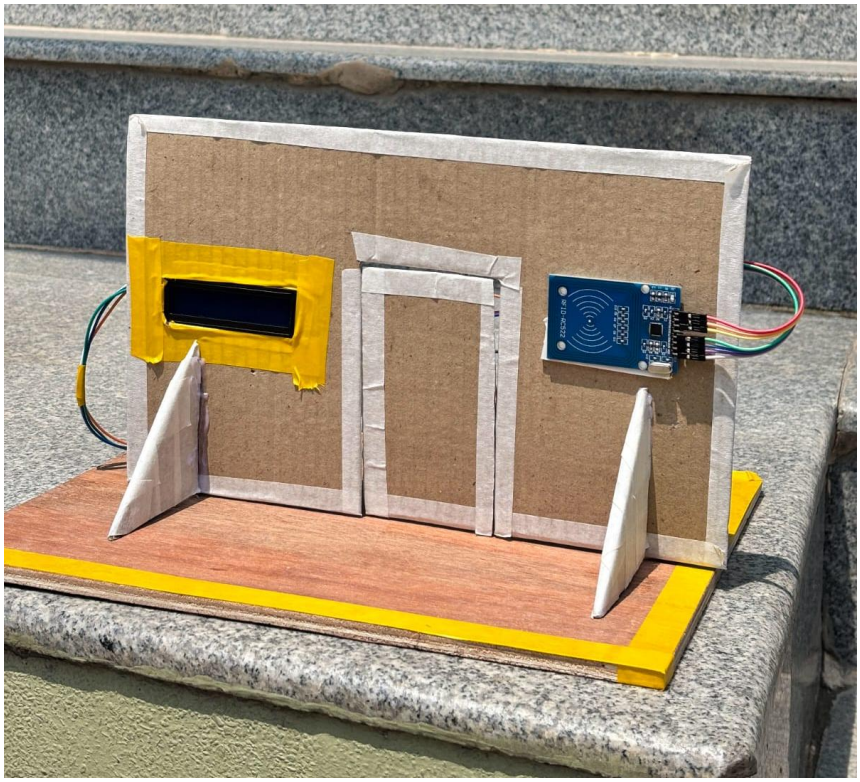

Figure 29: Overall system prototype assembled.

4. Results and Findings

4.1 Results

The end of the project led to the development of a working RFID Door Lock Access Control System utilizing Arduino Uno, MFRC522 RFID reader, LCD screen, and a servo motor. The system operates by granting or denying access based on scanned RFID tags through door automation that show immediate messages on the LCD screen. Multiple test cases conducted during this phase confirmed the system's functionality by assessing valid and invalid RFID access, servo operation, and message clarity. The system executed all of its main functions accurately in line with the specifications. The testing procedure involved capturing screenshots that verified each test scenario by displaying the LCD screen text for cases like "Door is open" when a valid tag was scanned and "Wrong card!" when trying to use an unregistered tag. The assessments confirm that the system operates as intended, providing secure automated door access features.

4.2 Testing

4.2.1 Test 1 – To Verify System Start-Up

Objective	To verify the system’s start-up functionality.
Actions	Step 1: Ensure all hardware components are properly connected to the Arduino. Step 2: Upload the code and power on the Arduino system using a USB cable. Step 3: Observe the LCD screen for any welcome message.
Expected Result	LCD should display "Welcome! Tap your card".
Actual Result	LCD displayed the correct message.
Conclusion	The test was successful.

Table 4: Test 1 – To Verify System Start-Up

Supporting Image for testing:

door_locker_servo | Arduino 1.8.11

File Edit Sketch Tools Help

door_locker_servo

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

#define SS_PIN 10
#define RST_PIN 9

String correctUID = "04AD4202";

byte lock = 0;
Servo servo;
LiquidCrystal_I2C lcd(0x27, 16, 2);
MFRC522 rfid(SS_PIN, RST_PIN);

void setup() {
  Serial.begin(9600);
  lcd.init();
  lcd.backlight();
  servo.attach(3);          // Attach servo
  servo.write(70);          // Door locked position
  SPI.begin();
  rfid.PCD_Init();

