INTERNET OF THINGS LAB

(CASE STUDY)

“DOOR LOCKING SYSTEM”

BACHELOR OF TECHNOLOGY IN INFORMATION TECHNOLOGY

Submitted By

N.Mohana Likitha (A21126511043)

S.Venkata Vishnu (A21126511056)

T.Bhavana (A21126511059)

Y.Lasya Sahithi (A21126511063)

Shaik Rijwan (A21126511200)

DEPARTMENT OF INFORMATION TECHNOLOGY, ANIL NEERUKONDA INSTITUTE OF TECHNOLOGY AND SCIENCES(UGC AUTONOMOUS)

(Affiliated to AU, Approved by AICTE and Accredited by NBA&NAAC with ‘A’ Grade)Sangivalasa-531162, Bheemunipatnam Mandal, Visakhapatnam District (A.P).

(2022–2023)

ACKNOWLEDGEMENT

With great pleasure we want to take this opportunity to express our heartfeltgratitude to all the people who helped in learning this course**.**

We awe our tributes to **Prof.M.Rekha Sundari,** Head of the Department, Information technology, ANITS, for providing us with the required facilities for the implementation of the project work.

On successful completion of our **Internet of Things (IOT) LAB**, we wish to express our sincere thanks and gratitude for lecturer in charge **Mrs.A.Surekha** mam, Assistant Professor, of Information Technology, ANITS for analyzing problems associated with our project work and for guiding us throughout the project. We express our warm and sincere thanks for the encouragement, untiring guidance and the confidence she had shown in us. We are immensely indebted for her valuable guidance throughout our project.

We thank all the staff members of IT department for their valuable advices and for providing resources as and when required.

Submitted by:

N.Mohana Likitha(A21126511043)

S.Venkata Vishnu(A21126511056)

T.Bhavana(A21126511059)

Y.Lasya Sahithi(A21126511063)

Shaik Rijwan(A21126511200)

ANIL NEERUKONDA INSTITUTE OF TECHNOLOGY AND SCIENCES

(UGC AUTONOMOUS)

(Affiliated to AU, Approved by AICTE and Accredited by NBA&NAAC with 'A' Grade)Sangivalasa, Bheemunipatnam Mandal, Visakhapatnam District (A.P).

PRAGNANAM BRAHMA

ANITS

CERTIFICATE

This is to certify that the project reported entitled **"DOOR LOCKING SYSTEM"** submitted by **N.Mohana Likitha, S.Venkata Vishnu, T.Bhavana, Y.Lasya Sahithi, Shaik Rijwan** in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** in **Information Technology** of **Anil Neerukonda Institute of Technology and Sciences**, Visakhapatnam is a record of bonafide work carried out under my guidance and supervision.

.

Lecturer Incharge	Head of the Department
Mrs.A.Surekha **Department of IT** **ANITS**	**Prof.M.Rekha Sundari** **Department of IT** **ANITS**

DECLARATION

We hereby declare that the project work entitled "**DOOR LOCKING SYSTEM"** submitted to Anil Neerukonda Institute of Technology and Sciences is a record of an original work done by **N. MOHANA LIKITHA (A21126511043), S. Venkata Vishnu (A21126511056),T. Bhavana (A21126511059),Y. LASYA SAHITHI (A21126511063)** ,**SHAIK RIJWAN (A21126511200)**, under the esteemed guidance of **Mrs. A. Surekha** Assistant Professor of Information Technology , Anil Neerukonda Institute of Technology and Sciences and this project work is submitted in partial fulfillment of the requirements for the award of degree bachelor of technology in information technology . This entire project is done to the best of our knowledge and not submitted for the award of other degree in any other universities.

PROJECT STUDENTS

N.Mohana Likitha(A21126511043)

S.Venkata Vishnu(A21126511056)

T.Bhavana(A21126511059)

Y.Lasya Sahithi(A21126511063)

Shaik Rijwan(A21126511200)

INDEX

DOOR LOCKING SYSTEM

ABSTRACT

This project proposes an innovative approach to door locking systems by integrating them with the Internet of Things (IoT) technology. The aim is to develop a smart and connected door locking system that enhances security, convenience, and accessibility for users. The integration of IoT enables remote monitoring, control, and automation of the door lock, transforming traditional access control mechanisms. The core components of the IoT-enabled door locking system include a microcontroller-based locking mechanism, wireless connectivity modules, and a cloud-based management platform. The microcontroller serves as the control unit, managing locking/unlocking operations and interfacing with various sensors and actuators. Wireless connectivity modules such as Wi-Fi or Bluetooth enable communication between the door lock and external devices, such as smartphones or smart home hubs.The cloud-based management platform provides a centralized interface for users to remotely monitor and control the door lock. Through a mobile application or web interface, users can lock/unlock the door, grant access to authorized individuals, and receive real-time notifications for security events. Additionally, the system can be integrated with other IoT devices and smart home ecosystems for seamless automation and integration.The implementation of the IoT-enabled door locking system involves hardware design, firmware development, and integration with cloud services. Advanced security measures, including encryption protocols and secure authentication mechanisms, are implemented to safeguard communication and protect against unauthorized access.The evaluation of the system includes testing its functionality, reliability, and security features in real-world scenarios. Performance metrics such as response time, connectivity stability, and power consumption are assessed to ensure optimal operation. User feedback and usability studies are conducted to identify user preferences and areas for improvement.

1.INTRODUCTION

The Door Locking System Project with IoT integration represents a pioneering endeavor aimed at revolutionizing traditional access control mechanisms. By merging the capabilities of Internet of Things (IoT) technology with conventional door locking systems, this project seeks to create a smart, connected, and secure solution for modern security challenges.

In today's dynamic environment, the demand for enhanced security and convenience is ever-growing. Traditional door locking systems, while effective, often lack the flexibility and accessibility required to meet the needs of contemporary users. This project addresses these limitations by harnessing the power of IoT to enable remote monitoring, control, and automation of door locks.

Through the integration of IoT technology, users gain the ability to remotely manage access to their premises, receive real-time notifications of security events, and seamlessly integrate their door locking system with other smart devices and home automation platforms. This not only enhances security but also elevates convenience and user experience to new heights.

This introduction sets the stage for the exploration of how the synergy between IoT and door locking systems can lead to innovative solutions that redefine the standards of security and accessibility in both residential and commercial settings.

1.2 IOT Definition:

The Internet of Things (IoT) refers to a network of interconnected devices, objects, and systems that communicate and exchange data over the internet. These devices, equipped with sensors, actuators, and connectivity modules, can collect and transmit data to centralized platforms or other connected devices, enabling remote monitoring, control, and automation. IoT technology facilitates the integration of physical objects into digital ecosystems, enabling them to interact with each other and with humans in intelligent ways. By leveraging IoT, devices can be made smarter, more efficient, and more responsive to user needs, leading to enhanced convenience, productivity, and insights across various domains, including smart homes, healthcare, transportation, agriculture, and industrial automation. The widespread adoption of IoT is driving digital transformation and ushering in an era of interconnectedness, where everyday objects become part of a vast networked infrastructure, revolutionizing the way we live, work, and interact with the world around us.

2.SYSTEM SPECIFICATIONS

2.1 Functional Requirements:

Functional Requirements for Door Locking System Project with IoT Integration:

1.Remote Locking and Unlocking: The system should allow users to remotely lock and unlock doors using a mobile application or web interface.

2.Access Control: Users should be able to grant temporary or permanent access to individuals through the mobile application, specifying the duration and level of access (e.g., one-time access, recurring access).

3.User Authentication: The system should support multiple authentication methods, including biometric (e.g., fingerprint recognition), PIN codes, and digital keys, ensuring secure access control.

