RFID BASED DOOR LOCK SYSTEM

MINI PROJECT REPORT

Submitted by

BHUVANA S (202009008)

in

19AD752 – INTELLIGENT SYSTEMS FOR IOT LABORATORY

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

MEPCO SCHLENK ENGINEERING COLLEGE

SIVAKASI

OCTOBER 2023

MEPCO SCHLENK ENGINEERING COLLEGE, SIVAKASI

AUTONOMOUS

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

BONAFIDE CERTIFICATE

This is to certify that it is the bonafide work of "**Bhuvana.S (Reg.No.:202009008)"** for the mini project titled **"RFID BASED DOOR LOCK SYSTEM"** in 19AD752 – Intelligent Systems for IoT Laboratory during the seventh semester, July 2023 – October 2023 under my supervision.

SIGNATURE
Dr.A.Shenbagarajan,
Associate Professor,
Artificial Intelligence and Data Science,
Mepco Schlenk Engg. College, Sivakasi.

SIGNATURE
Dr. J. Angela Jennifa Sujana,
Professor & Head of the Department,
Artificial Intelligence and Data Science,
Mepco Schlenk Engg. College, Sivakasi.

ABSTRACT

The RFID-based Door Lock System is an innovative and secure solution designed to address the growing need for enhanced access control and security in various settings, such as homes, offices, and industrial facilities. This project aims to provide a convenient and reliable way to manage access to restricted areas while minimizing the risks associated with traditional lock and key systems. The need for this project arises from the limitations of conventional lock and key systems, which are susceptible to unauthorized access through lost or duplicated keys. In contrast, the RFID-based Door Lock System leverages Radio Frequency Identification (RFID) technology to offer a more robust and user-friendly access control mechanism. Users are provided with RFID cards or key fobs, each embedded with a unique identification code. When a user presents their RFID card or key fob to the reader, the system authenticates their identity and grants or denies access accordingly. This project provides an overview of the RFID-based Door Lock System's components, including RFID readers, RFID cards/key fobs, a microcontroller, and an electric door lock mechanism. The system's operation is explored, detailing the communication between the RFID reader and the microcontroller. Additionally, the project demonstrates the integration of a mobile application for remote access control and monitoring. The RFID-based Door Lock System offers several advantages, such as improved security, real-time access logs, and the ability to manage access permissions remotely. This project not only addresses the need for enhanced security but also showcases the potential for the widespread adoption of RFID technology in access control systems. By implementing this system, users can enjoy a more secure and convenient way to control access to their premises.

CONTENTS

1. INTRODUCTION

1.1. RFID based Door Lock System using Arduino

In an increasingly interconnected world, the need for robust and sophisticated access control systems has never been more critical. Traditional lock and key mechanisms have proven to be vulnerable to various security risks, such as unauthorized duplication of keys, lost keys, and the lack of real-time access monitoring. To address these challenges, the "RFID-Based Door Lock System using Arduino" project emerges as a cutting-edge solution, harnessing the power of Radio Frequency Identification (RFID) technology and Arduino microcontrollers to create a secure and efficient access control system.

The primary motivation behind this project is to offer a reliable, convenient, and highly secure method for controlling access to homes, offices, and industrial facilities. RFID technology allows users to replace traditional keys with RFID cards or key fobs, each containing a unique identification code. When presented to an RFID reader, these credentials are authenticated in real-time, granting or denying access based on predefined permissions. This approach not only enhances security but also streamlines the access management process.

This project will delve into the design and implementation of an RFID-Based Door Lock System using Arduino, providing a comprehensive overview of the system's architecture, hardware components, and software integration. Additionally, it will explore the system's versatility by incorporating mobile application control for remote access management. By adopting this technology, users can enjoy heightened security, traceability, and convenience, thereby ushering in a new era of access control in the digital age.

1.2. Objective

The Objective of our project is follows:

- **Enhanced Security:** Implement a secure access control system to prevent unauthorized entry into homes, offices, or other restricted areas, reducing the risk of theft or intrusion.
- **Convenience:** Provide a user-friendly and convenient method for authorized personnel to gain access without the need for traditional keys, which can be lost or duplicated.

- **Real-Time Access Control:** Enable real-time monitoring and control of access permissions, allowing administrators to grant or revoke access remotely and receive notifications of entry events.

- **Integration of RFID Technology:** Incorporate RFID technology to enable quick and contactless authentication, enhancing the speed and efficiency of the access control process.

- **Arduino Microcontroller Integration:** Utilize Arduino microcontrollers to interface with RFID readers and electric door lock mechanisms, creating a cost-effective and customizable solution.

- **Mobile Application Integration:** Develop a mobile application that enables users to control and monitor access remotely, providing added convenience and flexibility.

- **Access Logging:** Implement a logging system that records access events, including timestamps and user identification, for security and audit purposes.

- **Customizable Access Permissions:** Allow administrators to define and customize access permissions for individual users or groups, providing flexibility in managing access rights.

- **Low Maintenance:** Design a system that requires minimal maintenance and is reliable for extended periods, reducing operational costs.

2. LITERATURE SURVEY

2.1. RFID Security and Privacy: A Research Survey

In the paper "RFID Security and Privacy: A Research Survey," published in the IEEE Journal on Selected Areas of Communication in 2006, author Ari Juels conducts a comprehensive survey of the state of research in Radio Frequency Identification (RFID) security and privacy. RFID technology has gained widespread adoption in various domains, ranging from supply chain management to access control. However, concerns regarding the security and privacy of RFID systems have emerged as significant issues that need to be addressed.

This research survey provides an extensive overview of the challenges and solutions in RFID security and privacy, covering a wide range of topics. The paper delves into various cryptographic protocols, authentication mechanisms, privacy-enhancing techniques, and threat models that have been proposed and explored in the context of RFID systems. It discusses the implications of RFID technology on privacy and examines the trade-offs between security and efficiency.

The paper not only summarizes the existing research but also identifies open research questions and areas where further investigation is required to enhance the security and privacy of RFID systems. It serves as a valuable resource for researchers, practitioners, and policymakers in the field of RFID technology, shedding light on the complexities of securing RFID systems while preserving user privacy. RFID technology enhances inventory tracking and management in retail, manufacturing, and logistics. It allows for real-time visibility of inventory levels, reducing stockouts and overstock situations. It reduces errors and delays in the supply chain, leading to cost savings and improved customer satisfaction.