  lcd.setCursor(3, 0);
  lcd.print("System Ready");
  delay(1500);
  lcd.clear();
}
```

Done uploading.

Figure 30: Screenshot of code uploaded to the microcontroller.

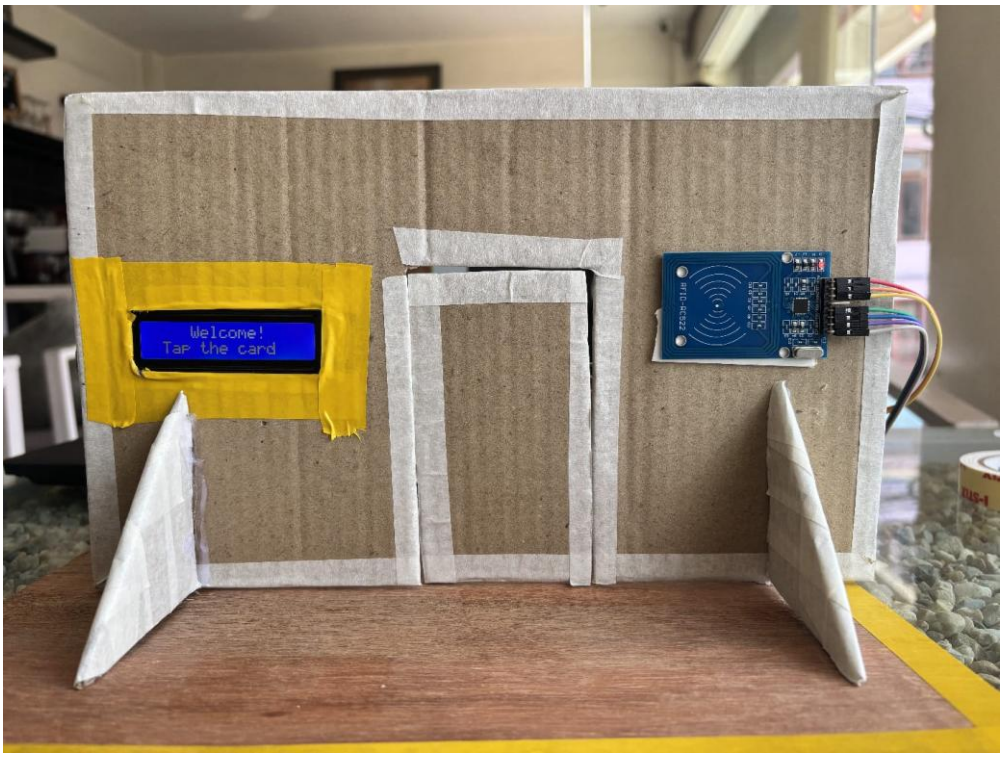

Figure 31: LCD displaying the welcome message during system start-up verification.

4.2.2 Test 2 –To Display and Retrieve New RFID Tag UID

Objective	To verify that the system reads and displays the UID code of a newly scanned RFID tag, it can be manually added to the Arduino code.
Actions	Step 1. Open the Serial Monitor in the Arduino IDE and ensure the baud rate is set correctly (typically 9600 or 115200). Step 2. Take a new RFID tag that is not yet stored in the system. Step 3. Place the tag near the RFID reader module. Step 4. Observe the Serial Monitor for the tag's UID to be printed. Step 5. Copy the UID and manually update the main Arduino code to include this UID as a valid card.
Expected Result	The system should print the new RFID tag's UID to the serial monitor immediately after scanning.
Actual Result	The system printed the new tag's UID correctly in the serial monitor, ready to be added in code.
Conclusion	The test was successful.

Table 5: Test 2 –To Display and Retrieve New RFID Tag UID

Supporting Image for testing:

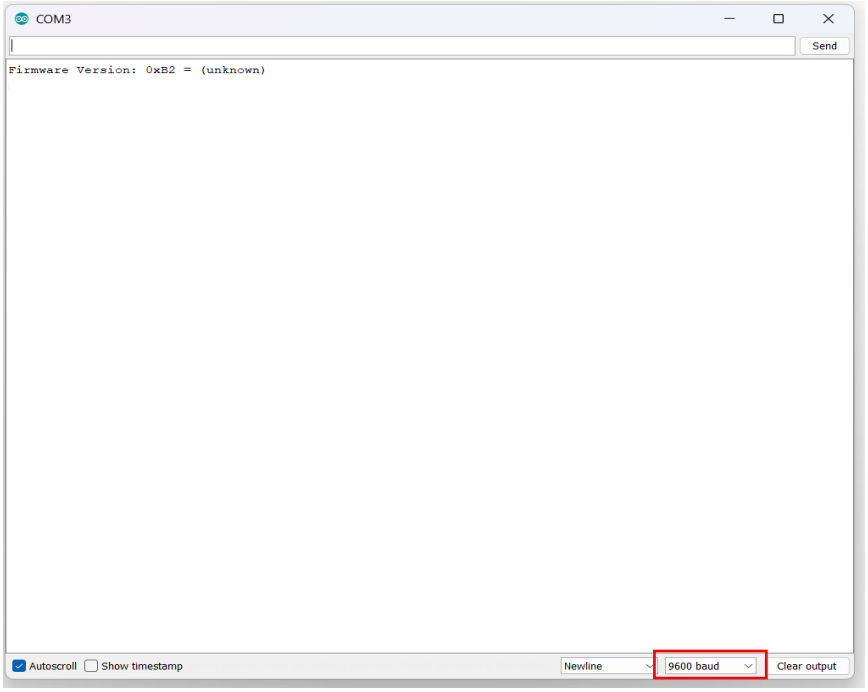

Figure 32: Baud rate set to 9600.

Figure 33: Scanning an unregistered RFID card and LCD displays its unique UID.

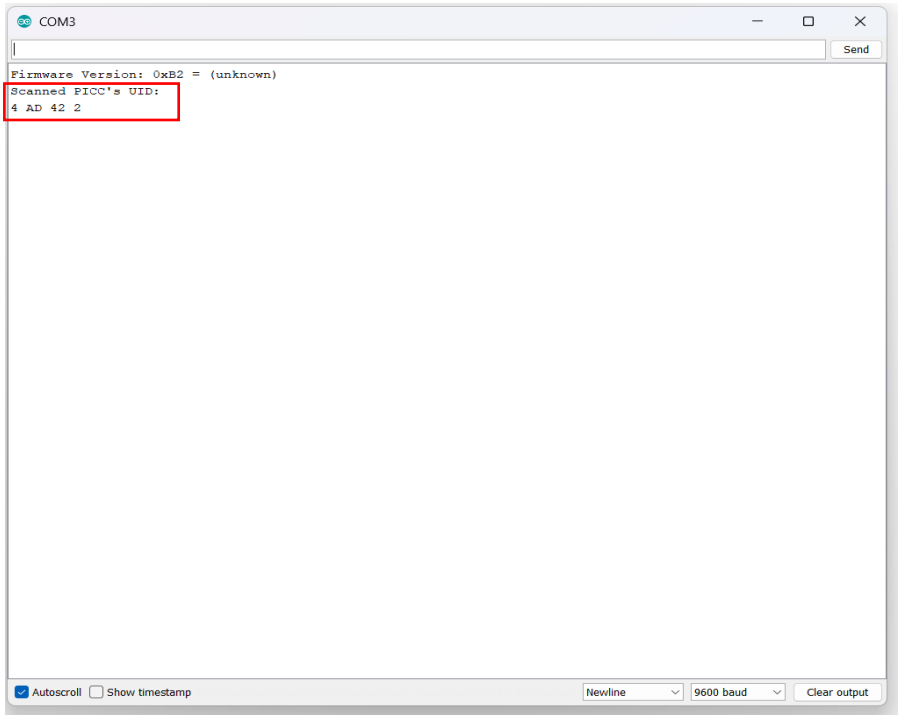

Figure 34: Serial Monitor displaying the scanned UID.

Figure 35: Registration of the scanned card in the system.

4.2.3 Test 3 – To Confirm Authorized Access and door locking

Objective	To confirm that the system allows access when a valid RFID tag is scanned.
Actions	Step 1. Take a valid RFID tag Step 2. Place the RFID tag near the RFID reader. Step 3. Wait for the tag to be detected. Step 4. Observe the LCD display as the door unlocks. Step 5. Wait 5 seconds and observe the system automatically locking the door again.
Expected Result	The LCD should display "Access Granted" and the servo should unlock the door. After 5 seconds, LCD should display "Door is locked" and the servo should return to the locked position.
Actual Result	LCD displayed "Access Granted" and the servo unlocked the door. After 5 seconds, the LCD displayed "Door is locked" and the servo locked the door automatically.
Conclusion	The test was successful.

Table 6: Test 3 – To Confirm Authorized Access

Supporting Image for testing:

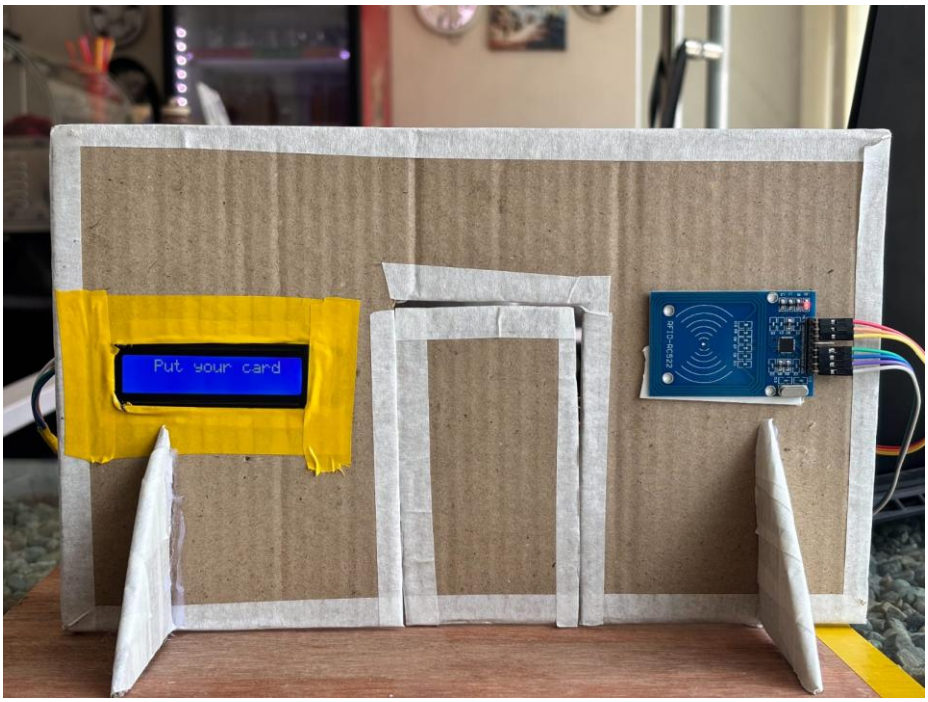

Figure 36: Initial setup where the door is locked.

Figure 37: Scanning a registered card and the door unlocked.

Figure 38: Door automatically locked after 5 seconds.

4.2.4 Test 4 - To Prevent Unauthorized Access

Objective	To verify that the system blocks unregistered RFID tags.
Actions	Step 1. Take an unregistered RFID tag. Step 2. Place the tag near the RFID reader. Step 3. Wait for the system to read and process the tag. Step 4. Observe the LCD and servo for any response.
Expected Result	The LCD should display "Access Denied!" and no servo movement should occur.
Actual Result	LCD displayed "Access Denied!" and the servo did not move.
Conclusion	The test was successful.

Table 7: Test 4 - To Prevent Unauthorized Access

Supporting Image for testing:

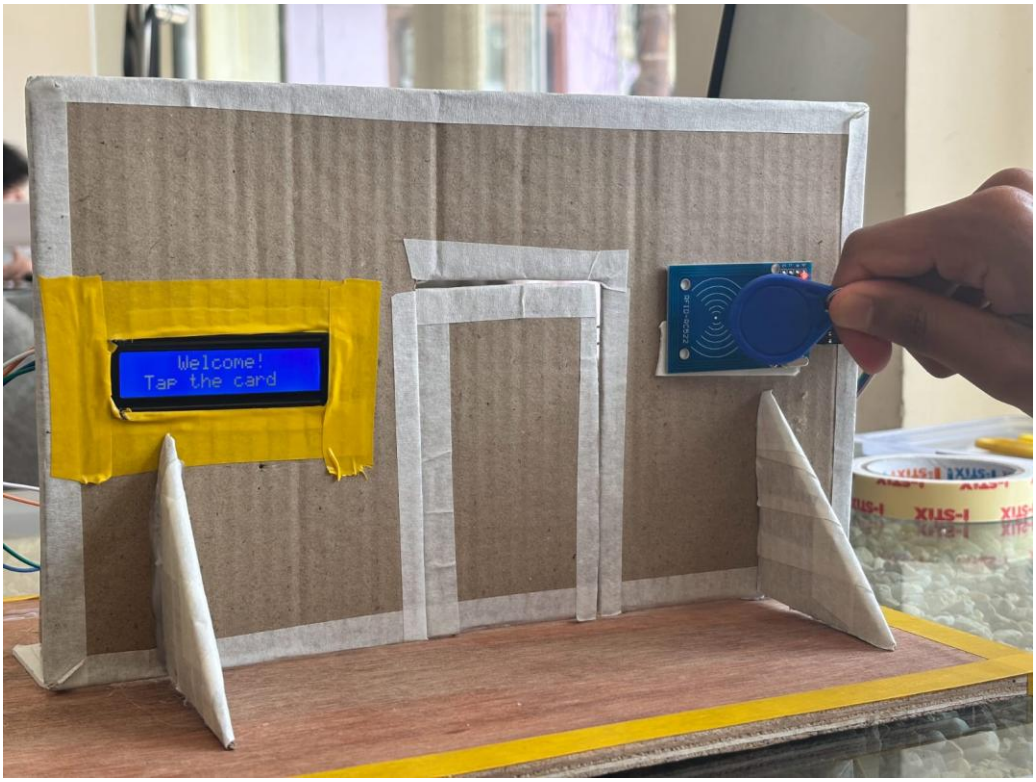