4.Real-time Notifications: Users should receive real-time notifications on their mobile devices for door status changes (e.g., locked, unlocked), unauthorized access attempts, or security breaches.

5.Integration with Smart Home Ecosystems: The system should seamlessly integrate with other IoT devices and smart home platforms, allowing for automation and synchronization of door locking actions with other smart home functionalities (e.g., lighting, security cameras).

6.Remote Monitoring: Users should be able to remotely monitor the status of their door lock, including access logs, battery status, and sensor readings (e.g., door position sensor), providing insights into the security and operational status of the system.

7.Tamper Detection: The system should include tamper detection mechanisms to alert users in case of unauthorized attempts to tamper with the door lock or its components.

8.Power Management: Efficient power management features should be implemented to optimize battery life for battery-operated door locking systems, with low-battery notifications and backup power options.

9.Scalability: The system architecture should be scalable to accommodate multiple doors and users, supporting a growing number of devices and users without compromising performance or security.

10.Secure Communication: Secure communication protocols, such as TLS encryption, should be employed to ensure the confidentiality and integrity of data transmitted between the door locking system, mobile applications, and cloud-based services.

2.2 Non Functional Requirements:

Non-Functional Requirements for Door Locking System Project with IoT Integration:

1.Security: The system must employ robust security measures to prevent unauthorized access, including encryption of data transmission, secure storage of user credentials, and resistance to hacking or tampering.

2.Reliability: The door locking system should operate reliably under varying conditions, with minimal downtime or system failures, ensuring uninterrupted access control.

3.Scalability: The system architecture should be scalable to accommodate a growing number of users, devices, and door locks, without compromising performance or security.

4.Performance: The system should have low latency and high responsiveness, with quick authentication and door locking/unlocking actions to provide a seamless user experience.

5.Interoperability: The system should be interoperable with a wide range of devices, platforms, and protocols, allowing for integration with existing infrastructure and future expansion.

6.Usability: The user interface (UI) of the mobile application and web interface should be intuitive, user-friendly, and accessible to users of varying technical proficiency, promoting ease of use and adoption.

7.Compatibility: The system should be compatible with a variety of door types, locking mechanisms, and architectural configurations commonly found in residential and commercial buildings.

8.Power Efficiency: For battery-operated door locks, the system should optimize power consumption to maximize battery life, with features such as low-power standby mode and efficient use of energy resources.

9.Data Privacy: User data, including personal information and access logs, should be handled with utmost confidentiality and comply with privacy regulations such as GDPR, ensuring user privacy and data protection.

10.Maintainability: The system should be easy to maintain and upgrade, with modular components and clear documentation, facilitating troubleshooting, software updates, and hardware replacements as needed.

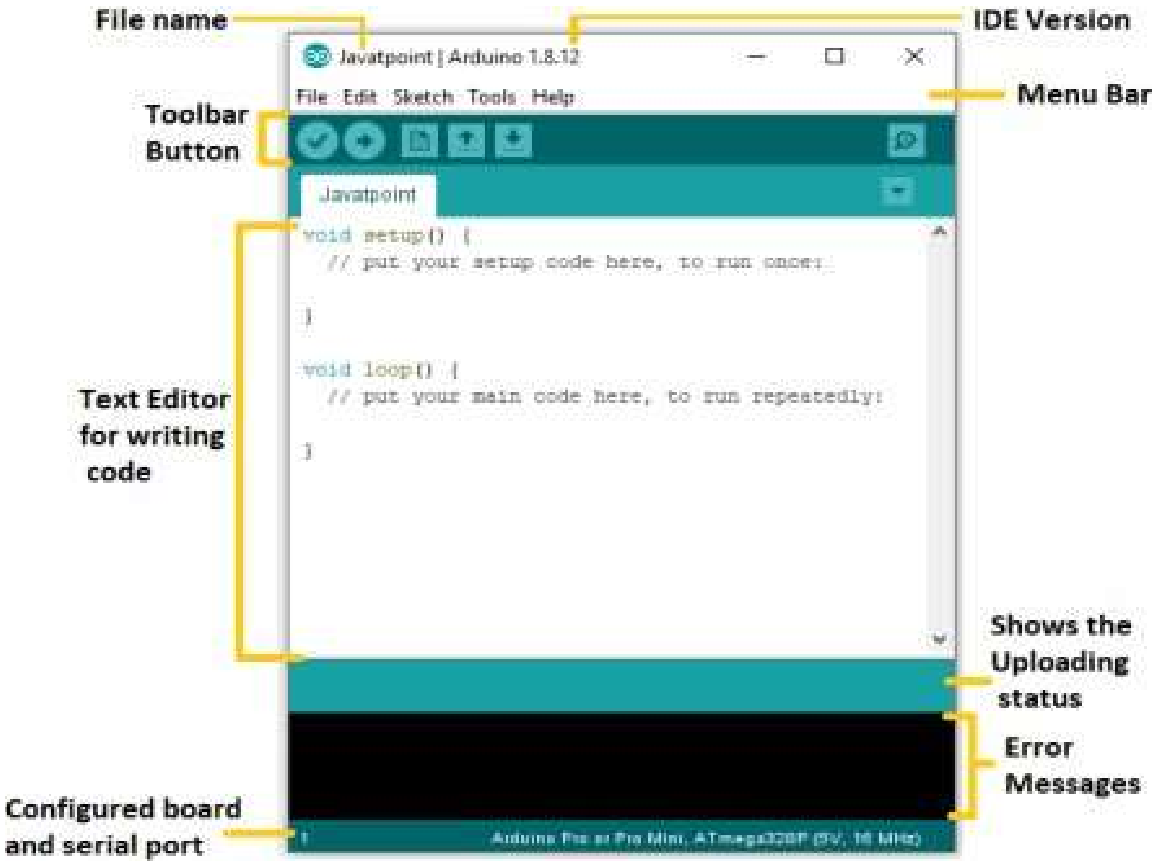
11.Integration with Legacy Systems: Provision should be made for integrating the IoT-enabled door locking system with legacy access control systems or security infrastructure already in place, ensuring seamless transition and compatibility.

12.Environmental Considerations: The system should be designed with environmental sustainability in mind, minimizing energy consumption, reducing electronic waste, and using eco-friendly materials where possible.

