

RFID BASED SMART DOOR LOCK USING ARDUINO

INTERDISCIPLINARY PROJECT

Submitted in partial fulfilment of the requirements for the award of
Bachelor of Technology in Information Technology

by

NARAN PREM KUMAR REDDY (41120121)



**DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

CATEGORY-1 UNIVERSITY BY UGC

Accredited "A++" by NAAC

12B Status by UGC |Approved by AICTE

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

MAY 2024



SATHYABAMA

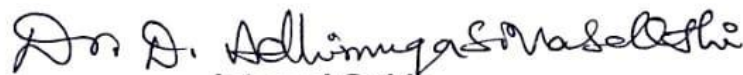
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **NARAN PREM KUMAR REDDY (41120121)** who carried out the project entitled "**RFID BASED SMART DOOR LOCK USING ARDUINO**" under my supervision from January 2024 to May 2024.


Internal Guide

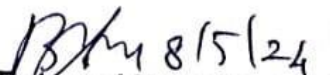
Dr.D.ADHIMUGA SIVASAKTHI


Head of the Department

Dr.R.SUBHASHINI, M.E.,Ph.D.,

Submitted for Viva voce Examination held on 08/05/24


Internal Examiner


External Examiner

DECLARATION

I NARAN PREM KUMAR REDDY hereby declare that the Project Report entitled "RFID BASED SMART DOOR LOCK USING ARDUINO" done by me under the guidance of DR.D.ADHIMUGA SIVASAKTHI, is submitted in partial fulfilment of the requirements for the award of Bachelor of Technology degree in Information Technology.

DATE: 08/05/24

PLACE: chennai

Handwritten signature of N. Prem Kumar in blue ink, with the first letters of the first and last names being capitalized.

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr.T.Sasikala, M.E., Ph.D, Dean**, School of Computing, **Dr.R.Subhashini, M.E., Ph.D.**, Head of the Department of Information Technology for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.D.Adhimuga Sivasakthi** for her valuable guidance, suggestions and constant encouragement which paved the way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

CERTIFICATE OF COMPLETION



HACKWIT TECHNOLOGIES PVT LTD
Redefine by Technologies

149, 1C, 2nd Floor, Mount Poonamallee Rd,
Ramapuram, Chennai - 600089.
admin@hackwittechnologies.com
www.hackwittechnologies.com

10.02.2024

CERTIFICATE FOR INTERNSHIP

TO WHOMSOEVER IT MAY CONCERN

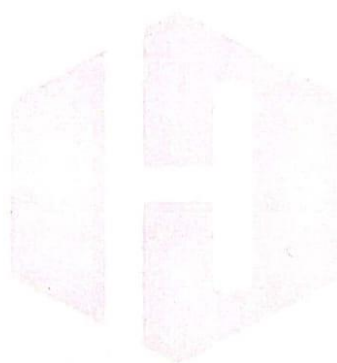
This is to Certify that **NARAN PREM KUMAR REDDY (Reg No: 41120121)** student of Sathyabama Institute of Science and Technology, B. Tech Information Technology, has successfully completed the Internship at Hackwit Technologies from 22nd January to 30th January 2024.

During the internship, **NARAN PREM KUMAR REDDY** has closely worked as a part of the **Internet of Things** by carrying out the project entitled **"RFID BASED SMART DOOR LOCK USING ARDUINO"**.

He demonstrated good developing and learning skill with self-motivated attitude to learn new things. His contribution to implement the Internet of Things was good. We wish him all the best for his future endeavors.

Best Regards,

Ravikumar S
CEO & Managing Director
Hackwit Technologies Pvt Ltd



CERTIFICATE OF COMPLETION



ABSTRACT

An innovative radio frequency identification (RFID) based smart door lock system designed to revolutionize access control using Arduino technology. This project introduces a robust and user-friendly mechanism for enhancing door security with RFID integration. By combining Arduino microcontroller capabilities with RFID technology, this system provides efficient and secure access control. The primary objective is to develop an efficient and user-friendly mechanism for enhancing door security using RFID technology in conjunction with Arduino microcontroller capabilities. The system consists of an Arduino Uno board, an RFID reader module, an electromagnetic relay, an light emitting diode (LED) indicator, and a buzzer. Each authorized user is issued a unique RFID tag/card for identification. When a user presents their RFID card to the reader, the Arduino authenticates the card's unique identifier against a predefined list of authorized users. Upon successful verification, the Arduino triggers the relay module to unlock the door while simultaneously activating a green LED indicator and emitting a short beep from the buzzer to signify authorized access. In case of unauthorized access attempts (i.e., presenting an invalid or unrecognized RFID card), the Arduino activates a red LED indicator and emits a continuous alarm sound from the buzzer, indicating denial of access without unlocking the door.

Key aspects of the project involve seamless hardware integration, Arduino programming for RFID card authentication, relay control for door lock actuation, and LED and buzzer feedback for access status indication. The significance of this project lies in its affordability, simplicity, and enhanced security features. By leveraging widely available components and open-source technology, the proposed system offers a practical solution for residential and small-scale commercial security applications. In conclusion, the RFID-based smart door lock system developed in this project demonstrates a viable approach to implementing advanced security features using Arduino and RFID technology, enhancing access control and providing real-time feedback to users.

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	vii
	LIST OF FIGURES	x
	LIST OF ABBREVIATIONS	xi
1	INTRODUCTION	1
	1.1 Importance of RFIF Based Smart Lock	1
	1.2 Role of IoT in RFID Based Lock System	2
	1.3 Benefits of RFID Technology	3
	1.4 Problem Statement	4
	1.5 Objectives	5
2	METHODOLOGY AND TECHNOLOGY	6
	2.1 Existing System and Proposed system	6
	2.2.1 Existing System	6
	2.2.2 Proposed System	7
	2.2.3 Open Problems in Existing System	9
	2.2 System Implementation and Functionality	11
	2.3 System Architecture for Smart lock System	14
	2.4 Input and Output Design	15
	2.5 Modules	17

2.6	Use Case Diagram For Door Lock System	19
2.7	Software Requirements Specification Document	19
2.7.1	Hardware Configuration	19
2.7.2	Software Configuration	26
2.7.3	Arduino Program Structure	31
2.8	Project Scope and Project Risk	33
2.8.1	Project Scope	33
2.8.2	Project Risks	33
3	RESULTS AND DISCUSSIONS	35
3.1	Result	35
3.2	Discussion	36
4	CONCLUSION AND FUTURE WORK	37
4.1	Conclusion	37
4.2	Future Work	37
	REFERENCES	39
	APPENDICES	40
A.	Source Code	40
B.	Screenshots	45

LIST OF FIGURES

FIGURE NO	FIGURE NAME	PAGE NO
2.1	Architecture Diagram For Smart Door Lock	14
2.2	Use Case Diagram For Door Lock System	19
2.3	RFID Scanner	20
2.4	RFID Tag	21
2.5	Relay Module	22
2.6	Arduino	23
2.7	Solenoid Lock	24
2.8	Lithium Ion Battery	25
2.9	USB Cable	25
2.10	Opening Arduino	27
2.11	Launching Arduino IDE	28
2.12	Arduino Software Opening New File	28
2.13	Selecting File Type	29
2.14	Selecting Board Type	29
2.15	Selecting Serial Port	30
2.16	Uploading Program to Board	30
2.17	Program Structure	32
3.1	Output of the model	35
4.1	Arduino Snapshot	45
4.2	Serial Monitor	45

LIST OF ABBREVIATIONS

ABBREVIATION	EXPANSION
RFID	- Radio Frequency Identification
LED	- Light Emitting Diode
IOT	- Internet Of Things
DC	- Direct current
VCC	- Voltage Common Collector
MCU	- Micro Controller Unit
IDE	- Integrated Development Environment

CHAPTER 1

INTRODUCTION

1.1 IMPORTANCE OF RFID BASED SMART LOCK

RFID based smart door lock plays a crucial role in today's digital age, smart door locks have emerged as a crucial component of modern home security systems, offering a blend of advanced technology and convenience. One of the primary reasons for their growing importance is the enhanced security they provide compared to traditional locks. Smart door locks utilize sophisticated authentication methods like RFID or keypad entry, along with encryption technologies, making it significantly challenging for unauthorized individuals to gain access. This heightened security helps reduce the risk of break-ins and theft, providing homeowners with peace of mind. One of the primary benefits is enhanced security. By integrating RFID technology with a smart door lock, the system utilizes unique RFID tags/cards assigned to authorized users for access. This method replaces traditional keys, which can be lost, duplicated, or stolen, with a more secure and tamper-resistant authentication process. The Arduino microcontroller effectively manages the RFID authentication, ensuring that only authorized individuals can unlock the door, thus minimizing the risk of unauthorized access and intrusions.

Another important aspect is convenience and ease of use. RFID-based smart door locks eliminate the need for physical keys, providing a keyless entry system that enhances convenience for users. Authorized individuals can simply present their RFID cards or tags to the reader, and the Arduino-controlled system will authenticate and grant access swiftly. This streamlined access process is particularly beneficial in scenarios where multiple users require access to the same door, such as in residential buildings or offices. A key benefit of smart door locks is the convenience they offer through remote access capabilities. By leveraging smartphone apps or voice commands compatible with popular smart home systems, users can lock or unlock their doors from anywhere. This feature is especially valuable for granting temporary access to family members, friends, or service providers without the need for physical keys, simplifying the management of access privileges.

Another notable advantage of smart door locks is their keyless entry functionality. Users can enter their homes using RFID cards, PIN codes, or biometric scans, eliminating concerns related to lost or stolen keys. This not only enhances convenience but also enhances security by reducing vulnerabilities associated with traditional keys. Many smart door locks also come equipped with activity monitoring features, providing users with real-time insights into who enters or exits their property and when. This visibility enhances security and allows for remote monitoring of household activities, enhancing overall awareness and control. Furthermore, smart door locks seamlessly integrate with other smart home devices and automation systems. They can be part of a comprehensive home security setup, enabling features like automatic door locking based on user-defined schedules or triggering lights and security cameras upon entry. This integration enhances overall security and contributes to a cohesive smart home ecosystem.

Smart door locks also offer flexibility by allowing users to grant temporary access to guests, contractors, or delivery personnel for specific time frames. This capability adds an extra layer of convenience and security, as access can be easily managed and revoked as needed. In emergency situations such as fires or medical emergencies, smart door locks can be integrated with alarm systems to automatically unlock doors for quick exit, improving overall safety for occupants. Additionally, some smart door locks contribute to energy efficiency by automatically locking doors when no one is home or adjusting settings based on occupancy, thereby optimizing energy usage.