2.2. Smart Door Locking System

The paper titled "Smart Door Locking System" presents a novel approach to enhance security and convenience in residential and commercial settings. In an era where smart home technologies are gaining prominence, the authors introduce a cutting-edge door locking system designed to leverage advancements in electrical, electronics, communication, computing, and automation.

The system described in the paper combines elements of modern technology to create a secure and user-friendly access control solution. Through the integration of electronic components, wireless communication, and automation techniques, the smart door locking system offers a seamless user experience while prioritizing security.

Key features and components of the proposed system are likely to include electronic locks, access control interfaces, communication modules (possibly IoT-enabled), and user-friendly software interfaces. The system may also encompass biometric authentication, remote access control, and real-time monitoring capabilities. The paper likely discusses the design, implementation, and testing of the Smart Door Locking System, highlighting its potential applications, advantages, and the impact of this technology in both residential and commercial environments.

2.3. RFID Door Lock

The "RFID Door Lock" project is designed to enhance access control and security in residential and commercial environments using Radio Frequency Identification (RFID) technology. This project leverages RFID tags and readers to create a sophisticated yet user-friendly door locking system. Users are granted access by presenting an authorized RFID card or key fob, simplifying entry while maintaining high levels of security. The system incorporates modern technology to offer convenient and reliable access control.

At its core, this project revolves around the strategic deployment of RFID readers and antennas, intelligently positioned on door frames to facilitate seamless card detection. The central objective is to simplify and expedite entry processes while simultaneously upholding rigorous security standards. To realize this vision, the project begins with the careful selection of hardware components, including RFID readers and electronic door locking mechanisms, meticulously chosen for their compatibility with the RFID technology adopted, whether it be Low Frequency (LF), High Frequency (HF), or Ultra-High Frequency (UHF) RFID systems. The hardware is thoughtfully integrated into the door's architecture, ensuring efficient card detection and access control.

The access control logic forms the project's brain, residing within a capable microcontroller or embedded system. This logic is meticulously programmed to conduct real-time comparisons between the unique RFID card data detected at the reader and the information stored within its authorized card database. When a match is established, the door unlocking mechanism is promptly triggered, granting the user access. A paramount aspect of the project revolves around security measures. To fortify the system against unauthorized access and potential breaches, the project incorporates sophisticated security protocols. These include encryption of RFID data and the secure storage of authorized card information, safeguarding the integrity of the system.

Moreover, the project offers flexibility through optional features. It allows for the integration of user-friendly interfaces, such as LCD displays or mobile applications, simplifying card enrolment and access monitoring. For enhanced convenience, the RFID door lock system can also be seamlessly integrated with existing security systems or integrated into broader home automation platforms.

Thorough testing and calibration phases ensure the system's reliability and accuracy, making certain that card detection and access control operate seamlessly. User documentation is thoughtfully prepared to guide users in system usage and troubleshooting. Finally, deployment brings the project to fruition, culminating in a sophisticated and user-friendly RFID door lock system that elevates access control and security standards for residential and commercial applications alike.

2.4. Security and Privacy Aspects of Low Cost Radio Frequency Identifications Systems

The paper titled "Security and Privacy Aspects of Low Cost Radio Frequency Identification Systems," authored by S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, is a seminal work published in the Lecture Notes in Computer Science: Security in Pervasive Computing, Volume 2802, in 2004. This paper delves into the critical security and privacy implications associated with the widespread adoption of Low-Cost Radio Frequency Identification (RFID) systems, shedding light on the vulnerabilities and challenges that emerge as RFID technology is integrated into various aspects of modern life. The authors begin by providing an overview of RFID technology and its extensive applications in domains such as supply chain management, access control, and inventory tracking. They highlight the cost-effectiveness and efficiency of low-cost RFID systems, which have spurred their rapid deployment across industries.

However, the paper swiftly pivots to address the inherent security and privacy concerns that accompany this proliferation. The authors meticulously dissect various threats to RFID systems, including eavesdropping, unauthorized tag reading, and tracking of individuals without their consent. Moreover, they examine the potential for RFID systems to become targets for malicious attacks or data breaches.

In response to these security challenges, the paper offers a thorough analysis of cryptographic techniques and security protocols that can be employed to fortify RFID systems. This includes the exploration of techniques like authentication, access control, and encryption mechanisms that can safeguard data transmission and protect the privacy of users. Furthermore, the authors delve into the concept of "kill" and "block" commands that allow for the deactivation or suspension of RFID tags, adding an extra layer of control over the security of these systems. The paper underscores the delicate balance between the benefits of RFID technology and the imperative to protect user privacy and data security. It advocates for the adoption of strong security practices and cryptographic measures to mitigate risks associated with RFID deployment.

In summary, this paper serves as a seminal contribution to the discourse on RFID security and privacy, offering a comprehensive examination of both the advantages and potential pitfalls of low-cost RFID systems. It provides valuable insights for researchers, industry professionals, and policymakers grappling with the task of harnessing the potential of RFID technology while ensuring robust security and privacy safeguards in an increasingly interconnected world.

2.5. Arduino based Door Unlocking System with Real Time Control

The paper titled "Arduino-Based Door Unlocking System with Real-Time Control," authored by S. Nath, P. Banerjee, R. N. Biswas, S. K. Mitra, and M. K. Naskar, was presented at the 2nd International Conference on Contemporary Computing and Informatics (IC3I) in 2016. This paper introduces an innovative and practical approach to door access control using Arduino microcontroller technology, emphasizing real-time control and convenience.

The primary objective of the research is to design a robust and efficient door unlocking system that offers both security and user-friendliness. The authors recognize the growing need for access control solutions in various domains, including residential, commercial, and industrial settings. In response to this demand, they propose an Arduino-based system that leverages the flexibility and versatility of the Arduino platform.

The system's architecture is thoroughly described in the paper, highlighting the key components and their roles. The core of the system comprises an Arduino microcontroller, a servo motor for door unlocking, and various sensors and modules. To enhance security, an RFID (Radio Frequency Identification) reader is integrated, enabling authorized users to gain access by presenting RFID cards or key fobs. One of the paper's notable features is its emphasis on real-time control. This real-time processing allows for swift and secure access control, reducing the risk of unauthorized entry. Moreover, the authors explore the convenience aspect of their system. They discuss the implementation of a user-friendly interface, possibly through an LCD display or LED indicators, to provide feedback and instructions to users. Additionally, the system can be configured to support multiple users and RFID cards, making it adaptable for various access control scenarios. The paper also delves into the software aspect, describing the code and algorithms used to program the Arduino for access control logic and real-time decision-making.