3.SYSTEM SOFTWARE

3.1 Arduino IDE:

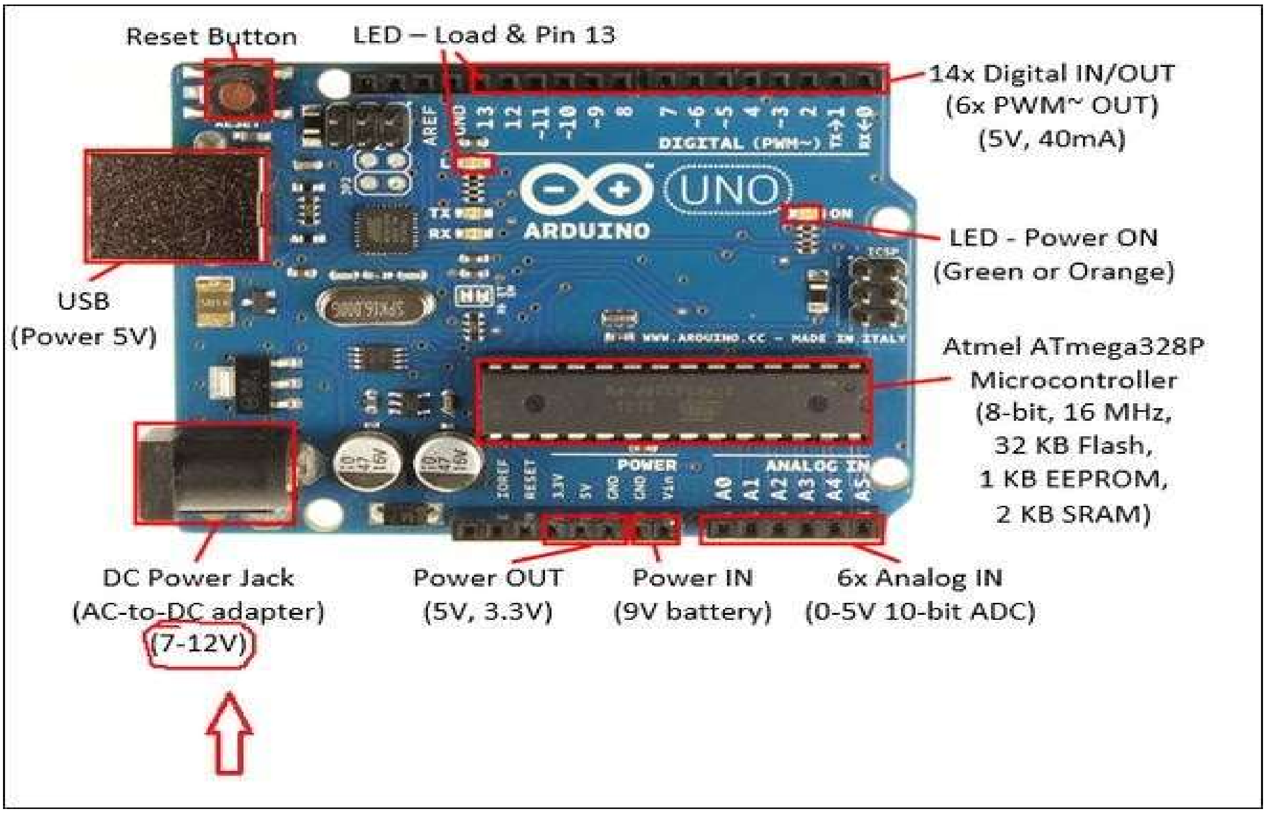
The Arduino Integrated Development Environment - or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console,a toolbar with buttons for common functions and a series of menus. It connects to the Arduino hardware to upload programs and communicate with them.



4.SYSTEM HARDWARE

4.1 Arduino Board:

Arduino is an open-source platform used for building electronics projects. Arduino consists of both a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or IDE (Integrated Development Environment) that runs on your computer, used to write and upload computer code to the physical board

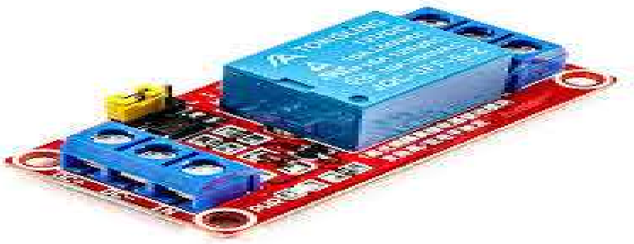


4.2 Solenoid Lock:

A solenoid unlock mechanism is a compact and efficient solution for door locking systems. When triggered by a control signal, the solenoid swiftly converts electrical energy into linear motion, either extending or retracting a bolt or latch to unlock the door. This electromechanical action occurs rapidly, allowing for seamless and secure access. Solenoid unlocks are favored for their reliability, responsiveness, and space-saving design, making them ideal for integration into electronic door locks across residential, commercial, and industrial settings.

4.3 Relay Module:

A relay module is a versatile electronic component commonly used in various applications, including door locking systems. It acts as an electrical switch that can be controlled by a low-voltage signal, typically from a microcontroller or other control circuitry. When the control signal is applied, the relay module toggles the state of its internal switch, allowing or interrupting the flow of high-voltage electrical current to connected devices such as solenoids or electromechanical locks. This simple yet effective functionality makes relay modules essential for enabling remote control, automation, and integration with IoT technologies in door locking systems.

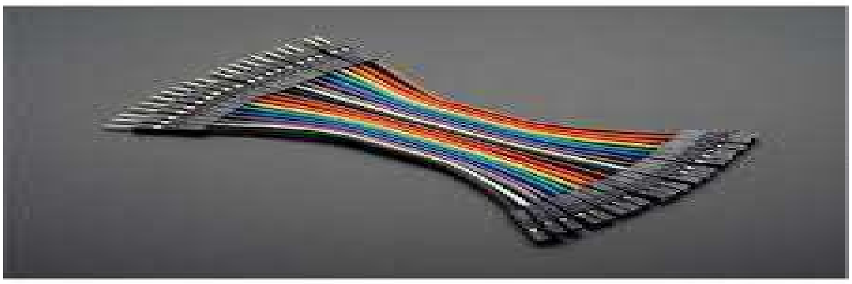


4.4 RFID Tags:

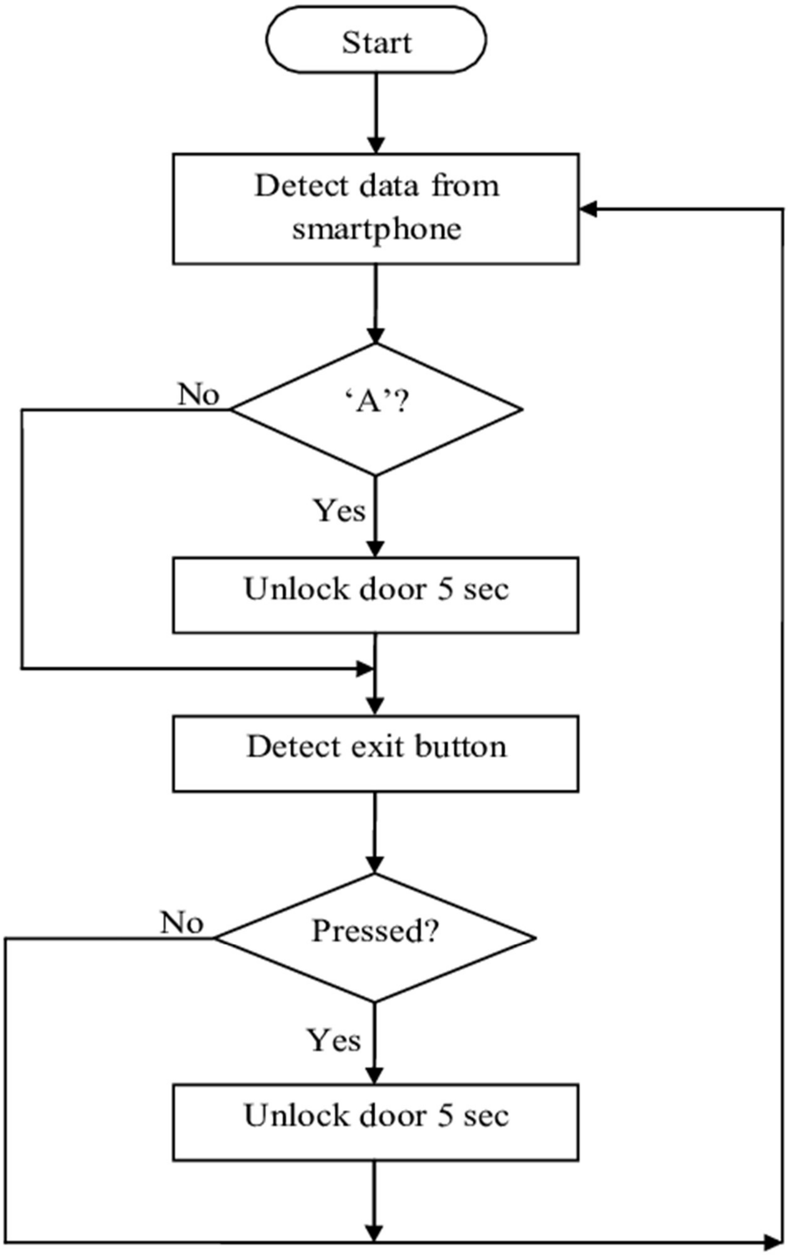
RFID (Radio Frequency Identification) tags are small electronic devices equipped with a microchip and an antenna. They're designed for identifying and tracking objects or assets remotely using radio waves. There are different types of RFID tags, including passive, active, and semi-passive. Passive tags rely on the energy transmitted by RFID readers to operate, while active tags have their own power source, typically a battery. Semi-passive tags use a combination of both approaches. RFID tags are used in various industries for applications such as inventory management, asset tracking, access control, and supply chain logistics, offering benefits like improved efficiency and accuracy in tracking and managing assets or inventory.