1.2 ROLE OF IoT IN RFID BASED SMART DOOR LOCK

The integration of IoT (Internet of Things) technologies plays a pivotal role in enhancing the capabilities and effectiveness of an RFID-based smart door lock system implemented with Arduino. IoT connectivity enables remote access and control, allowing users to securely manage the door lock from anywhere via smartphone apps or web interfaces. This remote functionality not only enhances convenience but also provides real-time monitoring and control over door access. Furthermore, IoT facilitates data monitoring and analytics by enabling the collection

and transmission of access logs to cloud-based platforms. These analytics offer valuable insights into usage patterns and security events, empowering proactive decision-making and enhancing overall security measures. Additionally, IoT enables seamless integration of the smart door lock into broader smart home ecosystems, enabling interoperability with other IoT devices such as security cameras or voice assistants. This integration enhances automation and security, with the door lock triggering actions like turning on lights or activating cameras upon entry. IoT also contributes to energy efficiency and scalability, allowing for optimized power management and centralized management of multiple door locks across different locations.

1.3 BENEFITS OF RFID TECHNOLOGY

RFID technology is convenient and offers a variety of advantages for medicine carts, pedestals, file cabinets, locker locks, and more. If you are considering purchasing electronic locks, here are some reasons to consider RFID

I. Touchless access

With hygiene a global priority, RFID locks offer a touch-free alternative for high-traffic settings where cleanliness is critical, such as hospitals, fitness centers, or the workplace. Users unlock their storage units with a simple swipe or tap of an authorized RFID card or fob, saving valuable time and enhancing the overall user experience.

II. Enhanced security

Traditional locks are vulnerable to lost keys or unauthorized duplication. RFID tags are highly encrypted, making replicating them more challenging and ensuring that only authorized individuals can access designated storage areas.

III. Seamless integration

Many organizations already use RFID-enabled IDs. The same RFID ID can be programmed to operate RFID locker locks, cabinets, pedestals, medicine

carts, secured merchandise displays, or anywhere controlled access is needed. Simplifying secure storage management and seamlessly integrating with existing technology.

IV. Adaptable to varied environments

RFID technology is versatile, catering to different settings and needs for shared or individual use to accommodate individual or multiple users in various environments.

V. Shared Use RFID locks

For simple day-use solutions, Shared Use allows credentialed users to access any available storage space with a valid credential. When the current user is done, the storage space is vacated, and the lock remains open and ready for another user.

VI. Assigned Use RFID locks

Assigned Use allows managers to program individual RFID credential(s) to a lock for long-term assigned storage so one or multiple users can access a dedicated secure storage space. To open the lock, the user presents an authorized RFID credential to unlock the assigned unit. To lock, the user closes the door, activating the auto-relock feature.

1.4 PROBLEM STATEMENT

The project aims to develop an RFID-based smart lock system using Arduino technology. The problem statement revolves around creating a secure and efficient locking mechanism that utilizes RFID technology to grant access only to authorized individuals. Traditional lock systems often rely on physical keys or codes, which can be lost, stolen, or easily replicated. This poses a security risk and can be inconvenient for users. By implementing an RFID-based smart lock, the project seeks to address these issues by utilizing RFID tags/cards as digital keys. Authorized users will have their unique RFID tags/cards registered in the system,

allowing them to unlock the door or access the secured area with a simple tap or swipe. The project involves integrating RFID reader modules, Arduino microcontroller boards, servo motors, and optional LEDs for indication. The key challenge lies in developing robust software to manage RFID authentication, control the servo motor for locking/unlocking, and ensure the system's reliability and security. Overall, the project aims to provide a user-friendly, secure, and technologically advanced solution for access control.

1.5 OBJECTIVES

The objectives of implementing a solenoid lock system integrated with RFID technology are multifaceted, aiming to establish a comprehensive access control solution that enhances security, convenience, and operational efficiency. At its core, the primary goal is to bolster security measures by leveraging RFID technology for user authentication, effectively replacing traditional lock-and-key mechanisms with a more robust and tamper-resistant system. This transition not only enhances the overall security posture but also streamlines access procedures, offering users a more convenient and efficient means of entry into controlled areas. Real-time access control capabilities are pivotal, allowing administrators to dynamically manage access permissions, thereby ensuring that only authorized individuals are granted entry as needed.

Additionally, the system aims to streamline user management processes, providing administrators with intuitive interfaces for enrolling, updating, and managing RFID credentials, thus ensuring accurate and up-to-date user information. Reliability and durability are paramount, with a focus on developing system components that exhibit high levels of reliability and resilience to minimize downtime and maintenance requirements. Moreover, seamless integration with existing infrastructure and scalability to accommodate varying user populations and access requirements are integral objectives, ensuring the system's versatility and adaptability to diverse environments.

CHAPTER 2

METHODOLOGY AND TECHNOLOGY

2.1. EXISTING SYSTEM AND PROPOSED SYSTEM

2.2.1. EXISTING SYSTEM

An RFID-based smart door lock system is a fascinating application of technology that combines radio-frequency identification (RFID) technology with door locking mechanisms to provide enhanced security and convenience. Here's an overview of how such a system works and why it's exciting

I. RFID Technology

RFID technology utilizes electromagnetic fields to automatically identify and track tags attached to objects. In the case of a smart door lock system, RFID tags are typically embedded in keycards or fobs carried by authorized users.

II. Authentication

When an authorized user approaches the door, they can simply wave their RFID keycard or fob near the RFID reader installed on the door. The reader then detects the unique identifier stored on the RFID tag and sends it to the central control unit of the door lock system for authentication.

III. Access Control

Upon successful authentication, the door lock system grants access to the user by unlocking the door mechanism. This eliminates the need for traditional physical keys, making it more convenient for users while also enhancing security since RFID tags can be encrypted and harder to duplicate compared to traditional keys.

IV. Remote Access

Many modern RFID-based smart door lock systems also offer remote access capabilities. Authorized users can remotely grant or revoke access to individuals, such as guests or service providers, via a smartphone app or

web interface. This feature adds an extra layer of flexibility and control over who can enter the premises.

V. Integration with Home Automation Systems

Another exciting aspect of RFID-based smart door locks is their integration with home automation systems. Users can seamlessly integrate the door lock into their existing smart home ecosystem, allowing for automation of tasks such as locking/unlocking the door based on predefined schedules or triggering other connected devices upon entry.

VI. Enhanced Security Features

Advanced RFID-based smart door lock systems may include additional security features such as tamper detection, intrusion alerts, and activity logs. These features provide users with greater peace of mind and help deter unauthorized access attempts.

VII. Energy Efficiency

Some smart door lock systems are designed to be energy-efficient, utilizing low-power RFID technology and implementing features like automatic locking after a specified period of inactivity to conserve energy.

2.2.2. PROPOSED SYSTEM

The proposed system encompasses a solenoid lock system integrated with RFID technology, designed to deliver secure and efficient access control. At its core, the system consists of several key components: the solenoid lock mechanism, an RFID reader, RFID tags or cards, a microcontroller unit (MCU), and a user interface. The solenoid lock serves as the primary means of physical access control, activating or deactivating to grant or deny entry based on RFID authentication. The RFID reader acts as the intermediary between the RFID tags/cards and the MCU, capturing and processing RFID signals for authentication purposes. RFID tags or cards are assigned to authorized users and serve as their unique credentials for access.

The MCU serves as the central processing unit, orchestrating the interaction between the solenoid lock, RFID reader, and user interface. It manages the authentication process, verifies RFID credentials, and controls the operation of the solenoid lock based on the authentication result. Additionally, the MCU stores and manages the database of authorized RFID credentials. The user interface provides a user-friendly means for administrators to manage the system and for users to interact with it. Administrators can enroll or revoke RFID credentials, configure access permissions, and monitor system status through the user interface. Users can present their RFID tags/cards to gain entry, receive feedback on access status, and view relevant information displayed on the interface.

In terms of functionality, the proposed system offers the following features:

I. Secure Authentication

Utilizes RFID technology for secure and reliable user authentication, minimizing the risk of unauthorized access.

II. Real-time Access Control

Enables dynamic management of access permissions, allowing administrators to grant or revoke access privileges instantly.

III. Audit Trail

Records access events and user activity, providing administrators with a comprehensive audit trail for monitoring and compliance purposes.

IV. User Management

Facilitates the enrolment, deletion, and management of RFID credentials, ensuring accurate and up-to-date user information.

V. Emergency Override

Incorporates an emergency override mechanism to enable manual access in case of system failure or emergency situations.

VI. Remote Management

Supports remote management capabilities, allowing administrators to monitor and control the system from a centralized location via cloud connectivity or network access.

VII. Scalability

Designed to scale seamlessly to accommodate varying user populations and access requirements, making it suitable for a wide range of applications and environments.

Overall, the proposed system offers a comprehensive and robust solution for access control, leveraging the capabilities of solenoid lock and RFID technology to deliver enhanced security, convenience, and flexibility.

2.2.3. OPEN PROBLEMS IN EXISTING SYSTEM

In existing solenoid lock systems integrated with RFID technology, several open problems persist, presenting opportunities for further research and improvement:

I. Security Vulnerabilities

Despite advancements in RFID technology, security vulnerabilities such as relay attacks, eavesdropping, and cloning of RFID credentials remain significant concerns. Developing robust encryption techniques and authentication protocols to mitigate these vulnerabilities is a pressing challenge.

II. User Authentication

Existing systems primarily rely on RFID tags/cards for user authentication, which may be susceptible to theft or misuse. Exploring alternative or supplementary authentication methods, such as biometrics or multi-factor authentication, could enhance security and reduce reliance on RFID credentials alone.

III. Reliability and Durability

Solenoid locks and RFID components are prone to wear and tear over time, affecting their reliability and durability. Improving the design and materials used in these components to enhance longevity and resilience in harsh environments is an ongoing challenge.

IV. Interference and Range Limitations

RFID systems can experience interference from other electronic devices or environmental factors, leading to communication errors or reduced read

range. Addressing these issues through improved antenna design, frequency management, or signal processing techniques is essential for reliable operation.

V. Integration Challenges

Integrating solenoid lock systems with existing infrastructure or third-party systems, such as building management systems or access control platforms, often presents interoperability challenges. Developing standardized interfaces and protocols to facilitate seamless integration is a complex but necessary endeavor.