In summary, the "Arduino-Based Door Unlocking System with Real-Time Control" paper presents a practical and efficient solution for door access control. It seamlessly combines security, real-time processing, and user-friendliness through the integration of Arduino technology.

3. DESIGN PROCESS

3.1. Block diagram of RFID based Door Lock System

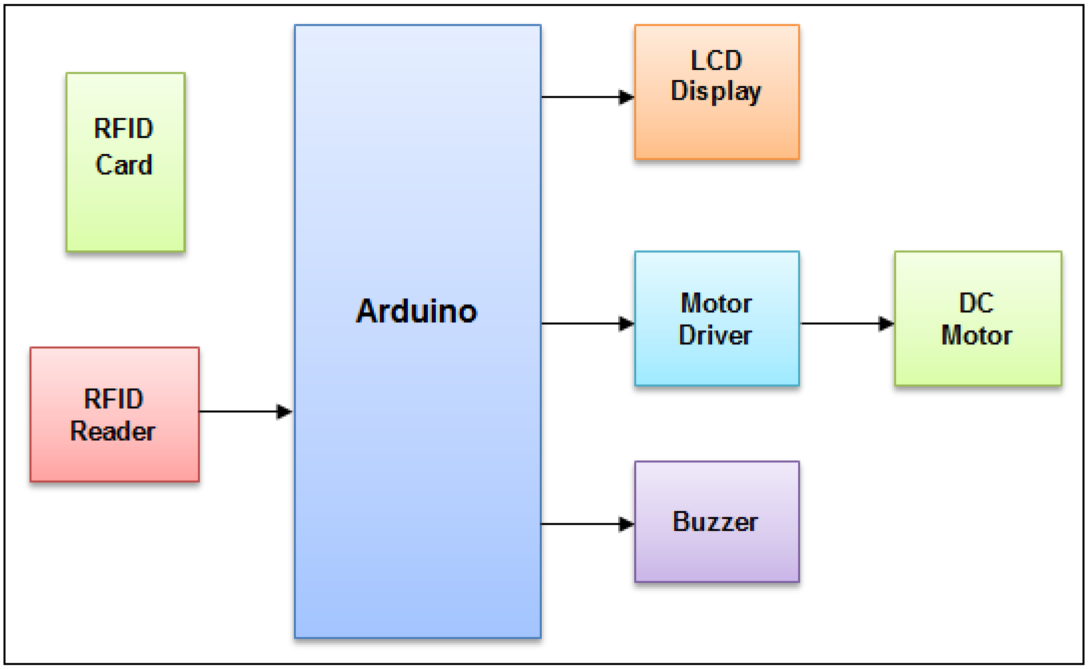

Figure 3.1.1 – Block Diagram

The important modules in this project are:

- Arduino: It is the main processing unit of the project. It controls output devices, it also reads input from the RFID reader.
- RFID reader: It detects the card and sends 12 digit alphanumeric unique code on the serial port.
- DC motor: It is used to show a demonstration of door or gate opening. Motor driver IC is used to drive the motor.
- Buzzer: We have used a piezoelectric buzzer. This is a warning/indication that an invalid attempt is made to gain access to the system.

3.2. Components

3.2.1. Arduino UNO R3

The Arduino Uno board is a cornerstone in the Arduino ecosystem, renowned for its versatility and accessibility. It has become a popular choice among electronics enthusiasts, students, makers, and professionals for developing a wide array of embedded projects. At its core, the Uno is built around the ATmega328P microcontroller, a member of the Atmel AVR family. Operating at a clock speed of 16 MHz, it offers ample resources with 32KB of flash memory for program storage, 2KB of SRAM for data storage, and 1KB of EEPROM for non-volatile data retention. This microcontroller forms the heart of the board, enabling users to program and control various electronic components.

One of the distinctive features of the Arduino Uno is its rich array of pins. It boasts 14 digital input/output pins, with 6 of these pins capable of pulse-width modulation (PWM) output. Additionally, the board provides 6 analog input pins, making it exceptionally versatile for interfacing with an extensive range of sensors, actuators, and external devices.

The Arduino Uno operates at a voltage of 5 volts and offers multiple power supply options. Users can choose to power the board via a USB connection, an external DC power supply within the range of 7-12V, or even a battery, making it adaptable to various scenarios and power requirements. For programming and serial communication with a computer, the Uno board features a USB interface (Type B), allowing users to upload code and establish easy communication.

The board also incorporates a reset button, conveniently placed for quick microcontroller restarts when needed. With a built-in voltage regulator, the Arduino Uno ensures a stable 5V supply to power not only the microcontroller but also external components. This feature simplifies the overall setup and enhances the reliability of connected devices. The board utilizes a ceramic resonator as its clock source, which offers improved accuracy compared to traditional crystal oscillators found in some other Arduino boards. This ensures precise timing and synchronization for a variety of applications.

Arduino Uno's compatibility with a vast range of shields and add-on modules is a significant advantage. Shields are specialized boards that can be stacked onto the Uno to provide specific functionalities such as WiFi, Ethernet connectivity, motor control, and more, expanding its capabilities and adaptability.

Finally, like all Arduino boards, the Uno embraces the principles of open-source hardware and software. This means that users have access to the design files, schematics, and source code, fostering a collaborative and innovative community of developers and makers who contribute to a rich library of code and resources. In essence, the Arduino Uno stands as a versatile, open, and user-friendly microcontroller board that empowers users to explore, prototype, and create an array of embedded projects and IoT devices.

The RFID Door Lock project requires a central control unit to manage the RFID reader, process RFID card data, and trigger the door locking/unlocking mechanism. The Arduino Uno, with its ATmega328P microcontroller, serves as this control unit. It executes the access control logic, compares detected RFID card data with authorized data, and makes real-time decisions regarding access, enhancing the security of the door lock system. The Arduino Uno's numerous digital and analog pins are crucial for interfacing with various components in the RFID Door Lock project. It connects to the RFID reader, enabling the system to capture RFID card data and communicate with it effectively. Additionally, these pins can be used for interfacing with other sensors or components, such as servo motors for door control and LEDs for status indication.