4.5 Jumper Wire:

Jumper wires are essential components in electronics projects, serving as flexible connectors to establish electrical connections between various components on a breadboard, circuit board, or prototype. These wires typically consist of thin, flexible insulated conductors with pins or connectors on each end, allowing for easy insertion and removal. By simply plugging them into the desired locations on a breadboard or connecting them to electronic components, jumper wires enable seamless prototyping, experimentation, and circuit testing without the need for soldering. Their versatility and ease of use make jumper wires indispensable for hobbyists, students, and professionals alike in creating and testing electronic circuits efficiently.



5.FLOWCHART



Start
Detect data from smartphone
No
'A'?
Yes
Unlock door 5 sec
Detect exit button
No
Pressed?
Yes
Unlock door 5 sec

6.METHODOLOGY

6.1 Description of the Methodology:

The development methodology for a door locking system with IoT integration involves a structured approach to ensure the successful implementation of the project. Initially, requirements are analyzed to define the functional and non-functional aspects, considering user needs, security requirements, and integration with IoT platforms. Following this, the system design phase involves architecting the hardware and software components, selecting suitable IoT modules, and determining authentication methods. Prototyping and development entail the creation of firmware/software for controlling the locking mechanism and implementing secure communication protocols. Integration and testing involve combining hardware and software components, conducting thorough testing, and evaluating system performance under various conditions. Once tested, the system is deployed in real-world environments, and optimization efforts focus on power efficiency, scalability, and interoperability. Finally, maintenance and support protocols are established to ensure ongoing system reliability and user satisfaction through updates, technical assistance, and troubleshooting. This structured methodology enables developers to systematically design, implement, and deploy a robust door locking system with IoT integration to meet modern security needs and user expectations.

6.2 Overall flow of project:

Let me provide you with a brief description of what the program does

1. **Library and Serial Configuration:-**
- The program includes the "Adafruit RFID tag " library for interfacing with a rfid tag.
- It uses SoftwareSerial to create a serial communication interface (mySerial) on pins 2 and 3.

2. **Fingerprint Sensor Initialization:-**
- An instance of the Adafruit_Rfid tag class named `finger` is created, associated with the `mySerial` interface.

3. **Pin Definitions:-**
- The program defines the pin for a relay (RELAY_PIN) that controls an electronic lock or similar device.
- The relay is initially turned off (HIGH), indicating a locked state.

4. **Access Delay:-**
- An access delay (ACCESS_DELAY) is set to 3000 milliseconds (3 seconds). This is the duration the lock will remain open after a successful Rfid tag match.

5. **Setup Function:-**
- The setup function initializes the Rfid tag and checks the password.
- If the password verification fails, the program enters an infinite loop.

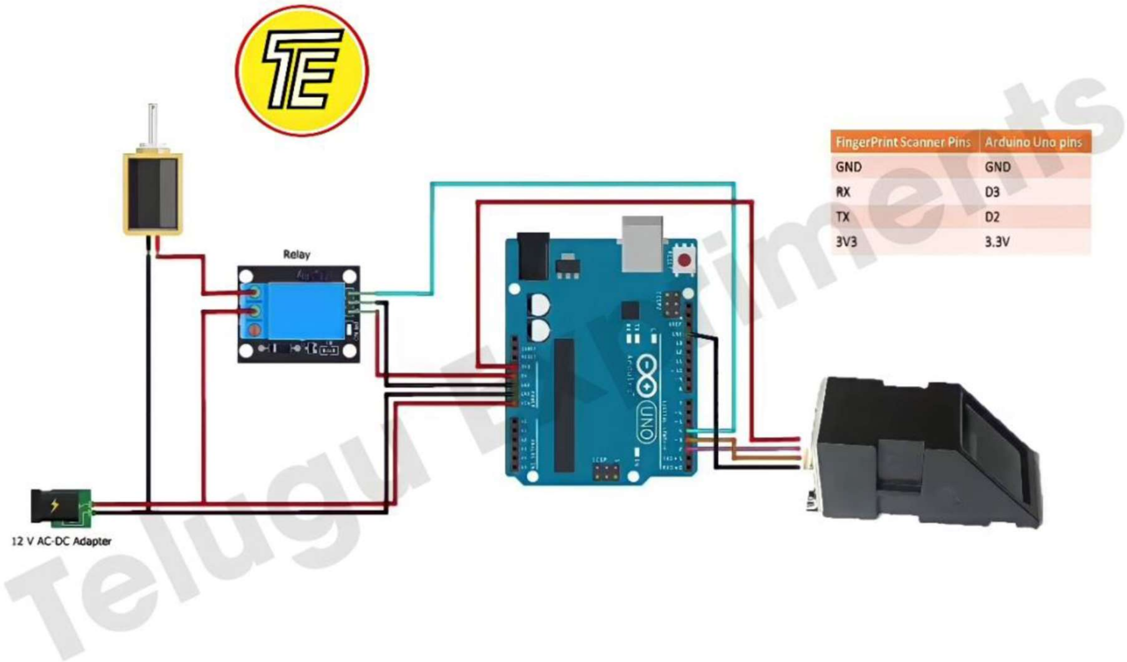
6. **Main Loop:-**
- The `loop` function continuously checks for a rfid match.
- If a Rfid match is found (via the getRfid function), it unlocks the relay (sets RELAY_PIN to LOW), waits for the specified access delay, and then locks the relay again.

7. **getRfid Function:-**
- This function captures a Rfid image, converts it to a template, and performs a fast search to find a matching template.
- If a match is found, it returns the corresponding Rfid ID; otherwise, it returns -1.

8. **Delay:-**
- There are delays included in the `loop` function to avoid continuous scanning and to provide some time for other processes.

In summary, this program controls access to a system using a Rfid tag. It initializes the sensor, checks the password, and continuously scans for Rfid. If a match is found, it unlocks a relay for a specified duration before locking it again. This kind of application is commonly used for biometric security systems.

6.3 Environmental Setup:



7.IMPLEMENTATION

Program in Embedded C or Assembly language must be placed here. Comments must be included.