Figure 39: Scanning an Unregistered RFID tag

Figure 40: LCD displaying "Access Denied!"

4.2.5 Test 5 – RFID Card Scanning.

Objective	To ensure that the RFID-based system accurately scans a valid RFID tag by verifying the stored credentials and triggering the appropriate unlocking mechanism.
Actions	Step 1. Take a valid (registered) RFID tag. Step 2. Place the RFID tag near the RFID reader. Step 3: Observe the LCD and servo motor activity.
Expected Result	The RFID reader must successfully scan the RFID card and execute the assigned task by displaying the appropriate message on the LCD and activating the servo motor to unlock the door.
Actual Result	In some instances, the RFID tag did not get detected despite being scanned. The LCD continued to display ‘Tap the Card’, and no servo movement was seen.
Conclusion	The test was unsuccessful as there was occasional failure in RFID tag detection.

Table 8: Test 5 – To scan RFID Scanning

Supporting Image for testing:

Figure 41 Failure of RFID to scan the card

5. Future Potential and Applications

5.1 Future Potential

As modern homes and buildings continue to evolve, traditional lock-and-key systems are gradually being replaced by more secure and intelligent solutions. This advanced access control technology offers unparalleled convenience and enhanced security, eliminating the need for physical keys that can be lost, duplicated, or stolen. According to recent industry projections, the global market for RFID-based locking systems is estimated at USD 5.4 billion in 2024 and is expected to experience significant growth, expanding at a compound annual growth rate of 17.4% (Research Nester, 2024). By 2037, the market is anticipated to surpass 43 billion USD, highlighting the rising global demand for secure and contactless access solutions. (Research Nester, 2024)

5.2 Applications in Specific Sectors

RFID door lock systems are poised to transform the future of both industrial and residential security by offering a smart, adaptable, and centralized access control solution. With support for a wide range of secure identification methods these systems eliminate the inefficiencies of physical key management and offer a seamless user experience

5.2.1 Financial Sector

In the future, the adoption of RFID-based access control systems will have the potential to greatly enhance security and compliance within the financial sector. Critical areas such as bank vaults, insurance repositories, and data center suites could be secured using RFID credentials, providing each employee with a unique, non-duplicable digital key. In the event of a lost or compromised card, access can be revoked instantly through centralized software, eliminating the need for costly physical re-keying. These systems could also be configured to generate automated daily audit logs, supporting future compliance with evolving regulatory standards like PCI-DSS and Basel III. Furthermore, by integrating RFID with two-factor authentication methods institutions could deter internal fraud and strengthen access control at sensitive zones. As technology matures, RFID systems are expected to reduce unauthorized access incidents and streamline audit processes by automatically logging and time-stamping every access attempt, offering financial institutions a scalable and secure solution for digital-era access management.