VI. User Experience

The user experience of existing solenoid lock systems can be suboptimal, with issues such as slow response times, complex user interfaces, or difficulty in enrollment and management of RFID credentials. Enhancing usability through intuitive interfaces, responsive feedback mechanisms, and simplified administration tools is critical for user acceptance and adoption.

VII. Power Management

Power consumption is a significant consideration, particularly in battery-operated solenoid lock systems. Optimizing power management strategies to maximize battery life while ensuring continuous operation is an ongoing challenge, especially in IoT or wireless applications.

VIII. Scalability and Flexibility

As the scale and complexity of access control systems increase, scalability and flexibility become paramount. Designing modular and scalable architectures that can accommodate growing user populations and evolving access requirements is a continuous challenge.

Addressing these open problems requires interdisciplinary collaboration and innovative approaches across fields such as cybersecurity, electronics, materials science, and human-computer interaction. By tackling these challenges, future solenoid lock systems integrated with RFID technology can become more secure, reliable, user-friendly, and adaptable to diverse applications and environments.

2.2 SYSTEM IMPLEMENTATION AND FUNCTIONALITY

I. Hardware Setup

The implementation of an RFID-based smart lock system begins with assembling the necessary hardware components. This includes an RFID reader, which scans RFID tags/cards for authentication. Additionally, a solenoid lock mechanism is required to physically control access to the door or entry point. A microcontroller, such as an Arduino, serves as the brain of the system, managing communication between the RFID reader, solenoid lock, and other components. The hardware setup ensures that the system can accurately read RFID credentials and actuate the lock mechanism accordingly.

II. Software Development

The software development phase focuses on creating the logic and functionality required for the smart lock system to operate securely and efficiently. This involves writing code to interface with the RFID reader, interpret RFID tag data, and verify user credentials against a database of authorized users. Additionally, the software implements mechanisms for controlling the solenoid lock, including protocols for locking and unlocking based on successful authentication. Error handling routines are also incorporated to address scenarios such as invalid credentials or communication errors.

III. Access Control Logic

A critical aspect of the smart lock system is its access control logic, which determines who is allowed to unlock the door. Upon scanning an RFID tag, the system compares the tag's unique identifier against a list of authorized users stored in memory. If a match is found, indicating that the scanned tag belongs to an authorized user, the system grants access by activating the solenoid lock mechanism to unlock the door. If no match is found, access is denied, and the door remains locked. This access control logic ensures that only authorized individuals can gain entry.

IV. User Feedback Mechanisms

To provide users with feedback on the status of their access attempts, the smart lock system incorporates various feedback mechanisms. For example, LED indicators may illuminate to signal successful authentication and door unlock, while an audible buzzer may sound to indicate access denial or other errors. Additionally, a graphical user interface (GUI) or display panel can be used to provide visual feedback and instructions to users. These feedback mechanisms enhance the user experience and help users understand the status of their access attempts.

V. Integration and Testing:

Once the hardware and software components have been developed, they are integrated into a cohesive system and subjected to rigorous testing. Integration involves connecting the RFID reader, solenoid lock, microcontroller, and other components according to the system design. Testing encompasses various scenarios, including successful and unsuccessful access attempts, communication errors, and hardware malfunctions. Through thorough testing, any bugs or issues are identified and addressed, ensuring that the smart lock system functions reliably in real-world environments.

VI. Security Measures:

Security is paramount in a smart lock system, as it directly impacts the safety and privacy of the protected space. To enhance security, measures such as encryption of RFID tag data, secure communication protocols, and tamper detection mechanisms may be implemented. Additionally, access logs and audit trails can be generated to track and monitor access attempts, providing valuable information for security analysis and incident response. By prioritizing security throughout the implementation process, the smart lock system can effectively safeguard against unauthorized access and protect the integrity of the secured space.

VII. Buzzer Activation and Alarm Notification

Buzzer activation and alarm notification play a crucial role in alerting nearby individuals and emergency responders to the presence of fire incidents in forested areas. The methodology for implementing this functionality involves configuring the piezo buzzer to generate audible alerts when the flame sensor module detects a fire. Firstly, the Arduino Uno's digital output pins are utilized to control the piezo buzzer's activation. The code is programmed to trigger the buzzer when the flame sensor detects a flame above a predefined threshold level. Upon detection of a fire, the Arduino sends a signal to the buzzer, causing it to emit a loud, attention-grabbing sound. Furthermore, to ensure effective alarm notification, the buzzer activation process is accompanied by visual indicators or notifications, if applicable. This may include flashing LED lights or text displays to provide additional warning signals and enhance situational awareness. Additionally, the duration and frequency of the buzzer's sound can be adjusted programmatically to convey different levels of urgency or severity of the fire incident.

Moreover, as part of the methodology, the system's response to alarm activation is thoroughly tested and validated under various fire simulation scenarios. This includes assessing the responsiveness of the buzzer to different flame intensities and distances from the sensor, as well as evaluating its performance in noisy or adverse environmental conditions. Adjustments to the buzzer activation parameters are made iteratively based on testing results to optimize its effectiveness in alerting nearby individuals and facilitating prompt response actions. Through meticulous configuration and testing, the methodology ensures that the buzzer activation and alarm notification mechanisms are robust, reliable, and capable of effectively alerting stakeholders to potential fire threats in forested areas.

VIII. Power Supply Management and Backup

Power supply management is crucial for ensuring the continuous operation of the forest fire detection system. The primary power source for the system is typically a 9V battery, providing portability and autonomy for standalone deployment.

However, efficient power management strategies are essential to maximize battery life and minimize the risk of system downtime. This involves implementing techniques such as low-power modes for the Arduino Uno when not actively sensing or processing data, as well as optimizing sensor sampling rates to conserve energy. Additionally, voltage regulation circuits may be employed to stabilize power output and protect sensitive components from voltage fluctuations. To mitigate the risk of power failure, backup power sources such as secondary batteries or solar panels can be integrated into the system, providing redundancy and ensuring continuous operation during prolonged periods of use or in the event of battery depletion.

Implementing a robust power supply management and backup system is essential to ensure the reliability and effectiveness of the forest fire detection system in remote and challenging environments. By carefully managing power consumption and incorporating backup power sources, the system can maintain continuous operation and provide timely alerts and responses to unauthenticated users, thereby enhancing overall resilience and effectiveness in security system..

2.3. SYSTEM ARCHITECTURE FOR SMART DOOR LOCK

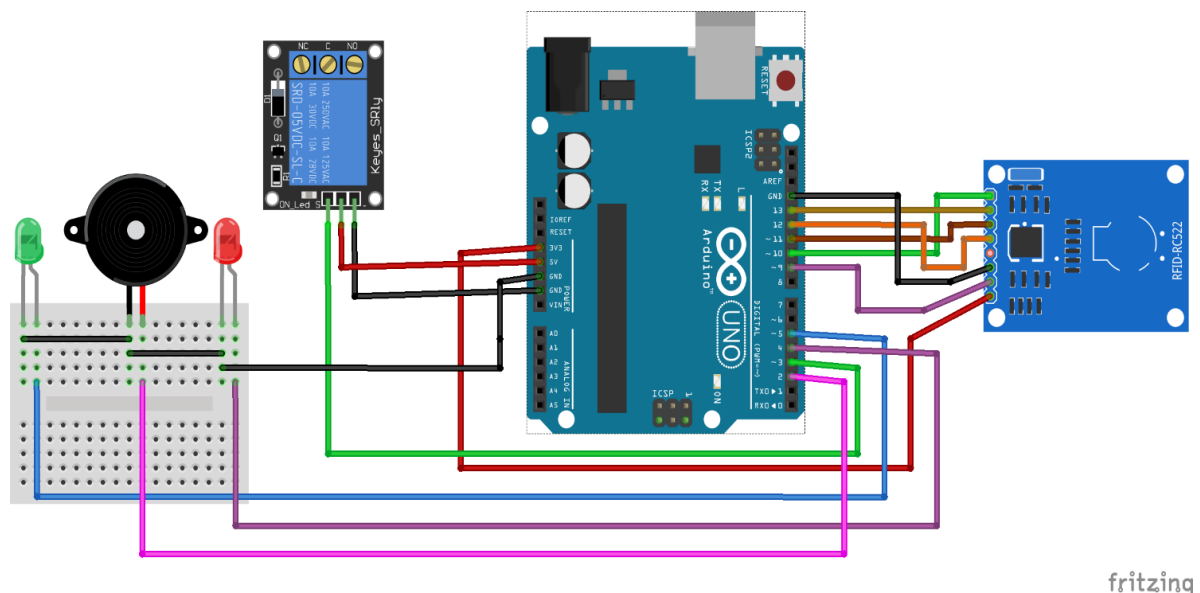


Fig 2.1 Architecture Diagram of smart door lock

RFID (Radio Frequency Identification) is a cheap and accessible technology. It can be used in many applications such as access control, security, asset tracking, person tracking, etc. You may have seen RFID door lock systems in hotels, offices, and many other places. Basically, they provide you a card and you have to just place the card near the RFID reader, within a second and the door will open. This RFID Solenoid door lock can be easily made at home just following this tutorial. Previously, we have also used the same technology on our RFID and IoT based projects. Here in this project, we are using Arduino and Relay to trigger the solenoid door lock. While RFID MF-RC522 is used to authenticate users so that your RFID tag acts as the key. If you place the wrong RFID card close to the RFID reader, a buzzer will beep to alert you about the wrong card.

2.4. INPUT AND OUTPUT DESIGN

In the proposed system architecture depicted in Figure 2.1, the input and output design for the forest fire detection system is outlined as follows:

I. INPUT DESIGN

The RFID based smart lock system's input design relies on a multi-pronged approach for immediate awareness:

- **RFID Reader Input:** The RFID reader serves as the primary input device, reading RFID tags/cards presented by users. Upon detecting an RFID tag, the reader sends the unique tag ID to the Arduino for authentication.
- **Motion Sensor Input :** Motion sensors detect movement near the door and trigger the activation of the RFID reader. This input helps conserve power by only activating the RFID reader when motion is detected.
- **Power Supply:** A 5V battery pack or DC power supply provides system power.
- **Microcontroller:** Arduino Uno (or compatible) reads sensor data and controls outputs.
- **Alarms:** A piezo buzzer generates sound to alert nearby personnel.

II. OUTPUT DESIGN

The RFID based smart lock system's input design relies on a multi-pronged approach for immediate awareness

- **Relay Module Output**

The relay module controls the solenoid lock mechanism based on input signals from the Arduino. When the Arduino authorizes access, it activates the relay module to unlock the solenoid lock, allowing the door to open.