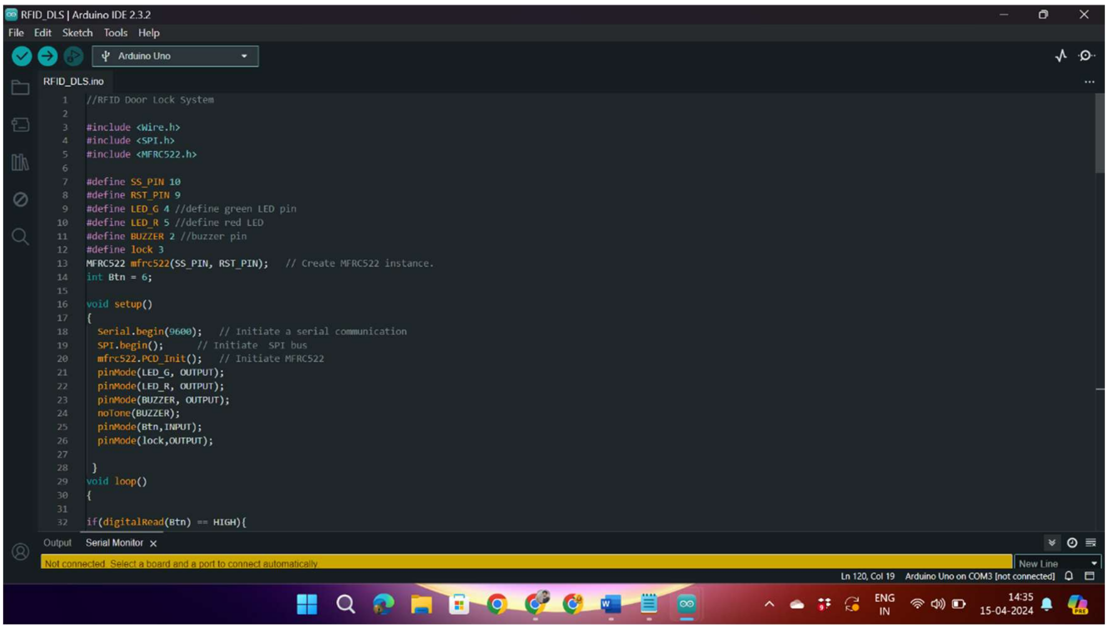
```
//RFID Door Lock System

#include <Wire.h>
#include <SPI.h>
#include <MFRC522.h>

#define SS_PIN 10
#define RST_PIN 9
#define LED_G 4 //define green LED pin
#define LED_R 5 //define red LED
#define BUZZER 2 //buzzer pin
#define lock 3
MFRC522 mfrc522(SS_PIN, RST_PIN);   // Create MFRC522 instance.
int Btn = 6;

void setup()
{
  Serial.begin(9600);   // Initiate a serial communication
  SPI.begin();      // Initiate  SPI bus
  mfrc522.PCD_Init();   // Initiate MFRC522
  pinMode(LED_G, OUTPUT);
  pinMode(LED_R, OUTPUT);
  pinMode(BUZZER, OUTPUT);
  noTone(BUZZER);
  pinMode(Btn,INPUT);
  pinMode(lock,OUTPUT);

 }
void loop()
{

if(digitalRead(Btn) == HIGH){

    Serial.println("Access Granted");
    Serial.println();
    delay(500);
    digitalWrite(LED_G, HIGH);
    tone(BUZZER, 2000);
    delay(100);
    noTone(BUZZER);
    delay(50);
    tone(BUZZER, 2000);
    delay(100);
    noTone(BUZZER);
    digitalWrite(lock,HIGH);
    delay(3000);
```

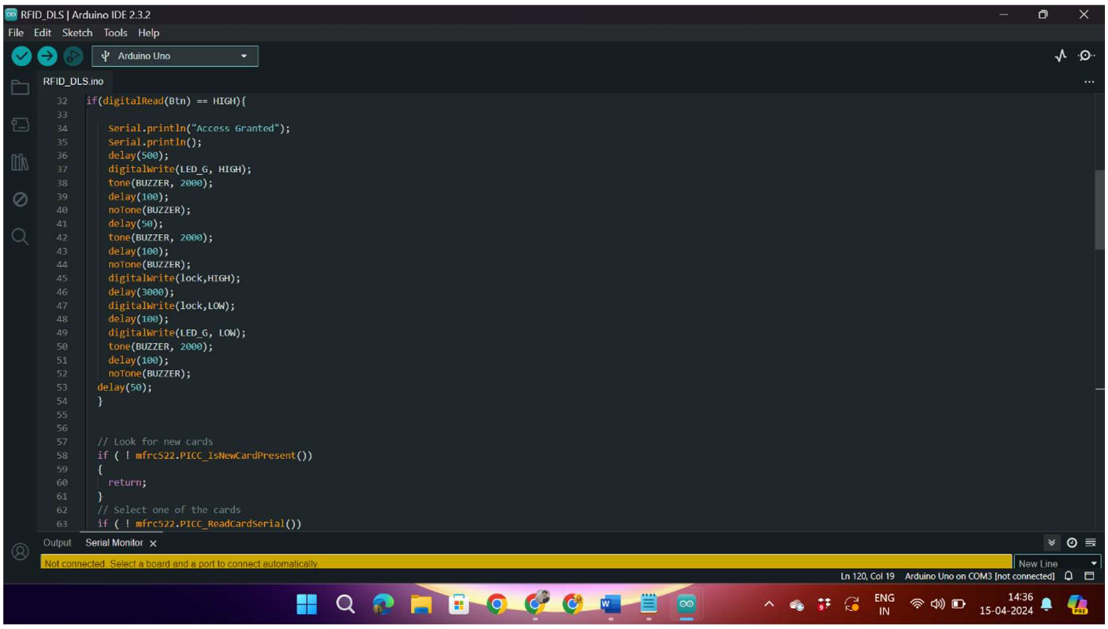
```
   digitalWrite(lock,LOW);
   delay(100);
   digitalWrite(LED_G, LOW);
   tone(BUZZER, 2000);
   delay(100);
   noTone(BUZZER);
  delay(50);
  }


  // Look for new cards
  if ( ! mfrc522.PICC_IsNewCardPresent())
  {
   return;
  }
  // Select one of the cards
  if ( ! mfrc522.PICC_ReadCardSerial())
  {
   return;
  }
  //Show UID on serial monitor
  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) == "13 C7 2A 0E") //change here the UID of card/cards or tag/tags that you want to
give access
  {
   Serial.println("Access Granted");
   Serial.println();
   delay(500);
   digitalWrite(LED_G, HIGH);
   tone(BUZZER, 2000);
   delay(100);
   noTone(BUZZER);
   delay(50);
   tone(BUZZER, 2000);
   delay(100);
   noTone(BUZZER);
```