5.2.2 Healthcare Sector

In the healthcare sector, RFID-based access control systems hold significant promises for enhancing security, hygiene, and operational efficiency in the future. Hospitals, clinics, and laboratories could secure high-risk areas such as operating theatres, pharmaceutical storage rooms, and electronic health record (EHR) repositories using contactless RFID cards, which support infection control by minimizing physical contact with shared surfaces. Future implementations may also integrate real-time locating systems (RTLS) using the same RFID infrastructure to monitor staff movement, enforce hand hygiene compliance, and reduce cross-contamination risks. Administrators will be able to issue time-bound credentials for visiting medical professionals or contractors and remotely revoke access when necessary, ensuring that only authorized individuals handle sensitive medical data or controlled substances. As adoption expands, RFID systems are expected to improve access traceability and support quicker investigation and resolution of security or hygiene-related incidents.

5.2.3 Security Sector

In the security sector, RFID access control systems are set to enhance perimeter protection and operational oversight in high-security environments such as government buildings, defense labs, and private security firms. These systems can integrate with identity management platforms and intrusion sensors to enforce clearance levels at each entry point. Utilizing encrypted credentials and tamper-resistant readers, these systems will be capable of preventing unauthorized duplication and credential fraud. Additionally, comprehensive entry logs generated by these systems will support post-incident investigations and help agencies demonstrate compliance with evolving national security standards. When combined with routine credential audits and the use of shielded card media, RFID access control is expected to significantly reduce risks related to espionage, insider threats, and unauthorized movement of assets in sensitive facilities.

6. Conclusion

The completion of this project marks the successful design and implementation of an RFID-based door lock system that demonstrates the practical application of Internet of Things technologies in enhancing physical security. By integrating the Arduino Uno microcontroller, RFID authentication, servo motor actuation, and an LCD interface, the system delivers a secure, contactless, and programmable access control solution suitable for modern environments.

The project achieved all intended objectives, including reliable user authentication, unlocking mechanisms, and real-time feedback to the user. Throughout development, technical challenges related to hardware interfacing, voltage regulation, and communication protocols were addressed through a methodical approach, collaborative effort, and the valuable guidance of the project supervisor. This process significantly contributed to the team's understanding of embedded systems, circuit integration, and the core principles of IoT system design.