- **LED Indicators**

LED indicators provide visual feedback to users about the status of the smart lock system. A green LED may indicate that the door is unlocked, while a red LED may indicate that access is denied.

- **Buzzer**

A buzzer can provide audible feedback to users about access attempts. A beep sound may indicate successful authentication, while a different sound may indicate access denial.

- **Integration with IoT Platform**

The system can be integrated with an IoT platform to provide remote access control and monitoring. Users can use a mobile app or web interface to lock/unlock the door and view access logs remotely.

III. OVERALL DESIGN CONSIDERATIONS

- The input and output design should prioritize user experience, providing clear and intuitive feedback about access attempts.
- Integration of optional sensors like motion sensors and door position sensors enhances system functionality and security.
- Flexibility should be built into the design to accommodate future expansion or customization, such as adding additional sensors or output devices.
- Attention should be paid to power consumption, especially for battery-powered systems, to ensure efficient operation and prolonged battery life.

- The system should be designed with reliability and security in mind, incorporating mechanisms to handle errors and prevent unauthorized access.

2.5 MODULES

In the process of bringing the forest fire detection system to life, meticulous attention is paid to the implementation of the circuit connections. This phase involves translating the conceptual design into a tangible reality by physically assembling the components and establishing the necessary electrical connections. Each component, from the Arduino Uno microcontroller to the flame sensor module, relay module, submersible motor, and piezo buzzer, is carefully integrated into the system architecture according to the specified wiring diagram. Through precise wiring connections and adherence to best practices in circuit design, the forest fire detection system begins to take shape, laying the foundation for subsequent testing and validation procedures. Building an RFID-based smart lock using Arduino involves several steps and requires the use of specific components/modules. Here's a step-by-step guide along with the necessary connections:

I. GATHER COMPONENTS

- Arduino Uno or similar microcontroller board
- RFID reader module (such as MFRC522)
- Servo motor or DC motor with a motor driver
- LEDs for indication (optional)
- Breadboard and jumper wires
- RFID tags/cards

II. CIRCUIT CONNECTION

- **Connect RFID Reader Module**
 - a) Connect the RFID reader module to the Arduino:
 - b) RFID Module SDA pin to Arduino Uno pin 10
 - c) RFID Module SCK pin to Arduino Uno pin 13

- d) RFID Module MOSI pin to Arduino Uno pin 11
- e) RFID Module MISO pin to Arduino Uno pin 12
- f) RFID Module GND pin to Arduino GND pin
- g) RFID Module RST pin to Arduino Uno pin 9
- h) RFID Module 3.3V pin to Arduino 3.3V pin

- **Connect solenoid lock (for locking/unlocking)**

- a) Connect the solenoid lock to the relay:
- b) Solenoid (+) pin to relay out pin
- c) Solenoid (-) pin to relay GND pin

- **Connect LEDs**

- a) Connect LEDs to the Arduino for indication purposes:
- b) Connect the cathode (short leg) of each LED to a digital pin on the Arduino through a current-limiting resistor (e.g., 220Ω).
- c) Connect the anode (long leg) of each LED to the Arduino's 5V pin.

- **Connect the Piezo Buzzer**

- a) The positive (red) wire to any digital pin on the Arduino, for example, pin
- b) The negative (black) wire to the GND pin on the Arduino.

- **Connect the DC Motor**

- a) One terminal of the DC motor to the 5V pin on the Arduino.
- b) The other terminal of the DC motor to the collector pin of the relay module.
- c) Lastly, connect the USB cable from the Arduino to the laptop for uploading the C code.

- **Connect the Relay Module**

- a) VCC to the 5V pin on the Arduino.
- b) GND to the GND pin on the Arduino.
- c) IN to any digital pin on the Arduino, for example, pin 3.

Make sure to adjust the code and connections according to your specific components and requirements. Additionally, consider implementing security measures such as encryption to protect RFID data.

2.6 USE CASE DIAGRAM FOR DOOR LOCK SYSTEM

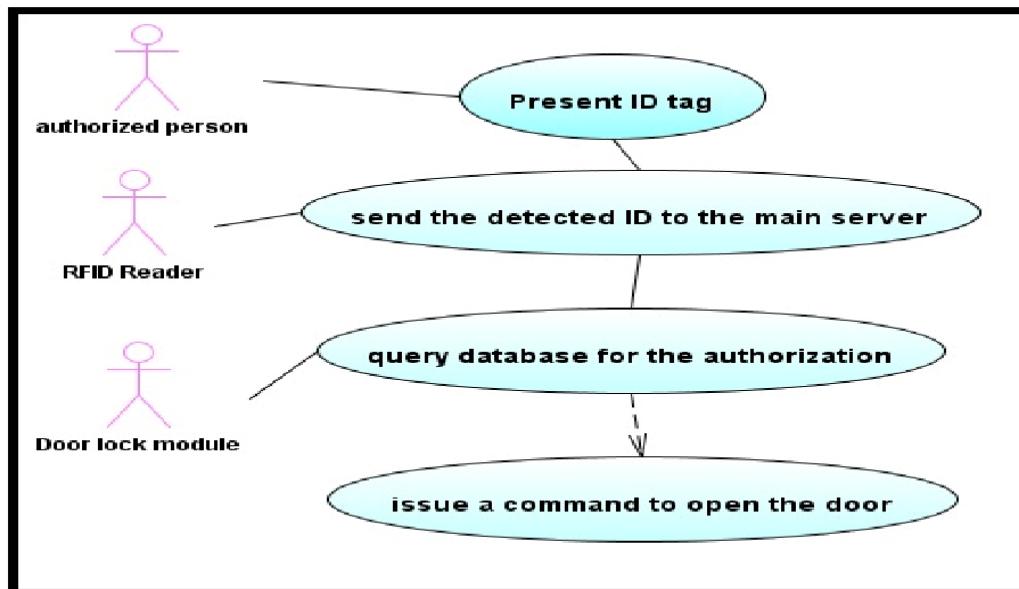


Fig 2.2 Use case diagram For Door Lock System

2.7 SOFTWARE REQUIREMENTS SPECIFICATION DOCUMENT

2.7.1. HARDWARE CONFIGURATION

The most IoT-Based Domestic & Commercial Appliance Control Along With IR Remote And Motion Detection Lighting Dept of ECE 38 commonly used Lithium Ion battery is the 18650 Cells, so will discuss about the same in this article. A typical 18650 cell is shown in the image below Like all batteries the Li-ion battery also has

a voltage and capacity rating. The nominal voltage rating for all lithium cells will be 3.6V, so you need higher voltage specification you have to combine two or more cells in series to attain it. By default all the lithium ion cells will have a nominal voltage of only ~3.6V. This voltage can be allowed to go down upto 3.2V when fully discharged and go as high as 4.2V when fully charged.

I. RFID Technology

The RFID Scanner depicted in Figure 2.3, consists of three components: a scanning antenna, a transceiver and a transponder. When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator. There are two types of RFID readers fixed readers and mobile readers. The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.



Fig 2.3 RFID Scanner

The transponder is in the RFID tag itself. The read range for RFID tags varies based on factors including the type of tag, type of reader, RFID frequency and interference in the surrounding environment or from other RFID tags and readers. Tags that have a stronger power source also have a longer read range.

II. RFID Tags

RFID tags, depicted in Figure 2.4, are a type of tracking system that uses smart barcodes in order to identify items. RFID is short for “radio frequency identification,” and as such, RFID tags utilize radio frequency technology. RFID tags are passive or active devices that store and transmit data wirelessly using radio waves. They offer advantages over traditional barcode systems, such as faster scanning and the ability to read multiple tags simultaneously. RFID technology finds extensive application in inventory management, supply chain logistics, and asset tracking across various industries. The tags consist of an integrated circuit and an antenna, enabling them to communicate with RFID readers within a certain range. Beyond commercial use, RFID tags are also employed in healthcare for patient tracking, in agriculture for livestock management, and in access control systems for security purposes.

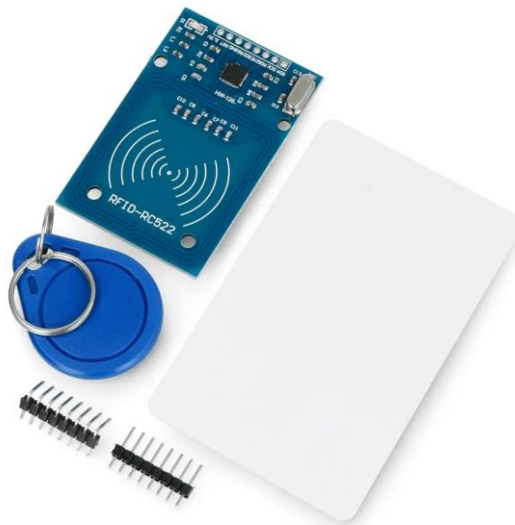


Fig 2.4 RFID tag

These radio waves transmit data from the tag to a reader, which then transmits the information to an RFID computer program. RFID tags are frequently used for merchandise, but they can also be used to track vehicles, pets, and even patients with Alzheimer’s disease.

III. Relay Module

The relay module, depicted in Figure 2.5, uses an electric current to open or close the contacts of a switch. This is usually done using the help of a coil that attracts the contacts of a switch and pulls them together when activated, and a spring pushes them apart when the coil is not energized. Relays serve as indispensable components in electrical systems, leveraging electric currents to manipulate switch contacts efficiently. By employing a coil to generate magnetic forces, relays can toggle switch positions, offering a reliable means of control. One key advantage lies in the minimal current required to activate the relay, contrasting with its ability to handle significantly higher currents. Moreover, the isolation between the coil and contacts ensures safety and versatility in various applications. This isolation enables relays to interface between low-voltage control systems, such as microcontrollers, and high-voltage mains currents, facilitating seamless integration. Thus, the inherent characteristics of relays make them vital for diverse tasks, from industrial automation to consumer electronics.