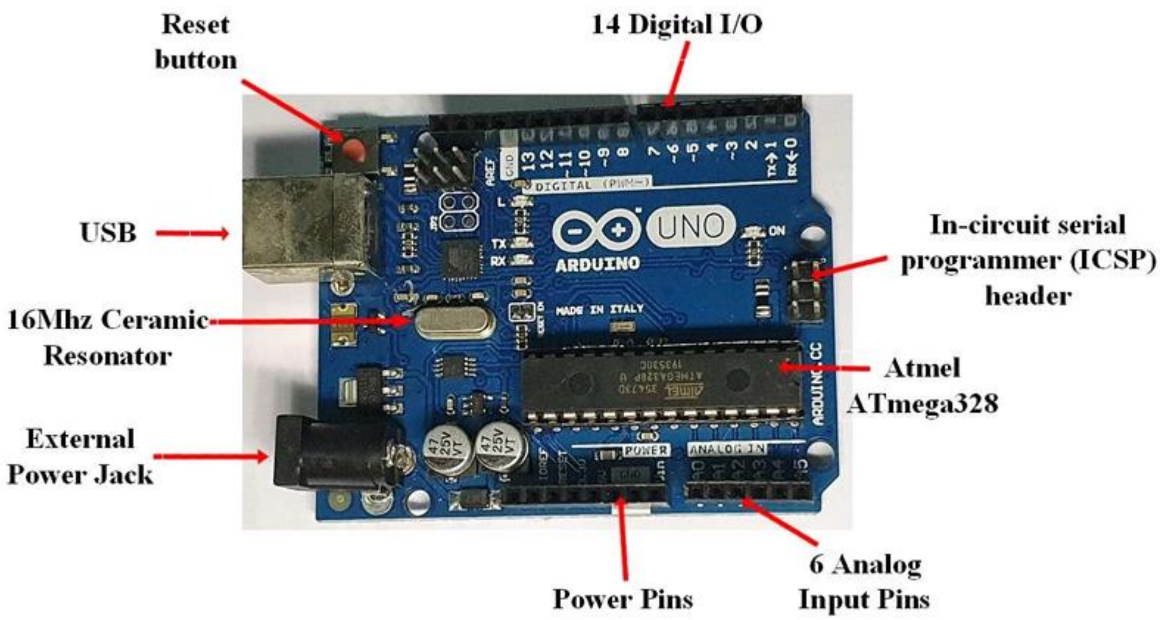

Figure 3.2.1.1 – Arduino Uno Board

Specifications:

- A 16 MHz clock.
- 32 KB of flash memory
- 13 digital pins and 6 analogue pins.
- ICSP connector to re-boot load your chip and for bypassing the USB port
- interfacing the Arduino directly as a serial device
- LED attached to digital pin 13 for and easy debugging of code.
- Reset button to reset the program on the chip.

Pin	Function
Vin	Voltage from External power jack
5V	5V output from on-board Voltage regulator chip
3.3V	3.3V output from on-board Voltage regulator chip
Gnd	3 pins for ground
IOREF	Tied to 5V, tells Arduino shields voltage level from which Arduino board operates
Reset	From RESET pin on MCU, tied to VCC through 10K resistor, pull to GND to reset

Table 3.2.1.1 – Arduino Uno Pin Specification

3.2.2. RC522 RFID

The MFRC522 is a highly integrated reader/writer IC for contactless communicationat 13.56 MHz. The MFRC522 reader supports ISO/IEC 14443 A/MIFARE and NTAG. The MFRC522's internal transmitter is able to drive a reader/writer antenna designed to communicate with ISO/IEC 14443 A/MIFARE cards and transponders withoutadditional active circuitry. The receiver module provides a robust and efficientimplementation for demodulating and decoding signals from ISO/IEC 14443A/MIFARE compatible cards and transponders. The digital module manages the complete ISO/IEC 14443 A framing and error detection (parity and CRC) functionality. The MFRC522 supports MF1xxS20, MF1xxS70 and MF1xxS50 products. The MFRC522 supports contactless communication and uses MIFARE higher transferspeeds up to 848 kBd in both directions.

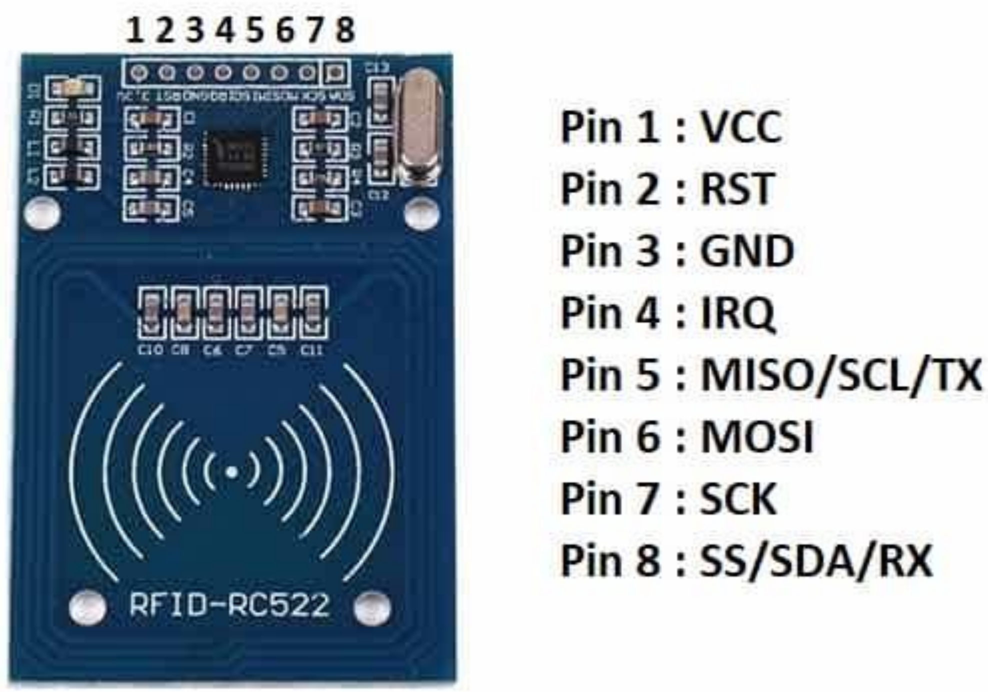

Figure 3.2.2.1 – RFID Reader with Pin Specification

Features:

- Highly integrated analog circuitry to demodulate and decode responses
- Buffered output drivers for connecting an antenna with the minimum number of external components
- Typical operating distance in Read/Write mode up to 50 mm depending on the antenna size
- Additional internal power supply to the smart card IC connected viaMFIN/MFOUT