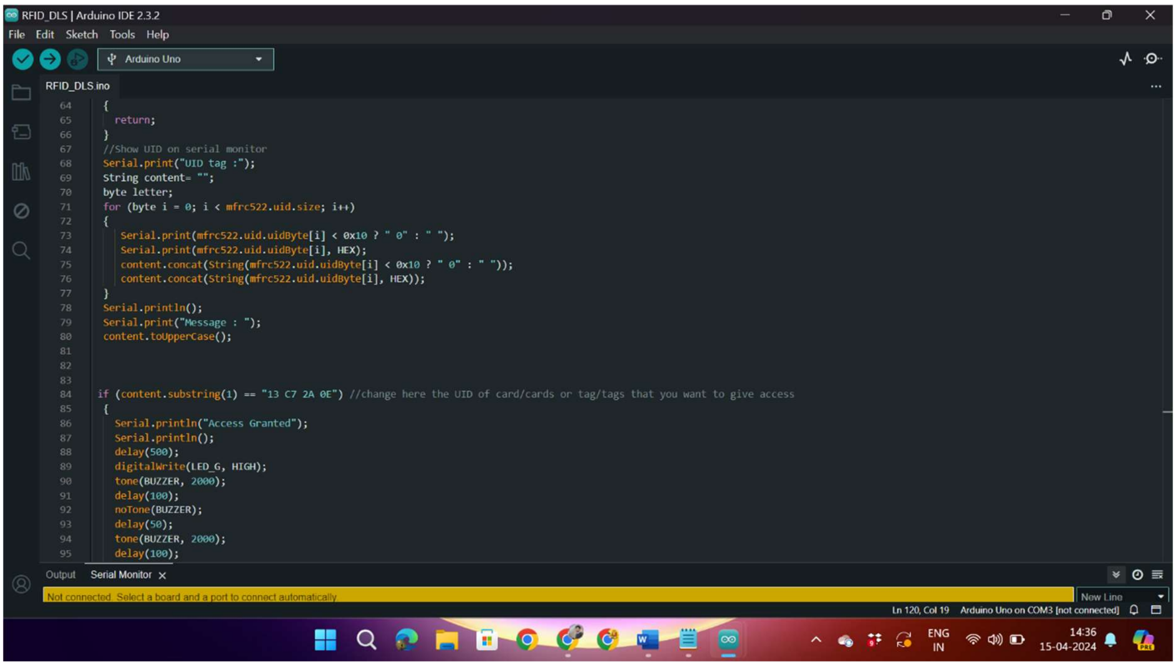
```
    digitalWrite(lock,HIGH);

    delay(3000);
    digitalWrite(lock,LOW);
    delay(100);
    digitalWrite(LED_G, LOW);
    tone(BUZZER, 2000);
    delay(100);
    noTone(BUZZER);
    delay(50);
  }

else
{
    digitalWrite(LED_R, HIGH);
    tone(BUZZER, 1500);
    delay(500);
    digitalWrite(LED_R, LOW);
    noTone(BUZZER);
    delay(100);
    digitalWrite(LED_R, HIGH);
    tone(BUZZER, 1500);
    delay(500);
    digitalWrite(LED_R, LOW);
    noTone(BUZZER);
    delay(100);
    digitalWrite(LED_R, HIGH);
    tone(BUZZER, 1500);
    delay(500);
    digitalWrite(LED_R, LOW);
    noTone(BUZZER);
 }
 if (content.substring(1) == "33 71 C8 A6") //change here the UID of card/cards or tag/tags that you want to
give access
  {
    Serial.println("Access Granted");
    Serial.println();
    delay(500);
    digitalWrite(LED_G, HIGH);
    tone(BUZZER, 2000);
    delay(100);
    noTone(BUZZER);
    delay(50);
    tone(BUZZER, 2000);
    delay(100);
    noTone(BUZZER);
    digitalWrite(lock,HIGH);

    delay(3000);
    digitalWrite(lock,LOW);
    delay(100);
```

```
    digitalWrite(LED_G, LOW);
    tone(BUZZER, 2000);
    delay(100);
    noTone(BUZZER);
    delay(50);
  }

else
{
    digitalWrite(LED_R, HIGH);
    tone(BUZZER, 1500);
    delay(500);
    digitalWrite(LED_R, LOW);
    noTone(BUZZER);
    delay(100);
    digitalWrite(LED_R, HIGH);
    tone(BUZZER, 1500);
    delay(500);
    digitalWrite(LED_R, LOW);
    noTone(BUZZER);
    delay(100);
    digitalWrite(LED_R, HIGH);
    tone(BUZZER, 1500);
    delay(500);
    digitalWrite(LED_R, LOW);
    noTone(BUZZER);
 }
 }
```

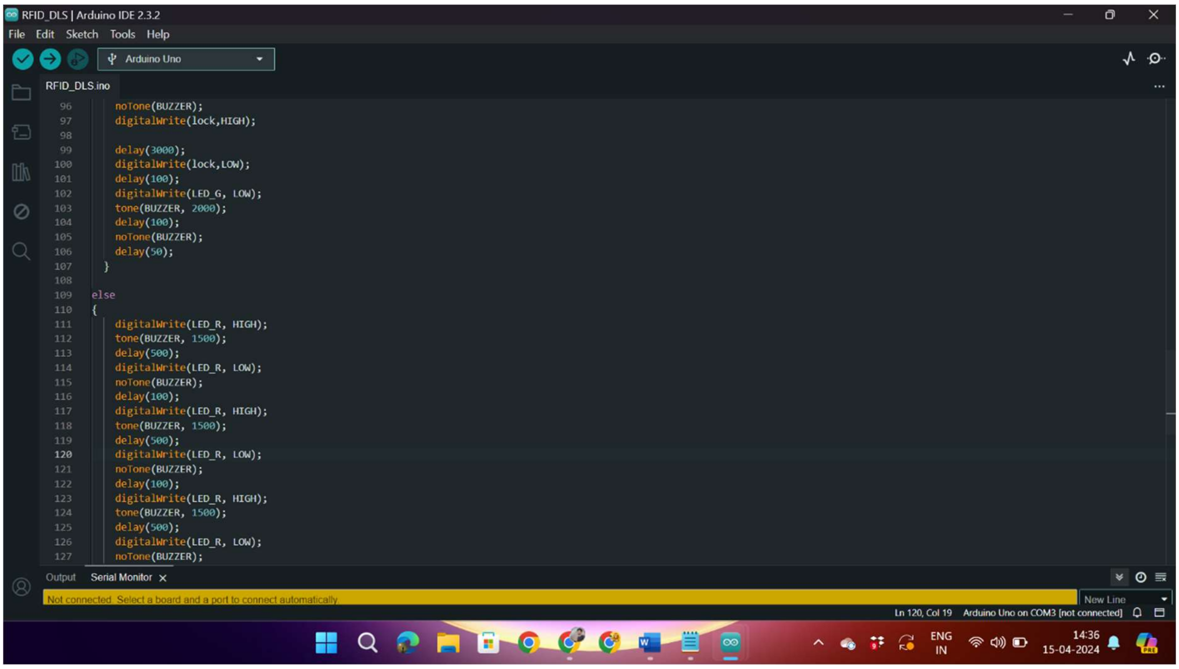
7.1 Compilation Step:



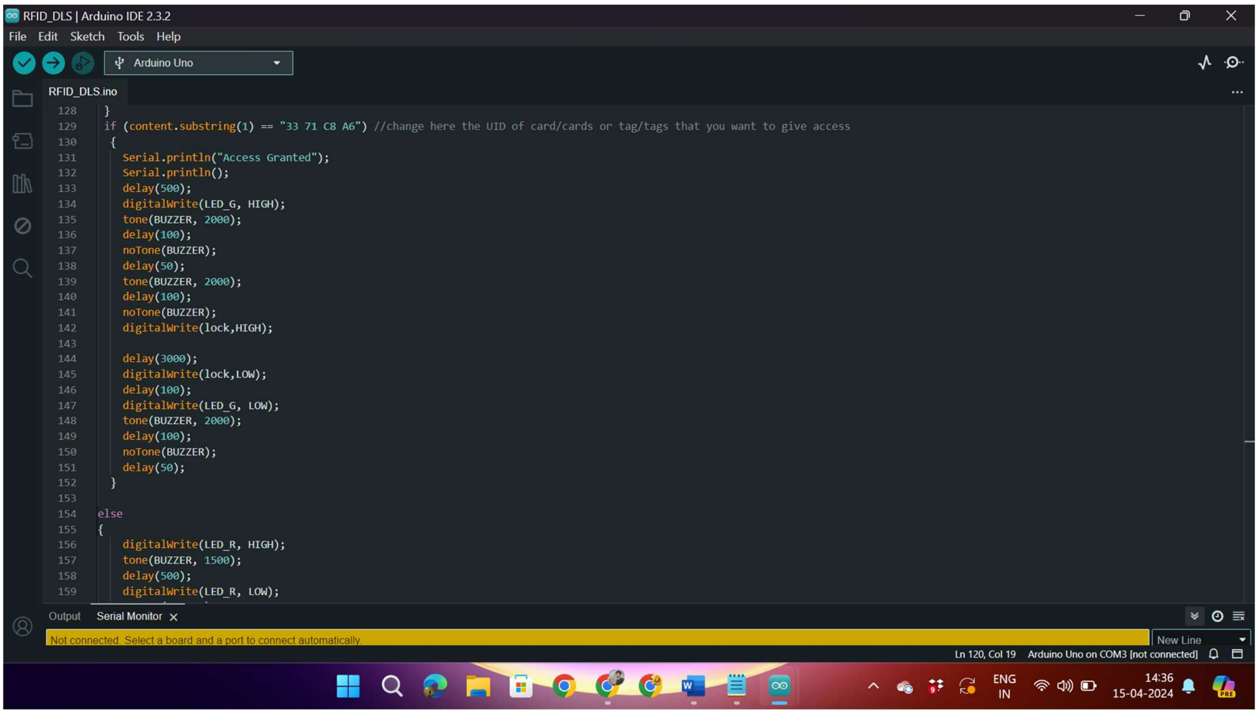


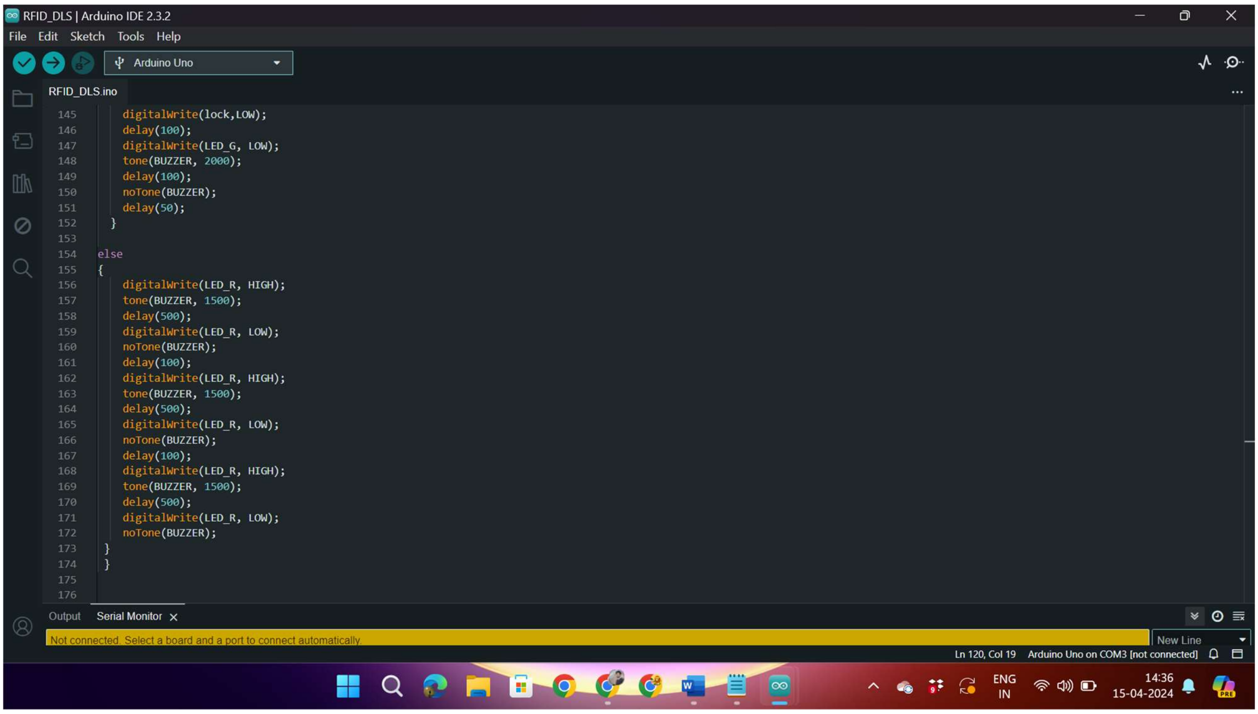


```
{
  return;
}
//Show UID on serial monitor
Serial.print("UID tag :");
String content= "";
byte letter;
for (byte i = 0; i < mfrc522.uid.size; i++)
{
   Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
   Serial.print(mfrc522.uid.uidByte[i], HEX);
   content.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
   content.concat(String(mfrc522.uid.uidByte[i], HEX));
}
Serial.println();
Serial.print("Message : ");
content.toUpperCase();



if (content.substring(1) == "13 C7 2A 0E") //change here the UID of card/cards or tag/tags that you want to give access
{
  Serial.println("Access Granted");
  Serial.println();
  delay(500);
  digitalWrite(LED_G, HIGH);
  tone(BUZZER, 2000);
  delay(100);
  noTone(BUZZER);
  delay(50);
  tone(BUZZER, 2000);
  delay(100);
```



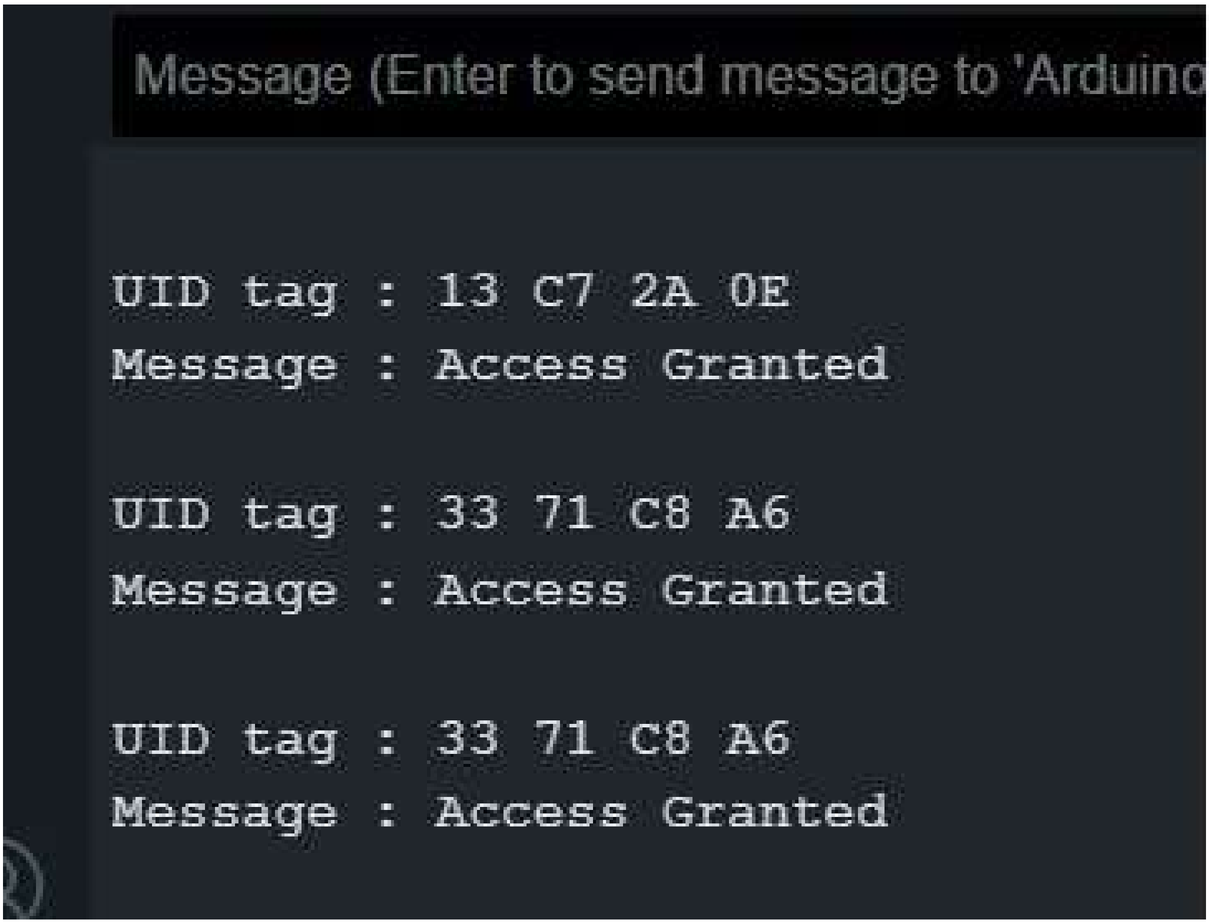
```
    noTone(BUZZER);
    digitalWrite(lock,HIGH);

    delay(3000);
    digitalWrite(lock,LOW);
    delay(100);
    digitalWrite(LED_G, LOW);
    tone(BUZZER, 2000);
    delay(100);
    noTone(BUZZER);
    delay(50);
  }

else
{
    digitalWrite(LED_R, HIGH);
    tone(BUZZER, 1500);
    delay(500);
    digitalWrite(LED_R, LOW);
    noTone(BUZZER);
    delay(100);
    digitalWrite(LED_R, HIGH);
    tone(BUZZER, 1500);
    delay(500);
    digitalWrite(LED_R, LOW);
    noTone(BUZZER);
    delay(100);
    digitalWrite(LED_R, HIGH);
    tone(BUZZER, 1500);
    delay(500);
    digitalWrite(LED_R, LOW);
    noTone(BUZZER);
```