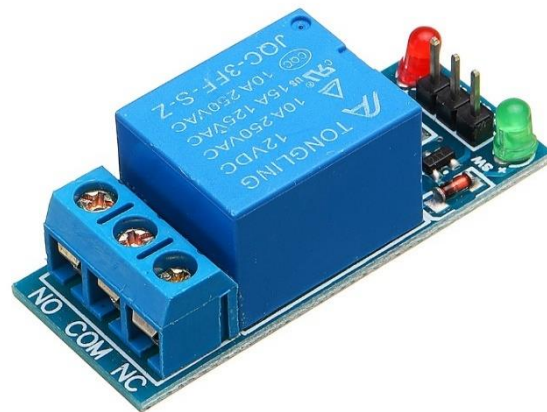


Fig 2.5 Relay Module

There are two advantages of this system – First, the current required to activate the relay is much smaller than the current that relay contacts are capable of switching, and second, the coil and the contacts are galvanically isolated, meaning there is no electrical connection between them. This means that the relay can be used to switch mains current through an isolated low voltage digital system like a microcontroller.

IV. Arduino Uno

The ArduinoUno is open-source Microchip ATmega328P microcontroller (MCU) and developed by Arduino.cc and initially released in 2010.^{[2][3]} The microcontroller board is equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (shields) and other circuits.^[4] The board has 14 digital I/O pins (six capable of PWM output), 6 analog I/O pins, and is programmable with the Arduino IDE (Integrated Development Environment), via a type B USB cable. It can be powered by a USB cable or a barrel connector that accepts voltages between 7 and 20 volts, such as a rectangular 9-volt battery. It has the same microcontroller as the Arduino Nano board, and the same headers as the Leonardo board. The hardware reference design is distributed under a Creative Commons Attribution Share-Alike 2.5 license and is available on the Arduino website. Layout and production files for some versions of the hardware are also available.

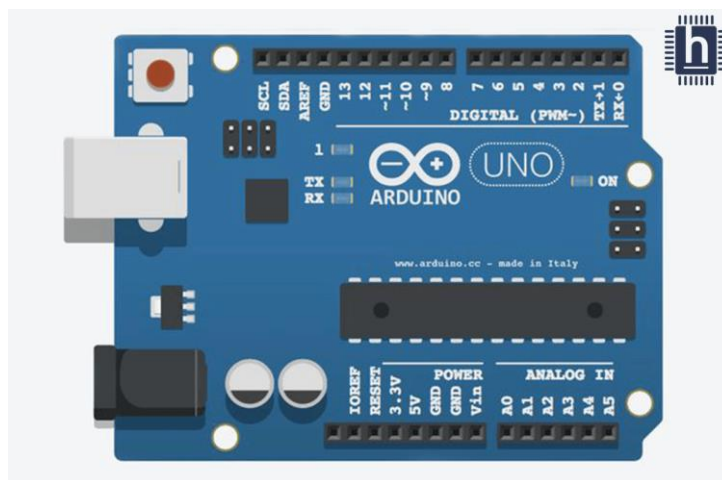


Fig 2.6 Arduino

V. Solenoid Lock

A solenoid lock works on the electronic-mechanical locking mechanism. This type of lock has a slug with a slanted cut and a good mounting bracket. When the power is applied, DC creates a magnetic field that moves the slug inside and keeps the door in the unlocked position. The slug will retain its position until the power is removed. When the power is disconnected the slug moves outside and locks the door



Fig 2.7 Solenoid Lock

VI. 12V Battery

The piezo buzzer, depicted in Figure 2.8, serves as an integral component of the forest fire detection system, providing audible alerts or alarms to notify nearby individuals and emergency responders of fire incidents. Consisting of a piezoelectric element and resonant cavity, the buzzer generates sound waves when subjected to an electrical signal, producing distinctive beeping or buzzing sounds. By interfacing with the Arduino Uno, the buzzer can be activated in response to fire detection signals from the flame sensor module, alerting stakeholders to potential fire threats and prompting timely evacuation or response actions. Its compact size, low power consumption, and high sound output make the piezo buzzer an effective tool for enhancing situational awareness and facilitating rapid response to fire emergencies.



Fig 2.8 Lithium Ion Battery

VII. USB Cable

The USB cable, depicted in figure 2.9, serves as the primary means of communication and power supply for the forest fire detection system. It enables connectivity between the Arduino Uno and a computer or external power source, facilitating tasks such as uploading sketches, debugging code, and monitoring sensor data using the Arduino Integrated Development Environment (IDE). Additionally, the USB cable can be used to power the Arduino Uno during programming and testing phases, offering flexibility and convenience in system development and deployment. Its plug-and-play compatibility and widespread availability make the USB cable an indispensable accessory for Arduino-based projects, ensuring seamless integration and operation of the forest fire detection system.

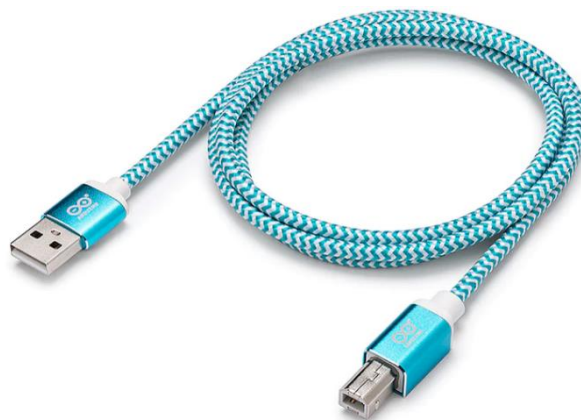


Fig 2.9 USB Cable

2.7.2. SOFTWARE CONFIGURATION

Arduino IDE (Integrated Development Environment) is required to program the NODE MCU board.

I. Programming Arduino

Once Arduino IDE is installed on the computer, connect the board with computer using USB cable. Now open the Arduino IDE and choose the correct board by selecting Tools>Boards>Arduino/Genuine Uno, and choose the correct Port by selecting Tools>Port. NODE MCU is programmed using Arduino programming language based on Wiring. To get it started with NODE MCU board and blink the built-in LED, load the example code by selecting Files>Examples>Basics>Blink. Once the example code (also shown below) is loaded into your IDE, click on the 'upload' button given on the top bar. Once the upload is finished, you should see the Arduino's built-in LED blinking. Below is the example code for blinking:

II. Arduino – Installation

After learning about the main parts of the NODE MCU board, we are ready to learn how to set up the Arduino IDE. Once we learn this, we will be ready to upload our program on the Arduino board. In this section, we will learn in easy steps, how to set up the Arduino IDE on our computer and prepare the board to receive the program via USB cable.

Step 1: About Arduino board

First you must have your Arduino board (you can choose your favorite board) and a USB cable. In case you use NODE MCU, Arduino Duemilanove, Nano, Arduino Mega 2560, or Diecimila, you will need a standard USB cable (A plug to B plug), the kind you would connect to a USB printer as shown in the following image.

Step 2: Download Arduino IDE Software

You can get different versions of Arduino IDE from the Download page on the Arduino Official website. You must select your software, which is compatible with

your operating system (Windows, IOS, or Linux). After your file download is complete, unzip the file as shown in Figure 2.10

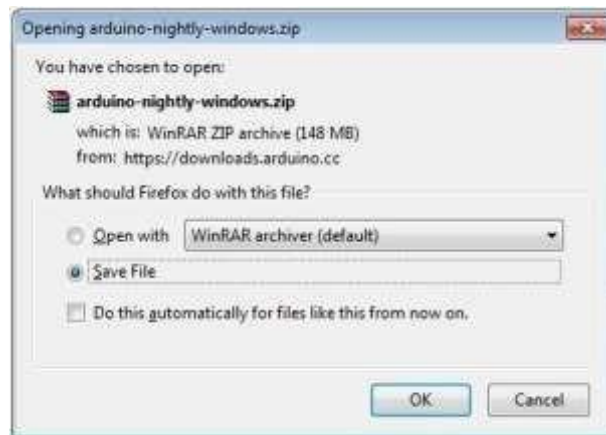


Fig 2.10 Opening Arduino

Step 3: Power up your board

The NodeMCU, Mega, Duemilanove, Arduino, and nano technology automatically draw power from either, the USB connection to the computer or an external power supply. If you are using an Arduino Diecimila, you have to make sure that the board is configured to draw power from the USB connection. The power source is selected with a jumper, a small piece of plastic that fits onto two of the three pins between the USB and power jacks. Check that it is on the two pins closest to the USB port. Connect the Arduino board to your computer using the USB cable. The green power LED (labeled PWR) should glow.

Step 4: Launch Arduino IDE

After your Arduino IDE software is downloaded, you need to unzip the folder. Inside the folder, you can find the application icon with an infinity label (application.exe). DoubleClick the icon to start the IDE. Figure 2.11, shows launching of Arduino IDE

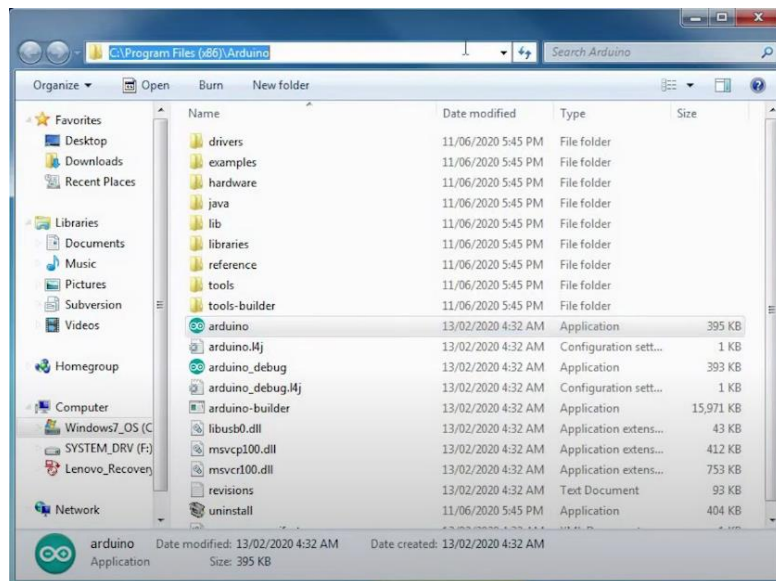


Fig 2.11 Launching Arduino IDE

Step 5: Open your first project

Once the software starts, you have two options:

- Create a new project.