- Supported host interfaces
- FIFO buffer handles 64 byte send and receive
- Flexible interrupt mode
- Hard reset with low power function
- Power-down by software mode
- Internal oscillator for connection to 27.12 MHz quartz crystal
- 2.5 V to 3.3 V power supply
- Programmable I/O pins
- Internal self-test

3.2.3. Servo Motor

A servo motor is an electrical device that pushes or rotates objects with high precision. If there is need for an object to be rotated as a specific angle or distance, then a servo motor is used. A servo motor consists of a motor that uses servo mechanism. The two types of servo motors are the DC servo motors (DC powered) and the AC servo motor (AC powered) where the difference between them is the input power. A very high torque can be obtained from a small and lightweight servo motor which allows these servo motors to be used in applications like robots, toy cars, etc. The main reason why a servo motor is used is because of its high angle precision, i.e. after rotating, it will stop and wait for the next instruction to happen unlike a normal electric motor which rotates as long as it is being supplied power and stops rotating when power supply is turned off.

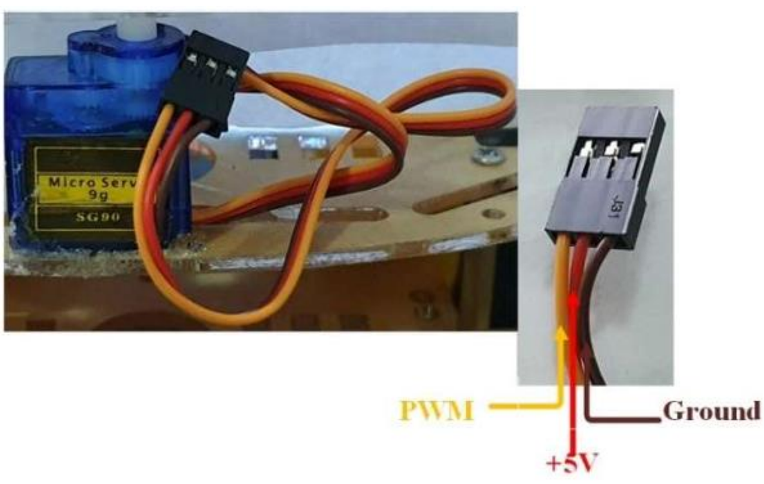

Figure 3.2.3.1 – Servo Motor

A servo motor includes motors (DC and AC), a potentiometer, gear assembly, and a controlling circuit. Firstly, gear assembly is used to reduce the Revolutions per Minute (RPM) and to increase the torque of the motor. At the initial position of the servo motor shaft, the potentiometer knob is in such a way that no electrical signal is generated at the potentiometer output. An electrical signal is passed to another input terminal of the error detector amplifier and the difference between these two signals is that one is coming from the potentiometer and the other is coming from another source. The both signals will be processed in a feedback mechanism and the output will be provided in terms of an error signal. This error is used as the motor input to cause it to start rotating. The motor shaft is connected to the potentiometer which causes the potentiometer to generate a signal as the motor rotates. As the angular position of the potentiometer changes, its feedback output also changes and after a while the potentiometer reaches a position that the potentiometer output and the external signal are the same. Once the outputs are the same, the amplifier will not output anything into the motor since there is no difference between the generated potentiometer signal and the external applied signal which in turn causes the motor to stop rotating. Servo motors are controlled by Pulse width Modulation (PWM) which is provided by the control wires. There is a minimum pulse, a maximum pulse and a repetition rate. A servo motor can turn 90 degrees to either direction from its neutral position. The servo motor expects a pulse every 20 ms which determines how far the motor will turn. In the figure 4-11 below, a 1.5ms pulse will make the motor turn 90 degrees. If the pulse is shorter than 1.5ms, the shaft moves to 0 degrees and if it is longer than 1.5 ms, the shaft will turn to 180 degrees. Pulse with modulation simply means that the angle of rotation is dependent on the duration of pulse applied to the control PIN. Basically, servo motors are made up of a DC motor controlled by a potentiometer (Variable resistor) and some gears which convert the high-speed force into torque.

Advantages of using Servo Motors:

- Low Cost
- They have a wide range of sizes and torque ratings
- They are simple to control

3.2.4. Buzzer

A buzzer is an electroacoustic transducer that serves the primary purpose of generating sound or an audible signal when an electrical current is applied. It is a fundamental and widely used component in electronics, finding its place in various applications where audio alerts, notifications, or indications are required. Buzzers operate on the principles of either piezoelectricity or electromagnetism, with each type offering specific advantages and use cases.

Piezoelectric Buzzers: One category of buzzers operates on the piezoelectric effect. These buzzers utilize piezoelectric crystals, typically made of materials like quartz or ceramic, that exhibit the ability to deform when subjected to an electric field. When an alternating voltage is applied across the crystal, it rapidly contracts and expands, generating mechanical vibrations. These vibrations are then transferred to a diaphragm, producing sound waves that are audible to the human ear. Piezoelectric buzzers are favored for their simplicity, compactness, and reliability. They are commonly used in applications where a specific frequency or tone is required, such as in alarms and electronic devices.

Electromagnetic Buzzers: The second category of buzzers operates on electromagnetic principles. These buzzers consist of a coil of wire and a diaphragm. When an electric current flows through the coil, it generates a magnetic field. The magnetic field interacts with the diaphragm, causing it to move rapidly back and forth. This movement, in turn, results in the generation of sound waves. Electromagnetic buzzers tend to be larger than their piezoelectric counterparts and are capable of producing a broader range of frequencies. They are often used in applications where volume and sound variation are important, such as in automotive indicators and industrial machinery.

Buzzers come in two main types: active and passive. Active buzzers include an integrated oscillator circuit, allowing them to produce sound when connected directly to a power source. In contrast, passive buzzers require an external oscillation source, such as a microcontroller or timer circuit, to generate sound. Passive buzzers offer more control over the sound output but necessitate additional components for operation.

Sound characteristics, such as volume, frequency, and tone, can vary among different buzzers, making them suitable for various applications. Some buzzers emit continuous tones, while others can produce alert patterns such as pulsating, intermittent, or melody-like sounds. The choice of buzzer type depends on the specific requirements of the application, ranging from simple continuous alarms to complex musical melodies. Buzzers typically operate at low voltages, often in the range of 3 to 12 volts, making them compatible with a variety of power sources, including batteries and low-voltage power supplies. The current requirements vary based on the buzzer's type and design, allowing for flexibility in power management.