RFID_DLS | Arduino IDE 2.3.2
File Edit Sketch Tools Help
Arduino Uno
RFID_DLS.ino
}
if (content.substring(1) == "33 71 C8 A6") //change here the UID of card/cards or tag/tags that you want to give access
{
Serial.println("Access Granted");
Serial.println();
delay(500);
digitalWrite(LED_G, HIGH);
tone(BUZZER, 2000);
delay(100);
noTone(BUZZER);
delay(50);
tone(BUZZER, 2000);
delay(100);
noTone(BUZZER);
digitalWrite(lock,HIGH);
delay(3000);
digitalWrite(lock,LOW);
delay(100);
digitalWrite(LED_G, LOW);
tone(BUZZER, 2000);
delay(100);
noTone(BUZZER);
delay(50);
}
else
{
digitalWrite(LED_R, HIGH);
tone(BUZZER, 1500);
delay(500);
digitalWrite(LED_R, LOW);
Output Serial Monitor
Not connected. Select a board and a port to connect automatically.
New Line
Ln 120, Col 19 Arduino Uno on COM3 [not connected]
ENG IN
14:36
15-04-2024

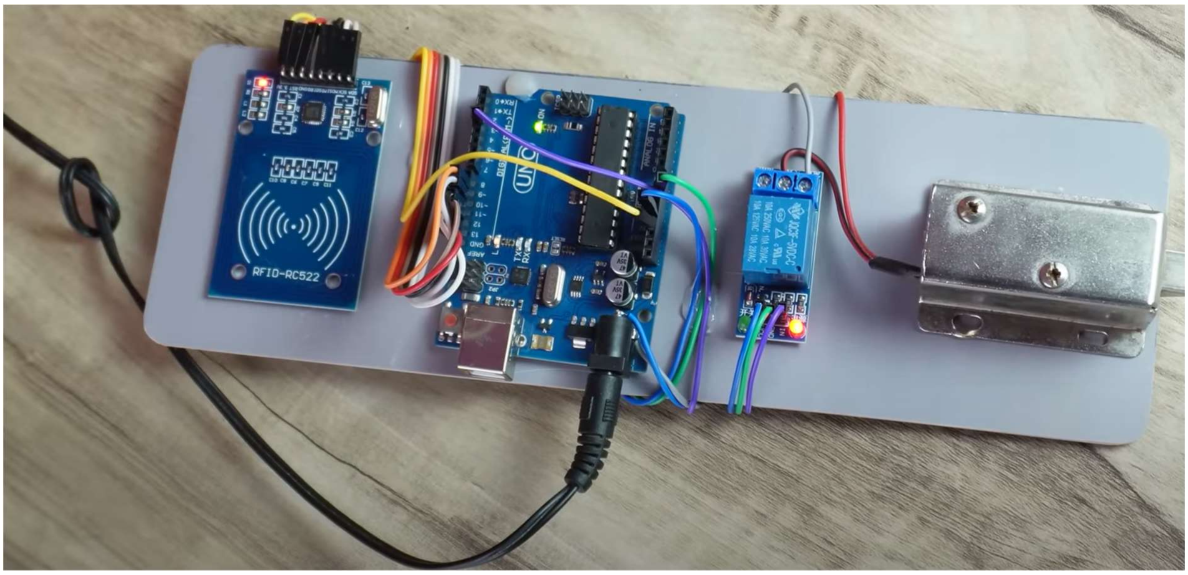

RFID_DLS | Arduino IDE 2.3.2
File Edit Sketch Tools Help
Arduino Uno
RFID_DLS.ino
digitalWrite(lock,LOW);
delay(100);
digitalWrite(LED_G, LOW);
tone(BUZZER, 2000);
delay(100);
noTone(BUZZER);
delay(50);
}
else
{
digitalWrite(LED_R, HIGH);
tone(BUZZER, 1500);
delay(500);
digitalWrite(LED_R, LOW);
noTone(BUZZER);
delay(100);
digitalWrite(LED_R, HIGH);
tone(BUZZER, 1500);
delay(500);
digitalWrite(LED_R, LOW);
noTone(BUZZER);
delay(100);
digitalWrite(LED_R, HIGH);
tone(BUZZER, 1500);
delay(500);
digitalWrite(LED_R, LOW);
noTone(BUZZER);
}
}
Output Serial Monitor
Not connected. Select a board and a port to connect automatically.
New Line
Ln 120, Col 19 Arduino Uno on COM3 [not connected]
ENG IN
14:36
15-04-2024

8.RESULT

The implementation of a door locking system with IoT integration delivers heightened security, convenience, and control. Users can remotely manage access through mobile apps or web interfaces, granting temporary permissions and receiving real-time notifications for enhanced peace of mind. Integration with smart home ecosystems enables seamless automation, while scalability ensures adaptability to varying needs and environments. Efficient power management prolongs battery life, and compliance with industry standards ensures reliability and compatibility. Overall, this system provides an intelligent and user-friendly solution for modern security challenges.



8.1 Cricuit diagram:



9.CONCLUSION

In conclusion, the Fingerprint Door Lock System represents a significant stride towards ensuring the safety and well-being of elderly individuals in their homes. By harnessing the power of biometric technology, our project introduces a secure and user-friendly solution tailored to the specific needs of the elderly. The emphasis on simplicity and intuitiveness in design aims to empower elderly users, providing them with an accessible means of controlling access to their living spaces. As we integrate fingerprint recognition into the fabric of home security, we envision a future where the FDLSE not only enhances the safety of the elderly population but also contributes to a more inclusive and user-centric approach to technology in our homes.

10. FUTURE SCOPE

In the future, door locking systems are poised for further innovation and advancement. Integration with emerging technologies like artificial intelligence (AI) and machine learning could enhance security by enabling predictive analysis of access patterns and anomaly detection. Enhanced biometric authentication methods, such as vein pattern recognition or facial recognition, may offer even higher levels of accuracy and convenience. Additionally, the integration of blockchain technology could provide tamper-proof access logs and enhance data security. The proliferation of smart home devices and the Internet of Things (IoT) could lead to deeper integration and interoperability, enabling seamless communication between door locks and other smart devices for enhanced automation and security. Moreover, advancements in materials science and manufacturing processes may lead to the development of more robust and tamper-resistant physical locking mechanisms. Overall, the future scope for door locking systems is promising, with opportunities for further innovation to meet evolving security needs and technological advancements.

11. REFERENCES

1.https://youtu.be/1LUj7gRxcqU?feature=shared