Click on “File” in the menu bar, then select “New” to start a new sketch as shown in figure 2.12

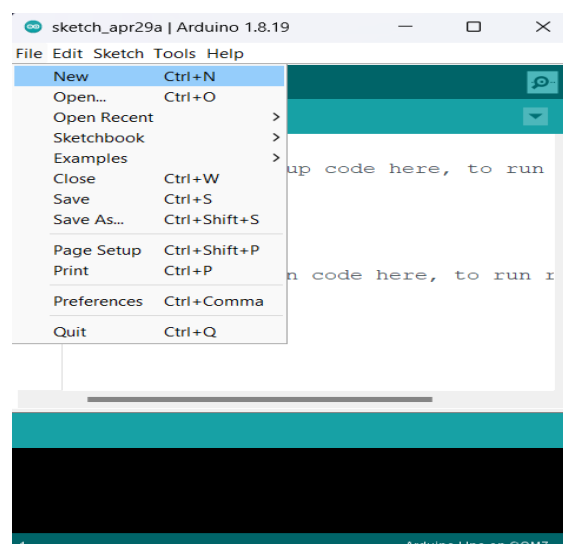


Fig 2.12 Arduino Software Opening New File

To open an existing project example, select File ->Example-> Basics->Blink. Here, we are selecting just one of the examples with the name Blink. It turns the LED on and off with some time delay. You can select any other example from the list.

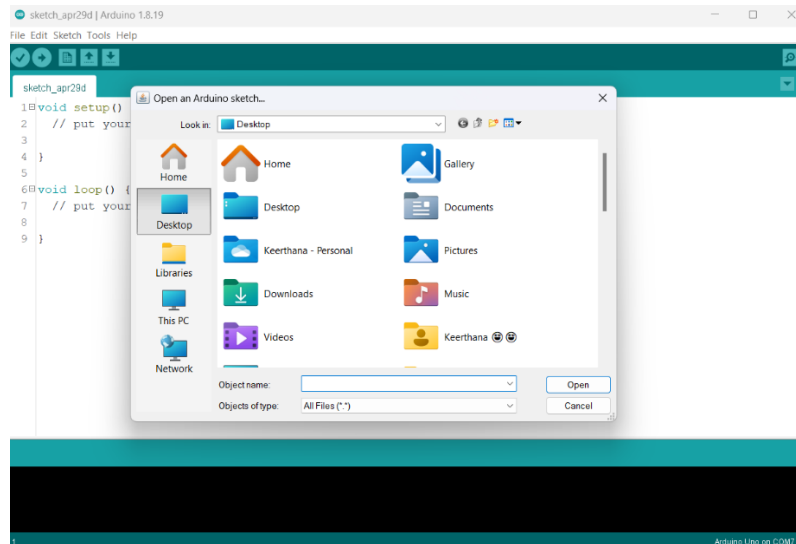


Fig 2.13 Selecting File Type

Step 6: Select your Arduino board

To avoid any error while uploading your program to the board, you must select the correct Arduino board name, which matches with the board connected to your computer. Go to Tools -> Board and select your board.

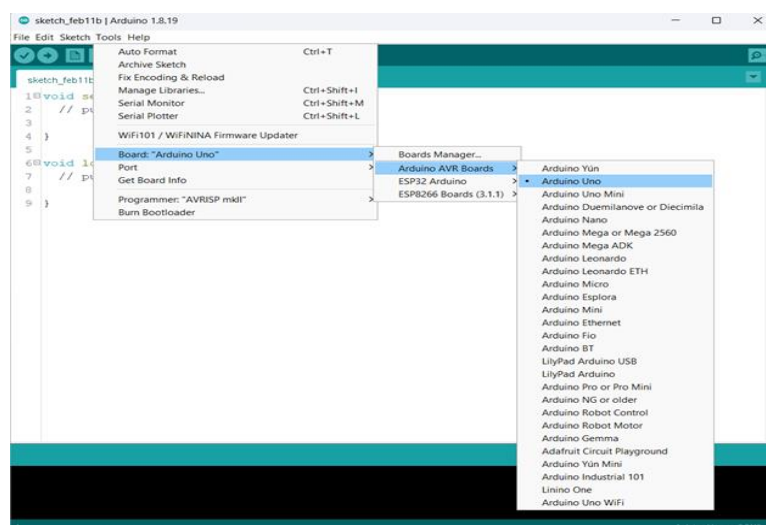


Fig 2.14 Selecting Board Type

Step 7: Select your serial port

Figure 2.15, illustrates the Selection of the serial device of the Arduino board. Go to Tools -> Serial Port menu. This is likely to be COM3 or higher (COM1 and COM2 are usually reserved for hardware serial ports). To find out, you can disconnect your Arduino board and re-open the menu, the entry that disappears should be of the Arduino board. Reconnect the board and select that serial port.

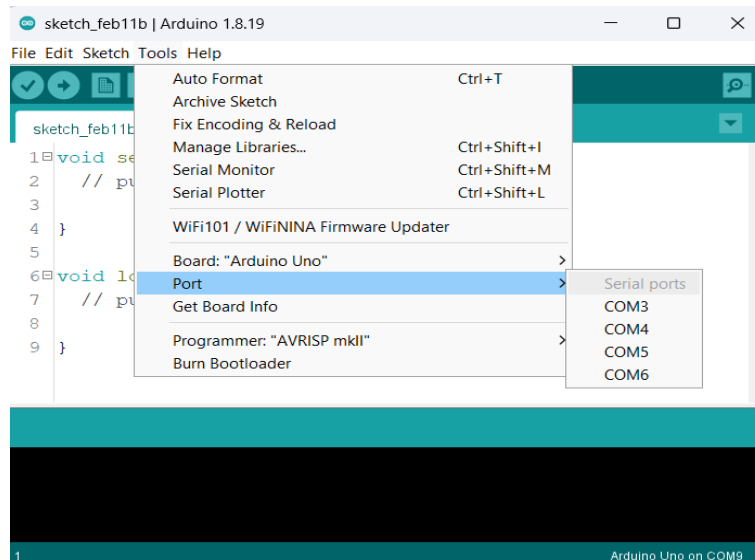


Figure 2.15 Selecting Serial Port

Step 8: Upload the program to your board

Before explaining how we can upload our program to the board, we must demonstrate the function of each symbol appearing in the Arduino IDE toolbar as shown in figure 2.17.

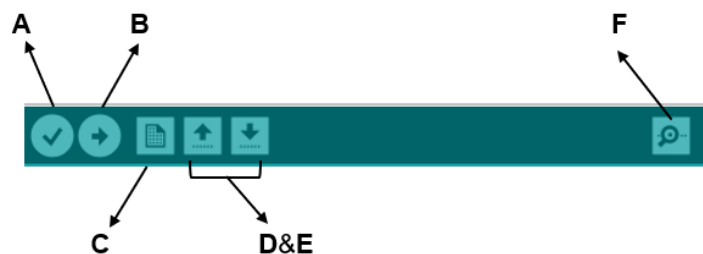


Figure 2.16 Uploading Program To Board

- A. Used to check if there is any compilation error.
- B. Used to upload a program to the Arduino board.
- C. Shortcut used to create a new sketch.
- D. Used to directly open one of the example sketch.
- E. Used to save your sketch.
- F. Serial monitor used to receive serial data from the board and send the serial data to the board.

Now, simply click the "Upload" button in the environment. Wait a few seconds; you will see the RX and TX LEDs on the board, flashing. If the upload is successful, the message "Done uploading" will appear in the status bar.

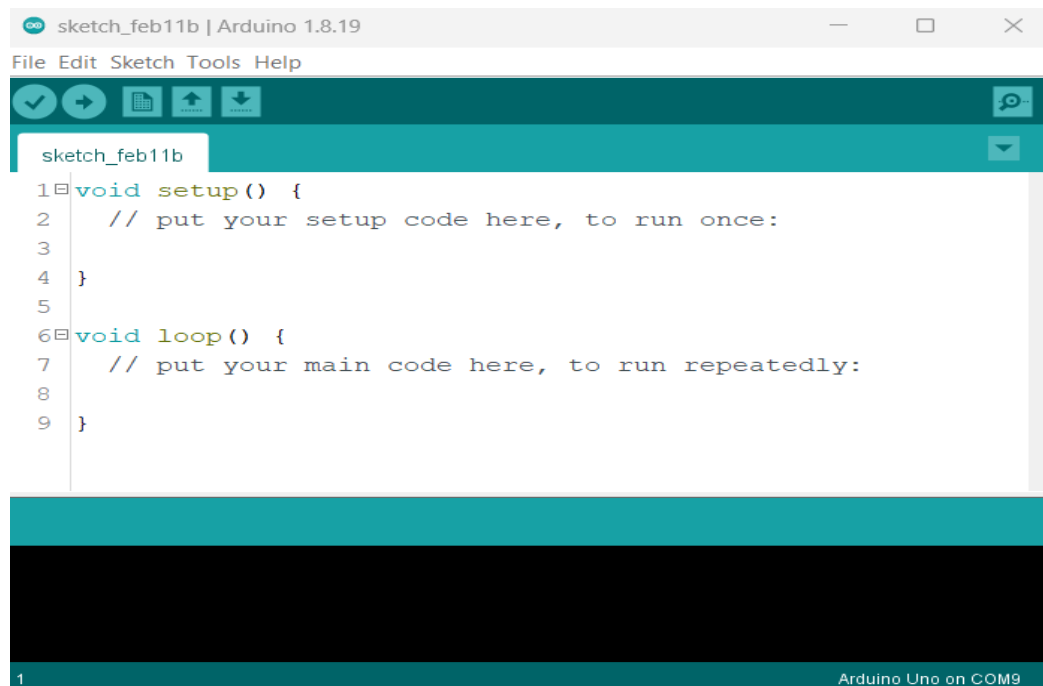
Note: If you have an Arduino Mini, NG, or other board, you need to press the reset button physically on the board, immediately before clicking the upload button on the Arduino Software.

2.7.3 ARDUINO PROGRAM STRUCTURE

We will study in depth; the Arduino program structure and we will learn more new terminologies used in the Arduino world. The Arduino software is opensource. The source code for the Java environment is released under the GPL and the C/C++ microcontroller libraries are under the LGPL. Sketch: The first new terminology is the Arduino program called "sketch". Structure Arduino programs can be divided in three main parts: Structure, Values (variables and constants), and Functions. In this tutorial, we will learn about the Arduino software program, step by step, and how we can write the program without any syntax or compilation error. If you have an Arduino Mini, NG, or other board, you need to press the reset button physically on the board, immediately before clicking the upload button on the Arduino Software

Let us start with the Structure. Software structure consist of two main Function:

- I. () function
- II. Loop() function



```
sketch_feb11b | Arduino 1.8.19
File Edit Sketch Tools Help
sketch_feb11b
1 void setup() {
2   // put your setup code here, to run once:
3
4 }
5
6 void loop() {
7   // put your main code here, to run repeatedly:
8
9 }
```

1 Arduino Uno on COM9

Figure 2.17 Program Structure

The setup () function is called when a sketch starts. Use it to initialize the variables, pin modes, start using libraries, etc. The setup function will only run once, after each power up or reset of the Arduino board.