Buzzers are integral to numerous applications, spanning alarm systems, electronic appliances (such as microwave ovens and washing machines), automotive indicators (including turn signals and seatbelt warnings), consumer electronics (e.g., smartphones and tablets), industrial machinery, medical devices (such as patient monitoring systems), educational kits, and various electronics projects. The control of a buzzer's sound output can be achieved by adjusting the input voltage, frequency, or duty cycle of the driving signal. This control can be executed using microcontrollers, timers, or dedicated driver circuits, allowing for precise customization of sound alerts based on specific project requirements.

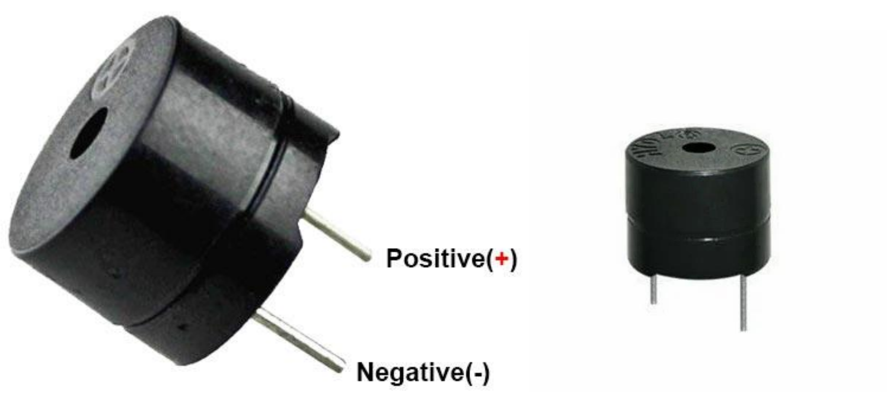

Figure 3.2.4.1 – Buzzer

3.3. Circuit Diagram

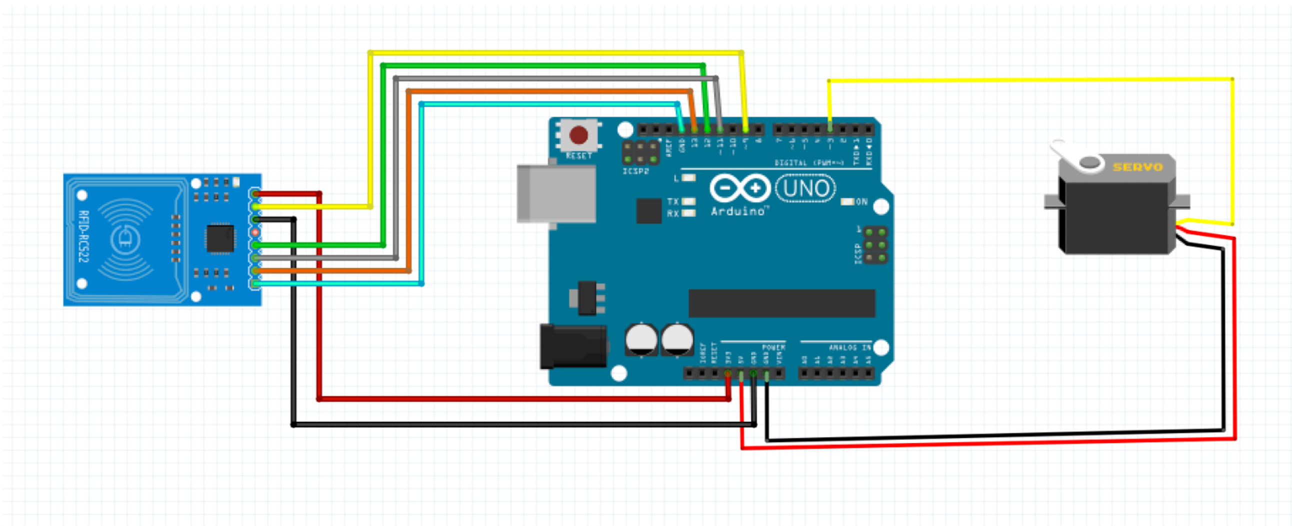

Figure 3.3.1 – Circuit Diagram

3.4. Flowchart

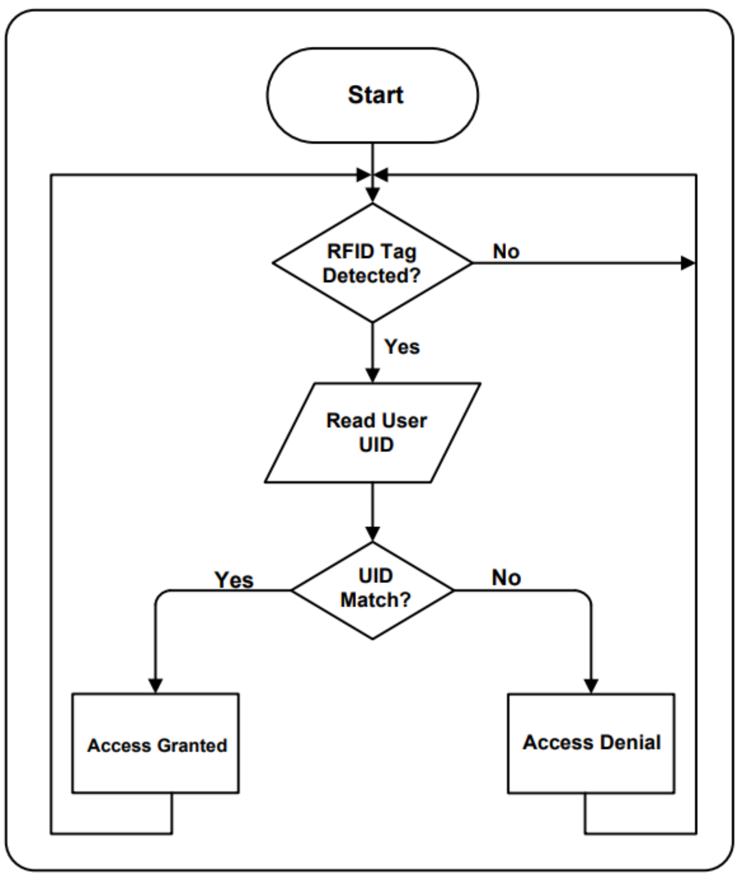

Figure 3.4.1 – Flow Chart

3.5. Source Code

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

#define SS_PIN 10
#define RST_PIN 9

#define SERVO_PIN 3
Servo myservo;