The broader impact of this project lies in its scalability, adaptability, and relevance to current and emerging security demands. In an era where contactless technologies are increasingly prioritized, RFID-based systems offer a forward-looking alternative to traditional mechanical locks. Their ability to support centralized credential management, audit trails, and real-time system responses makes them particularly valuable in sensitive environments such as healthcare facilities, financial institutions, educational campuses, and government buildings. Furthermore, the system's low cost and modular design make it a feasible solution for deployment in developing regions, where affordability and ease of implementation are critical.

The project also supports educational outcomes by providing a hands-on platform for students to engage in real-world IoT applications, fostering skill development in electronics, programming, and system integration. As smart infrastructure continues to evolve globally, systems such as the one developed in this project will play a vital role in advancing the security and efficiency of access control technologies.

7. References

Adruino, 2020. *Adruino uno.* [Online]
Available at: https://docs.arduino.cc/
[Accessed 3 April 2025].

Advanced Motion Controls, 2024. *What is a Servo Motor: Definition, Origins, Components, Types & Applications.* [Online]
Available at: https://www.a-m-c.com/servomotor/

Alghamdi, A., 2020. *Security Lock systems: From Problem Statement to System Design Name of the Author,* s.l.: s.n.

Bannister, A., 2016. *IFSEC Insider.* [Online]
Available at: https://www.ifsecglobal.com/global/few-businesses-will-have-mechanical-only-locks-10-years-from-now-62-of-security-professionals-believe/
[Accessed 18 04 2025].

CDC, 2020. *selectagents.* [Online]
Available at: https://www.selectagents.gov/compliance/guidance/security-plan/appendix-2.htm/
[Accessed 18 04 2025].

Devkota, N., 2021. Obstacles of Implementing Industry 4.0 in Nepalese Industries and Way-Forward. *International Journal of Finance Research,* 2(4), pp. 286-295.

Jordi Salazar, S. S., 2017. *Internet of Things,* Technicka 2, Prague 6, Czech Republic: Czech Technical University of Prague.

Market Data Forecast logo, 2024. *Market Data Forecast logo.* [Online]
Available at: https://www.marketdataforecast.com/market-reports/smart-locks-market
[Accessed 25 04 2025].

microdigisoft, 2022. *Introduction- RC522 RFID Module For Arduino.* [Online]
Available at: https://microdigisoft.com/introduction-rc522-rfid-module/

Paranagama, C., 2022. *A Review on Existing Smart Door Lock Systems,* s.l.: s.n.

Poly Notes Hub, 2024. *I2C LCD Module – Pinout and Specifications | New Topic [2024].* [Online]
Available at: https://polynoteshub.co.in/i2c-lcd-module/

Rajbhandari, S., 2022. *National Library of Medicine.* [Online]
Available at: https://pubmed.ncbi.nlm.nih.gov/35243054/
[Accessed 21 04 2025].

Research Nester, 2024. *Research Nester.* [Online]
Available at: https://www.researchnester.com/reports/rfid-locks-market/1315
[Accessed 01 05 2025].

Sharma, V., 2022. RFID Based Access Control System Using Arduino. *International Research Journal of Modernization in Engineering Technology and Science ,* 4(3), pp. 655-659.

TsangJean, 2024. *gialer.* [Online]
Available at: https://www.gialer.com/blogs/news-and-blogs/deciphering-the-distinctions-rfid-cards-vs-tags#

Walter, E., 1995. *Cambridge Advanced Learner's Dictionary" (CALD).* Cambridge: Cambridge University Press.

8. Appendix

8.1 Appendix A: Source Code

8.1.1 Code for Initial card registration