After creating a setup () function, which initializes and set the initial values, the loop () function does precisely what its name suggests, and loops consecutively, allowing your program to change and respond. Use it to actively control the Arduino board.

2.8 PROJECT SCOPE AND PROJECT RISK

2.8.1 PROJECT SCOPE

The scope of this project includes the following:

The solenoid lock system using RFID technology aims to provide a secure access control solution for various applications. By integrating a solenoid lock mechanism with RFID technology, the system ensures efficient and reliable authentication of users while offering convenience and ease of use. The project involves the design and implementation of hardware and software components, including the solenoid lock, RFID reader, microcontroller, and user interface. Functional requirements such as RFID credential enrollment, real-time access control, and emergency override mechanisms will be addressed to ensure the system's effectiveness. Throughout the project, emphasis will be placed on testing, validation, and adherence to ethical and legal considerations regarding data privacy and security. Upon completion, the solenoid lock system will offer a robust and user-friendly solution for controlling access to secured areas or assets.

2.8.1 PROJECT RISK

The following are some of the risks associated with this project:~

Implementing a solenoid lock system using RFID technology presents several potential risks that need to be identified and addressed. Here are some project risks associated with such a system:

- I. **Technical Compatibility Issues:** There is a risk of compatibility issues between different hardware and software components, such as the RFID reader, microcontroller, and solenoid lock. Variations in communication protocols or power requirements could lead to integration challenges.
- II. **RFID Interference:** Environmental factors or nearby RFID devices could cause interference, leading to unreliable authentication or communication errors. This risk should be assessed to ensure consistent performance.

- III. Security Vulnerabilities: RFID systems can be vulnerable to various attacks, such as relay attacks or cloning of RFID cards/tags. Failure to implement robust encryption and authentication protocols could compromise the security of the system.
- IV. Reliability of Solenoid Lock: The solenoid lock's reliability is critical for the system's effectiveness. Risks include mechanical failures, overheating, or power fluctuations affecting the solenoid's operation, leading to potential security breaches or lockouts.
- V. Data Privacy Concerns: Storing and managing user data, including RFID credentials, raises privacy concerns. Risks include unauthorized access to stored data, data breaches, or mishandling of sensitive information, leading to legal and reputational consequences.
- VI. User Acceptance and Training: Introducing a new access control system requires user acceptance and proper training. Risks include resistance to change, difficulty in understanding system operation, and potential misuse due to lack of awareness or training.
- VII. Regulatory Compliance: Failure to comply with relevant regulations and standards related to access control, data privacy, and security could lead to legal liabilities, fines, or injunctions.

To mitigate these risks, thorough planning, rigorous testing, adherence to industry best practices, and ongoing monitoring and maintenance are essential throughout the project lifecycle. Additionally, establishing contingency plans and maintaining open communication with stakeholders can help mitigate the impact of unforeseen challenges.

CHAPTER 3

RESULTS AND DISCUSSION

3.1 RESULTS

The Figure 3.1 shows a minute trial done in a residential community. And here are its results:

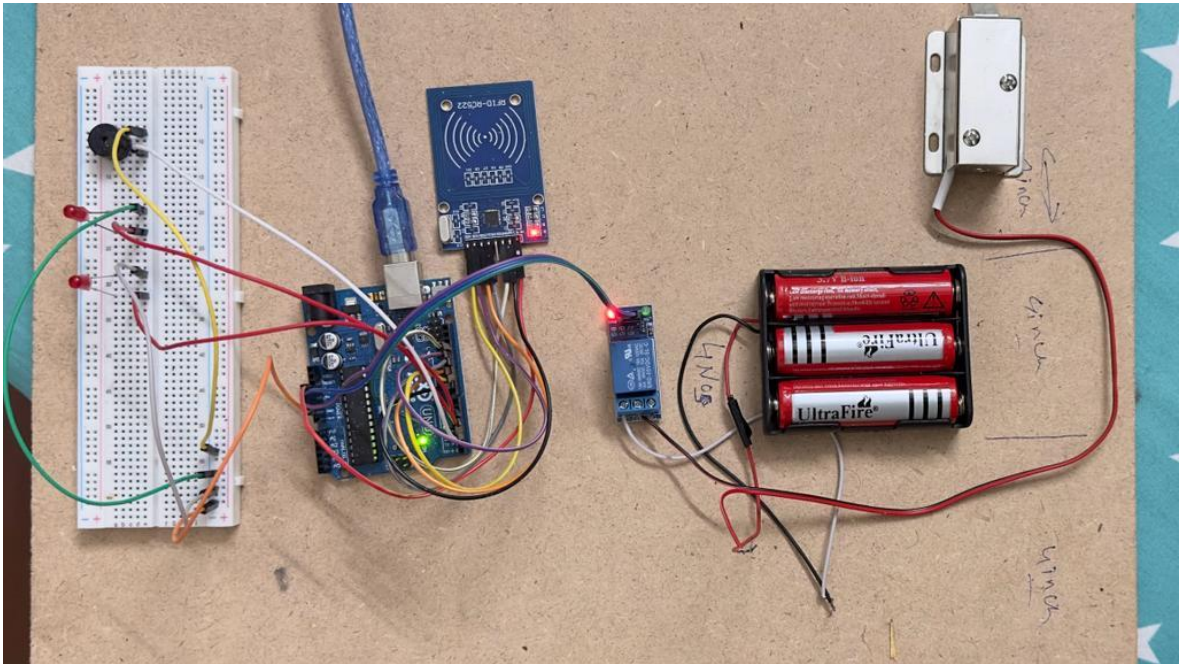


Fig 3.1 Output of the model

The implementation of a solenoid lock system integrated with RFID technology yields highly favorable results, significantly enhancing access control across various domains. By seamlessly combining RFID's secure authentication capabilities with the reliability of solenoid locks, the system achieves robust security measures while streamlining access procedures. Users benefit from the system's simplicity and efficiency, effortlessly gaining entry by presenting their RFID credentials without the need for physical keys. Real-time access control capabilities empower administrators to dynamically manage access permissions, ensuring only authorized individuals can enter designated areas or access specific assets. Moreover, the system offers valuable features such as audit trails and reporting functionalities, enabling thorough monitoring of access events for compliance and

security purposes. Its scalability and flexibility make it adaptable to diverse environments, while potential integration with existing systems further enhances its utility and interoperability. Despite initial investment costs, the long-term benefits in terms of reduced administrative overhead, enhanced security, and improved user experience make the RFID-based solenoid lock system a highly cost-effective solution. Overall, the successful implementation of this system delivers tangible improvements in security, convenience, efficiency, and user satisfaction, establishing it as a cornerstone technology in modern access control applications.

3.2 DISCUSSION

The RFID-based smart lock project represents a noteworthy intersection of technology and practicality, offering a compelling solution to contemporary access control challenges. By leveraging Arduino microcontrollers and RFID technology, the project provides a sophisticated yet accessible means of securing entry points while streamlining user interaction. The discussion surrounding this project delves into various aspects, starting with its core functionality: the integration of RFID readers and servo motors to authenticate and actuate locking mechanisms. This seamless interaction not only enhances security by replacing traditional keys with digital RFID tags but also enhances user convenience through swift, contactless access. Moreover, the project prompts considerations regarding its broader implications, including scalability, interoperability, and adaptability to diverse environments. From residential homes to commercial facilities, the versatility of RFID-based smart locks opens avenues for widespread adoption, potentially revolutionizing access control practices across various sectors. Additionally, the project sparks discourse on the balance between security and usability, emphasizing the importance of robust authentication protocols and user-friendly interfaces. Furthermore, discussions may extend to the project's feasibility, addressing technical challenges, cost-effectiveness, and potential limitations in real-world deployment. Overall, the RFID-based smart lock project serves as a catalyst for dialogue on the intersection of technology, security, and user experience, underscoring its potential to redefine conventional notions of access control in the digital era.

CHAPTER 4

CONCLUSION AND FUTURE WORK

4.1. CONCLUSION

In conclusion, the integration of a solenoid lock system with RFID technology represents a significant advancement in access control solutions, offering a multitude of benefits across various domains. By combining the secure authentication capabilities of RFID with the reliability and efficiency of solenoid locks, this system provides a robust and streamlined approach to access management. The convenience afforded to users, who can effortlessly gain entry by presenting RFID credentials, enhances overall user experience while maintaining stringent security standards. Real-time access control features empower administrators to dynamically adjust permissions, ensuring secure access to designated areas or assets. Moreover, the system's scalability, flexibility, and potential for integration with existing infrastructure enhance its adaptability to diverse environments and applications. While initial investment costs may be higher, the long-term advantages, including reduced administrative overhead and enhanced security, contribute to its overall cost-effectiveness. In summary, the successful implementation of a solenoid lock system using RFID technology offers tangible improvements in security, convenience, efficiency, and user satisfaction, making it a vital component of modern access control strategies.

4.2. FUTURE WORK

Future work for the solenoid lock system integrated with RFID technology presents exciting opportunities for further innovation and refinement. One avenue for advancement involves exploring advanced security measures to counter emerging threats like relay attacks or RFID cloning. Strengthening encryption protocols and integrating multi-factor authentication methods can fortify the system's defenses against unauthorized access attempts. Additionally, integrating biometric

authentication, such as fingerprint or facial recognition, could bolster security and reduce reliance solely on RFID credentials. Another promising direction involves incorporating cloud connectivity to enable remote management and monitoring, enhancing administrative control and accessibility. Mobile access control using smartphones as virtual RFID credentials represents another area ripe for exploration, offering increased convenience for users. Moreover, integrating the system with IoT devices for automation and energy-efficient designs to prolong battery life are crucial considerations for future development. Usability studies and feedback gathering can provide valuable insights to refine the user interface and functionality, ensuring optimal user experience. Finally, pursuing interoperability standards and compatibility with third-party solutions can enhance the system's versatility and integration capabilities. By pursuing these avenues for future work, the solenoid lock system using RFID technology can evolve into a more robust, adaptable, and user-friendly access control solution, meeting the evolving demands of security environments.