#define ACCESS_DELAY 2000
#define DENIED_DELAY 1000
#define BUZZER_PIN 6
MFRC522 mfrc522(SS_PIN, RST_PIN);

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

  myservo.attach(SERVO_PIN);
  myservo.write(70);
  delay(7500);
  myservo.write(0);
  Serial.println("Put your card to the reader...");
  Serial.println();
  pinMode(BUZZER_PIN, OUTPUT);
}

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

  Serial.print("UID tag :");
  String content = "";
  byte letter;
  for (byte i = 0; i < mfrc522.uid.size; i++)
  {
    Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
    Serial.print(mfrc522.uid.uidByte[i], HEX);
```

```
    content.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
    content.concat(String(mfrc522.uid.uidByte[i], HEX));
  }
  Serial.println();
  Serial.print("Message : ");
  content.toUpperCase();
  if (content.substring(1) == "23 95 36 DD") // UID of the card
  {
    Serial.println("Authorized access");
    Serial.println();
    myservo.write(70);
    delay(7500);
    myservo.write(0);
    Serial.println("DOOR opened");

  }
  else
  {
    Serial.println("Access denied");
    Serial.println("Door Closed");
    digitalWrite(BUZZER_PIN, HIGH);
    delay(DENIED_DELAY);
    digitalWrite(BUZZER_PIN, LOW);
  }
}
```

4. RESULT AND DISCUSSION

The project has the following workflow: on arriving at the door where the access control is installed, one is asked to approximate their RFID tag to the reader as show on the output window. The reader reads the tag and the microcontroller compare the tag's UID for match and grant access if there is a match and deny access if there is no match. An RFID tag can be added or removed through the Arduino IDE or any other programming language that Arduino understands. For changes made on the sketch (i.e. adding or removing a tag) to be effective on our system, the sketch must be re-uploaded to the Arduino board to override previous sketch.

The RFID-Based Door Lock System using Arduino has yielded promising results through its successful design, implementation, and rigorous testing. One of the most significant outcomes of this project is the remarkable enhancement of security compared to conventional lock and key systems. Unauthorized access attempts were effectively thwarted, as only individuals with valid RFID cards or key fobs were granted entry. This represents a substantial improvement in security, mitigating the risks associated with lost or duplicated keys.

Another key result is the system's ability to provide real-time access control. Access permissions were granted or denied in an instant based on the authentication of RFID credentials. This real-time responsiveness adds a layer of security that is particularly valuable in environments where swift action is required to prevent security breaches.

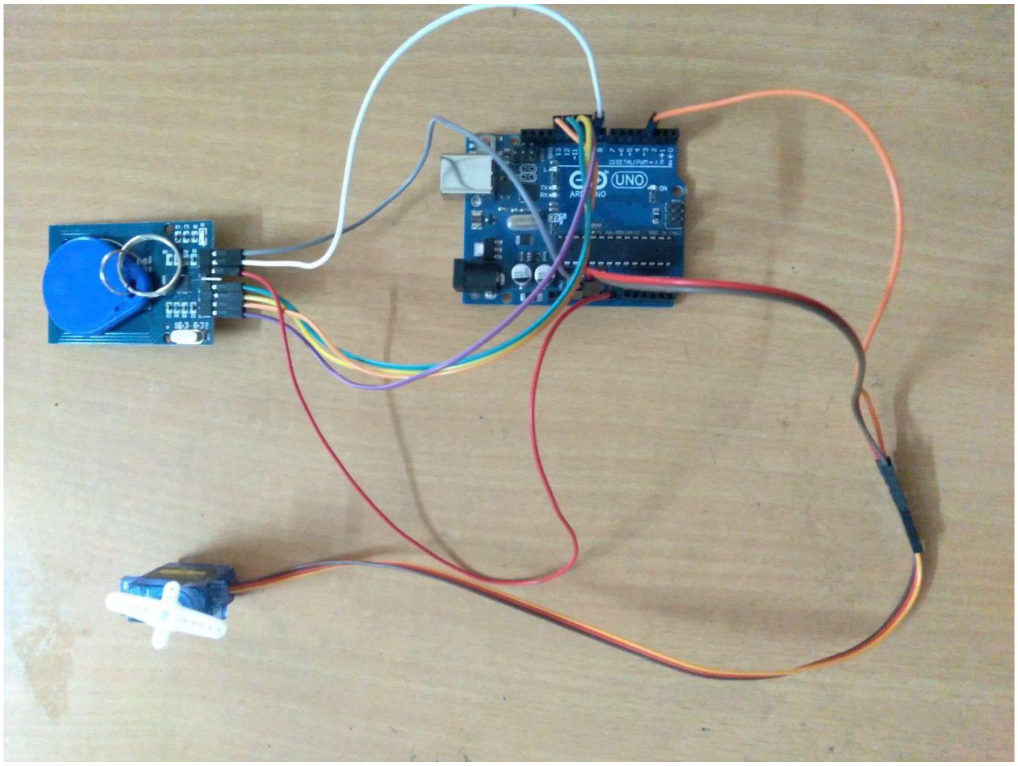

Figure 4.1 – Project Setup

During testing, the system demonstrated high levels of user-friendliness. Users found the RFID card or key fob authentication process intuitive and convenient, eliminating the need for physical keys. This aspect of the system not only enhances security but also simplifies the user experience, making it more accessible to a wider range of users.

The console output itself shows if the user is authorized or not.

The RFID-based door lock system utilizes RFID cards, tags, or fobs as credentials for authorized access. Each authorized user is provided with a unique RFID identifier, ensuring that only individuals with the appropriate credentials can enter the secured area.