```
#include <LiquidCrystal_I2C.h>

#include <SPI.h>

#include <MFRC522.h>


#define RST_PIN 9

#define SS_PIN  10

byte readCard[4];

byte a = 0;


LiquidCrystal_I2C lcd(0x27, 16, 2);

MFRC522 mfrc522(SS_PIN, RST_PIN);


void setup() {

  Serial.begin(9600);

  lcd.init();

  lcd.backlight();

  while (!Serial);

  SPI.begin();1

  mfrc522.PCD_Init();

  delay(4);

  mfrc522.PCD_DumpVersionToSerial();
```

```
  lcd.setCursor(2, 0);
  lcd.print("Put your card");
}

void loop() {
  if ( ! mfrc522.PICC_IsNewCardPresent()) {
    return 0;
  }
  if ( ! mfrc522.PICC_ReadCardSerial()) {
    return 0;
  }

  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Scanned UID");
  a = 0;
  Serial.println(F("Scanned PICC's UID:"));
  for ( uint8_t i = 0; i < 4; i++) {  //
    readCard[i] = mfrc522.uid.uidByte[i];
    Serial.print(readCard[i], HEX);
    Serial.print(" ");
    lcd.setCursor(a, 1);
    lcd.print(readCard[i], HEX);
    lcd.print(" ");
```