REFERENCES

JOURNALS

- [1] G. Sowmya, G. Divya Jyothi, N Shirisha, K Navya and B Padmaja. (2018).
lot Based Smart Door Lock System. International Journal of Engineering &
Technology, 7(3), 223-225.
- [2] Nishad. N. Gupte and Mihir R. Shelar. (2013). Smart Door Locking System.
International Journal of Engineering Research & Technology, 2(11), 2214-
2217.
- [3] O. Agbo David, Madukwe Chinaza and O. OdinyaJotham. (2017). Design
And Implementation Of A Door Locking System Using Android App.
International Journal Of Scientific & Technology Research, 6(8), 198-203.
- [4] Ketan Rathod, Rambabu Vatti, Mandar Nandre and Sanket Yenare. (2017).
Smart door security using Arduino and Bluetooth application. International
Journal of Current Engineering and Scientific Research, 4(11), 73-77.
- [5] Lubhansh Kumar Bhute, Gagandeep Singh, Avinash Singh, Vikram Kansary,
Preetam Rao Kale and Shailendra Singh. (2017). Automatic Door Locking
System Using Bluetooth Module. International Journal for Research in
Applied Science & Engineering Technology, 5(5), 1128-1131.
- [6] Rahul Satoskar and Akarsh Mishrac. (2018). Smart Door Lock and Lighting
System using Internet of Things. International Journal of Computer Science
and Information Technologies, 9(5), 132-135.
- [7] EZ Orji, CV Oleka and UI Nduanya. (2018). Automatic Access Control
System using Arduinoand RFID. Journal of Scientific and Engineering
Research, 5(4), 333-340.

APPENDICES

A. SOURCE CODE:

```
#include <Wire.h>

#include <SPI.h>

#include <MFRC522.h>


#define SS_PIN 10
#define RST_PIN 9
#define LED_G 4 // Green LED pin
#define LED_R 5 // Red LED pin
#define BUZZER 2 // Buzzer pin
#define LOCK 3 // Lock control pin
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 (!Imfr522.PICC_IsNewCardPresent())

```

```

{
    return;
}

// Select one of the cards
if (!mfrc522.PICC_ReadCardSerial())
{
    return;
}

//Show UID on serial monitor
Serial.print("UID tag :");
String content = "";
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) == "03 64 0A 13") // Replace with the UID of the
authorized tag
{
    Serial.println("Access Granted");
    Serial.println();
    delay(500);
    digitalWrite(LED_G, HIGH);
    tone(BUZZER, 2000);
}

```

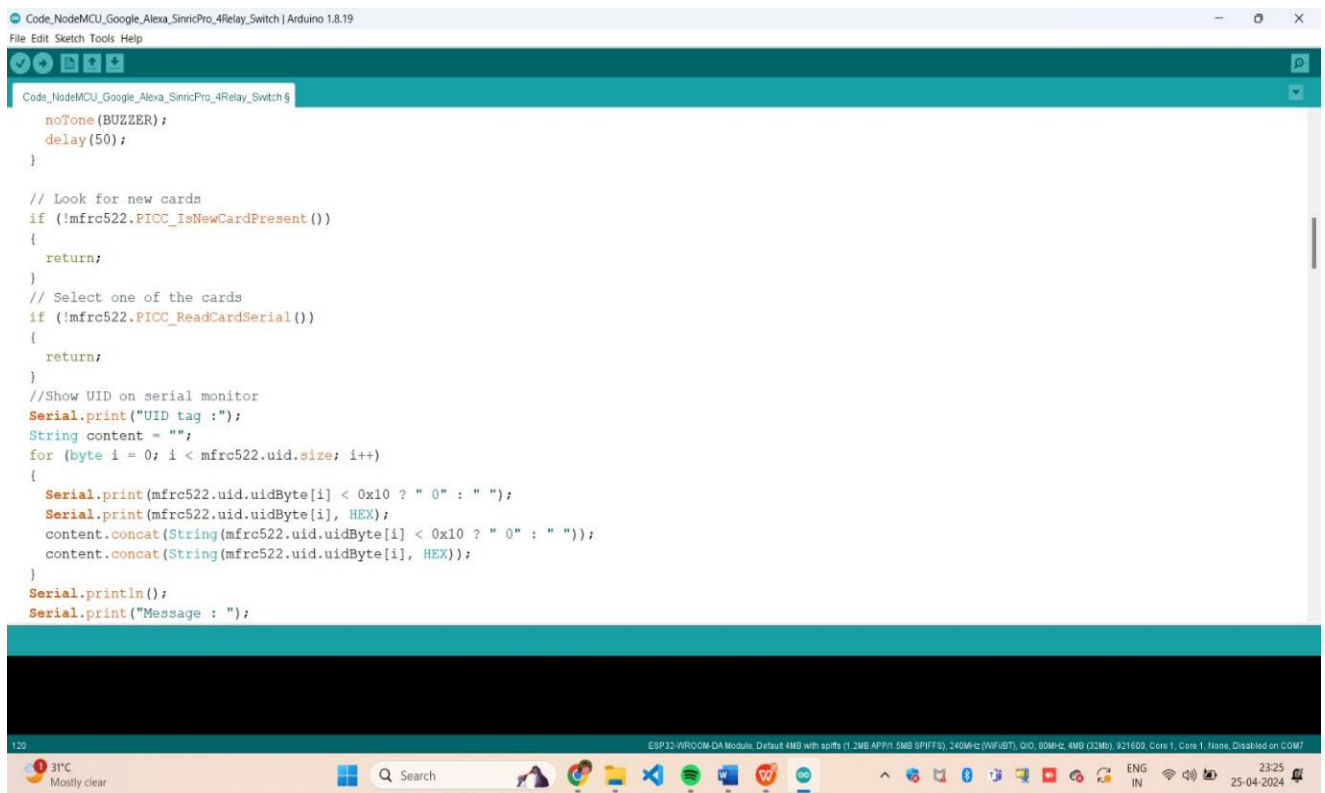
```

delay(100);
noTone(BUZZER);
delay(50);
tone(BUZZER, 2000);
delay(100);
noTone(BUZZER);
digitalWrite(LOCK, LOW);
delay(3000);
digitalWrite(LOCK, HIGH);
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);  
}  
}
```

B. SCREENSHOTS



```
Code_NodeMCU_Google_Alexa_SinricPro_4Relay_Switch | Arduino 1.8.19
File Edit Sketch Tools Help

Code_NodeMCU_Google_Alexa_SinricPro_4Relay_Switch$
noTone(BUZZER);
delay(50);
}

// Look for new cards
if (!mfr522.PICC_IsNewCardPresent())
{
    return;
}
// Select one of the cards
if (!mfr522.PICC_ReadCardSerial())
{
    return;
}
//Show UID on serial monitor
Serial.print("UID tag :");
String content = "";
for (byte i = 0; i < mfr522.uid.size; i++)
{
    Serial.print(mfr522.uid.uidByte[i] < 0x10 ? " 0" : " ");
    Serial.print(mfr522.uid.uidByte[i], HEX);
    content.concat(String(mfr522.uid.uidByte[i] < 0x10 ? " 0" : " "));
    content.concat(String(mfr522.uid.uidByte[i], HEX));
}
Serial.println();
Serial.print("Message : ");
```

Fig 4.1 Arduino Snapshot

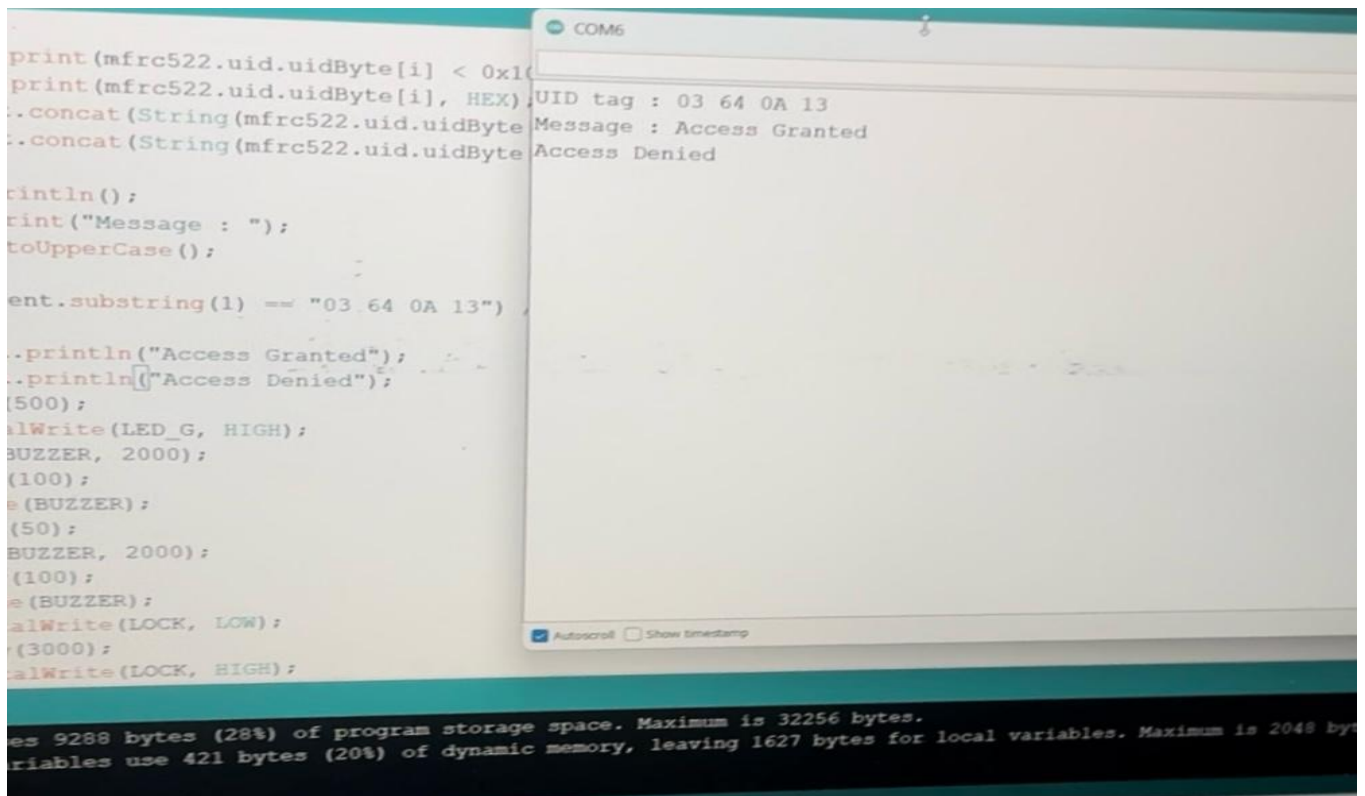


Fig 4.2 Serial Monitor