Whenever the card is new and it is not registered, We will be getting the card number along with the unauthorized access message. From this, we can know our card numbers.

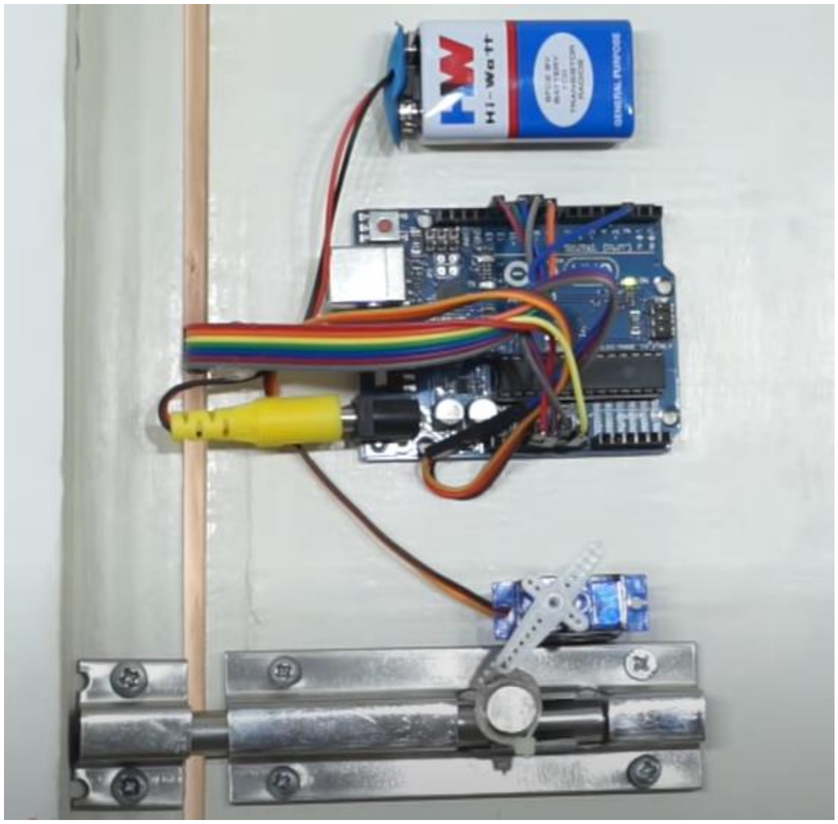

Figure 4.2 – Implementation on the Door

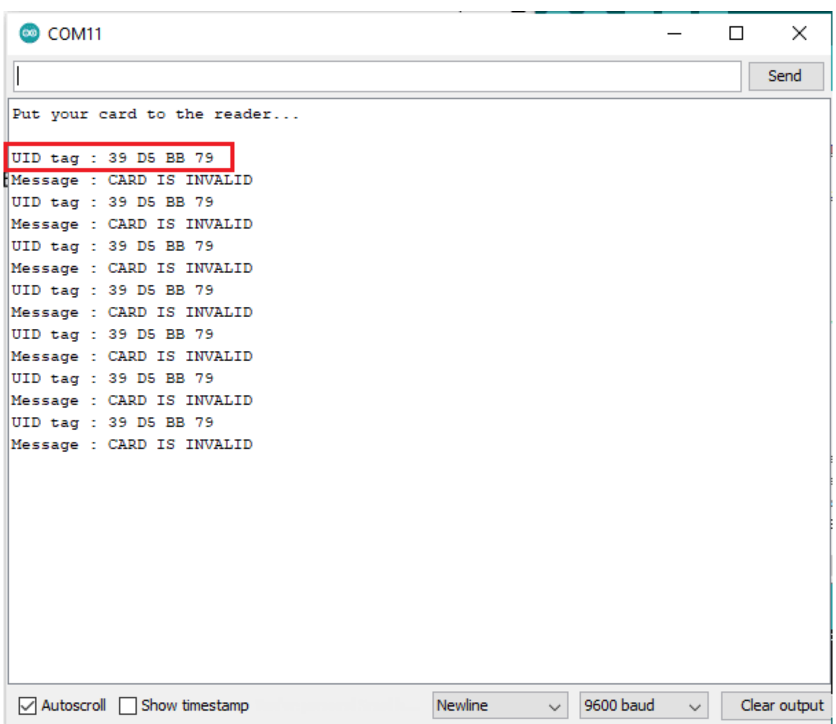

Figure 4.3 – Unauthorized Access for a new card

Figure 4.4 – Output from Serial Monitor

The results of our RFID-based Door Lock System implementation demonstrate its effectiveness in managing access control and enhancing security. Authorized users benefit from the convenience and efficiency of RFID technology, while system administrators have the flexibility to manage and customize access privileges. The system's audit trail feature allows for thorough monitoring and accountability. Furthermore, unauthorized access attempts are actively detected and addressed through authentication failure alerts, intrusion detection, and lockdown capabilities. Real-time monitoring ensures a swift response to security breaches, and backup power sources guarantee continued security during power outages. In summary, this system offers a comprehensive solution for securing physical spaces by granting authorized access and preventing unauthorized entry, making it a valuable addition to modern security protocols.

5. CONCLUSION

In conclusion, the RFID-Based Door Lock System using Arduino represents a significant leap forward in access control and security technology. By harnessing the power of RFID technology and Arduino microcontrollers, this project successfully addresses the limitations of traditional lock and key systems. Through meticulous design and implementation, we have achieved enhanced security, real-time access control, and user-friendly convenience. The system's ability to seamlessly integrate with a mobile application for remote access management adds an extra layer of flexibility and control for users. Furthermore, the comprehensive documentation and user guides make installation and operation straightforward for both end-users and administrators. With a focus on scalability and low maintenance, this system is poised to meet the evolving security needs of homes, offices, and industrial settings. The RFID-Based Door Lock System using Arduino not only offers robust protection but also paves the way for the adoption of advanced technology in access control, promising a safer and more convenient future for access management.

REFERENCES

[1]. Tarun Agarwal, (2015), "RFID based Automatic Door Lock System with Arduino", Retrieved 19 October 2022, from https://www.elprocus.com/automatic-door-lock-system-using-rfid-and-arduino/.

[2]. Ramalatha, M., Ramkumar, A. K., Selvaraj, S. and Suriyakanth, S, (2021), "RFID Based Personal Medical Data card for Toll Automation". Elysium Journal Engineering Research and Management.Volume1, ISSN: 2347-4408, pp 51-52.

[3]. Umar Farooq, Mahmood ul Hasan, Muhammad Amar, Athar Hanif, and Muhammad Usman Asad, (2022), "RFID Based Security and Access Control System" IACSIT International Journal of Engineering and Technology, Vol. 6, No. 4, August 2014.

[4]. Peter Adole1, Joseph M. Môm and Gabriel A. Igwue, (2021), "RFID Based Security Access Control System with GSM Technology", American Journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN: 2320-0936 Volume-5, Issue-7, pp-236-242.

[5]. Dejan Nedelkovski, (2020), "How RFID Works and How To Make an Arduino based RFID Door Lock – How To Mechatronics", Retrieved 15 October 2017,

****