```
    delay(500);
    a += 3;
  }
  Serial.println("");
  mfrc522.PICC_HaltA();
  return 1;
}
```

8.1.2 Code for execution of door locking mechanism

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

#define SS_PIN 10
#define RST_PIN 9

String correctUID = "04AD4202";

byte lock = 0;
Servo servo;
LiquidCrystal_I2C lcd(0x27, 16, 2);
MFRC522 rfid(SS_PIN, RST_PIN);

void setup() {
  Serial.begin(9600);
  lcd.init();
  lcd.backlight();
  servo.attach(3);          // Attach servo
```

```
  servo.write(70);          // Door locked position
  SPI.begin();
  rfid.PCD_Init();

  lcd.setCursor(3, 0);
  lcd.print("System Ready");
  delay(1500);
  lcd.clear();
}

void loop() {
  lcd.setCursor(4, 0);
  lcd.print("Welcome!");
  lcd.setCursor(1, 1);
  lcd.print("Tap the card");

  if (!rfid.PICC_IsNewCardPresent()) return;
  if (!rfid.PICC_ReadCardSerial()) return;

  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Scanning...");

  String readUID = "";
  for (byte i = 0; i < rfid.uid.size; i++) {
    byte temp = rfid.uid.uidByte[i];
    if (temp < 0x10) {
      readUID += "0";
    }
```

```
  readUID += String(temp, HEX);
 }
 readUID.toUpperCase();

 if (readUID == correctUID) {
  if (lock == 0) {
   servo.write(250);       // Unlock door
   lcd.clear();
   lcd.setCursor(0, 0);
   lcd.print("Access Granted");
   lock = 1;

   // Wait 5 seconds before auto-locking
   delay(5000);

   // Auto-lock if user didn't lock manually
   if (lock == 1) {
    servo.write(70);      // Lock door
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Door Locked");
    lock = 0;

    delay(2000);          // Show locked message
    lcd.clear();          // Then clear screen
   }

  } else if (lock == 1) {
   servo.write(70);       // Manual lock
```

```
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("Door Locked");
      lock = 0;

      delay(2000);           // Show locked message
      lcd.clear();           // Then clear screen
    }
  } else {
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Access Denied");
    delay(2000);
    lcd.clear();
  }

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

8.2 Appendix B: Picture of the System

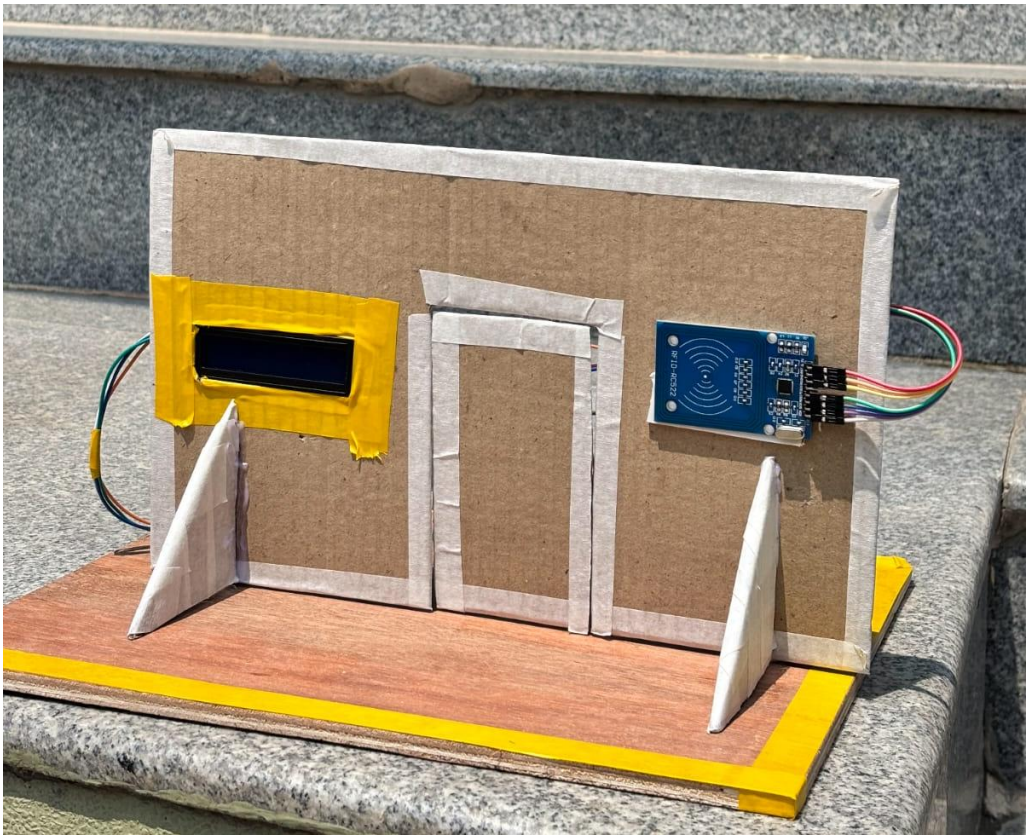

Figure 42 Front vies of the prototype

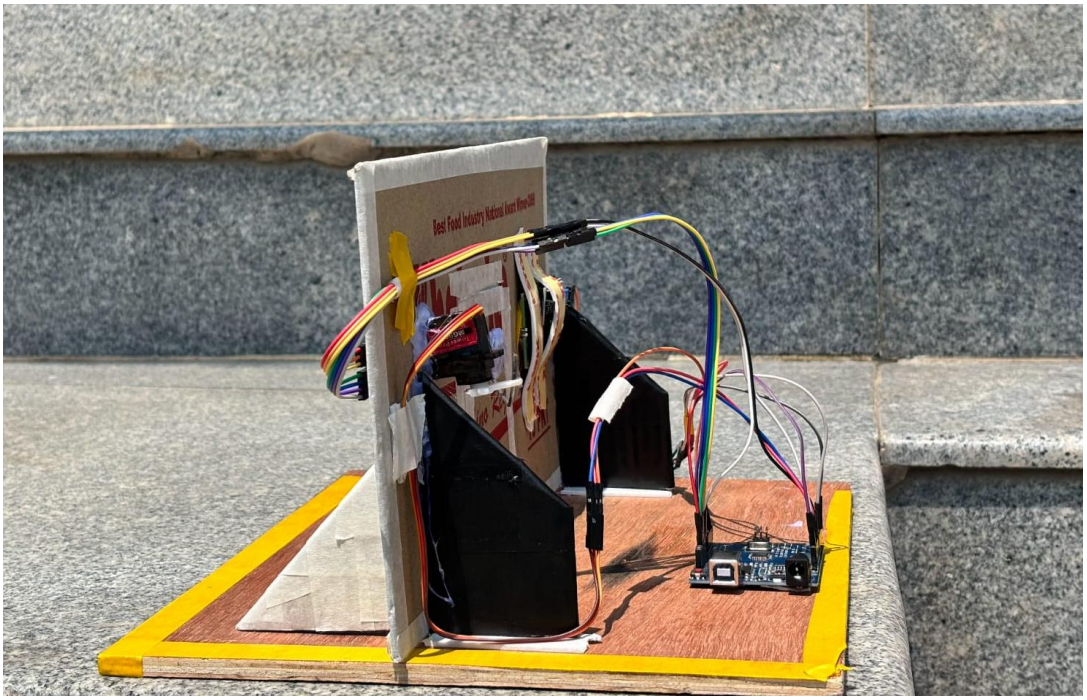

Figure 43 Right view of the prototype

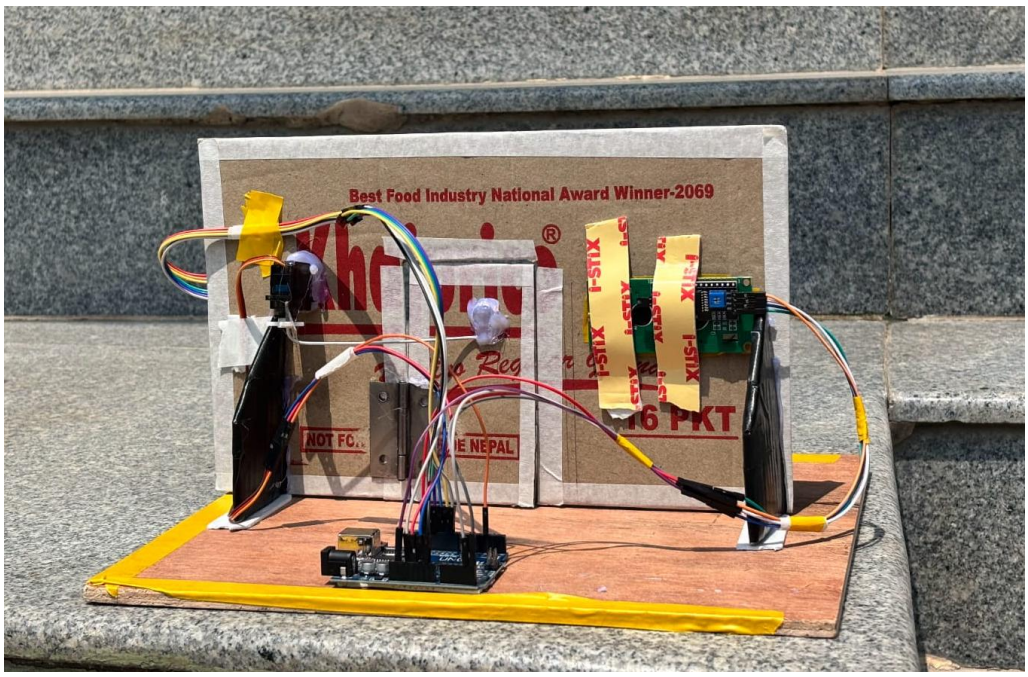

Figure 44 Back view of the prototype

Figure 45 Left view of the prototype

8.3 Appendix C: Design Diagrams

`

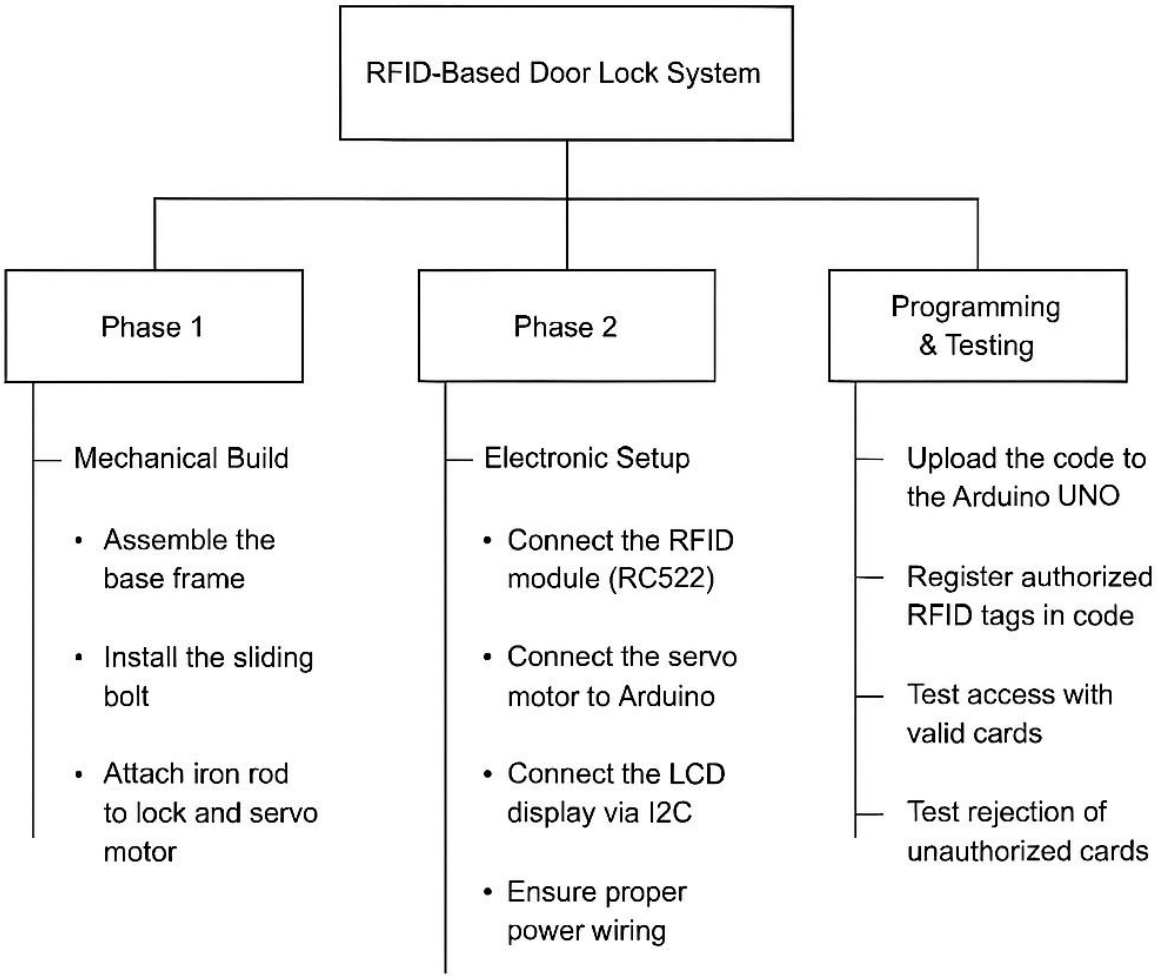

Figure 46: Work Breakdown Structure of the RFID-Based Door lock System

8.4 Appendix D: Evaluation of the prototype

Advantages	Disadvantages
The system enables contactless entry, enhancing hygiene and minimizing physical wear compared to traditional key-based locks.	The system relies on a continuous power supply; in the absence of backup power, it may become non-functional during outages.
RFID cards can be easily deactivated or replaced if lost or stolen, eliminating the need to replace physical locks.	Without proper encryption and security protocols, RFID tags may be susceptible to cloning or unauthorized access attempts.
Each RFID tag contains a unique identifier, which enhances authentication security and reduces the likelihood of unauthorized duplication.	Routine maintenance and occasional troubleshooting may require technical expertise or familiarity with embedded systems.
The system supports entry logging and activity tracking, offering improved access management and accountability for secure areas.	The initial setup process requires investment in electronic components, as well as time and knowledge for programming and hardware integration.

Table 9: Evaluation Table

8.5 Appendix E: Individual contribution plan

Student Name	Role
Siddartha Amatya	Oversaw the final integration of hardware and software components. Managed initial setup, ensured power stability, and contributed to multiple testing sessions. Helped compile the conclusion and supported proofreading of the final document.
Stuti Timilsina	Took lead in integrating the LCD display and ensuring clear user feedback. I participated in testing, debugging, and co-writing the results and testing sections. Also assisted in formatting the report and ensuring documentation consistency.
Sushant Chaudhary	Focused on programming Arduino, including RFID tag detection and servo control. Focused on debugging code and helped explain the software logic in the report. Participated actively in testing and hardware troubleshooting.
Chirag K.C.	Worked on the physical structure and servo motor mounting. Created initial diagrams, including the circuit and flowchart visuals. Assisted with system wiring and documentation of design phases and future applications.
Sayam Rai	Contributed to collecting and organizing all hardware components. Participated in assembling the mechanical locking system and assisted in testing the final prototype. Helped write the system overview and hardware requirement sections of the report.

Table 10: Contribution Plan