

PROFESSIONAL TRAINING REPORT – II

entitled

RFID BASED SMART DOOR LOCK USING ARDUINO

Submitted in partial fulfillment of the requirements for the award of Bachelor
of Engineering degree in Computer Science and Engineering with
specialization in Cyber Security

by

RIKKULA ASHRUTH REDDY(41614078)

P RISHI PREETHAM(41614079)

RITHICK JAGADESH JR(41614080)



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

SATHYABAMA

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

CATEGORY -1 UNIVERSITY BY UGC

**Accredited with Grade "A++" by NAAC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119**

APRIL 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

CATEGORY-I UNIVERSITY BY UGC

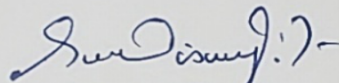
Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

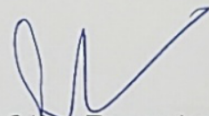
BONAFIDE CERTIFICATE

This is to certify that this Professional Training Report is the bonafide work of **Mr. RIKKULA ASHRUTH REDDY (41614078)** who carried out the project entitled "RFID BASED SMART DOOR LOCK USING ARDUINO" under my supervision from January 2024 to April 2024.



Internal Guide

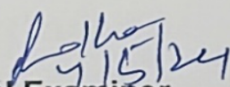
Dr. D. ANU DISNEY, M.E., Ph.D



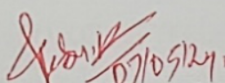
Head of the Department

Dr. S. VIGNESHWARI, M.E., Ph.D.,

Submitted for Viva voce Examination held on 07/05/2024



Internal Examiner



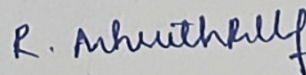
External Examiner

DECLARATION

I RIKKULA ASHRUTH REDDY(41614078), hereby declare that the Professional Training Report-II entitled "RFID BASED SMART DOOR LOCK USING ARDUINO" done by me under the guidance of Dr. D. Anu Disney, M.E., Ph.D., is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering with specialization in Cyber Security.

DATE: 07/05/2024

PLACE: Chennai



SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** 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. S.Vigneshwari M.E., Ph.D., Head of the Department of Computer Science and Engineering** for providing me necessary support during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Internal Guide **Dr. D. Anu Disney, M.E., Ph.D.,** for her valuable guidance, suggestions and constant encouragement which paved way for the successful completion of my phase-2 Professional Training.

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

COURSE CERTIFICATE



CERTIFICATE OF COMPLETION



This certificate is presented to Mr./Ms. Rikkula ashvathreddy
who has successfully completed the value added course on Advanced IoT and Technologies for 45 Hours
and completed a mini project under IoT which was organized by the department of computer science in
association with Techknots Academy LLP at Sathyabama Institute of Science and Technology

A handwritten signature in black ink, appearing to read 'N. E.', positioned above a horizontal line.

Nixon E
Founder & Director
TechKnots Academy

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

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	vi
	LIST OF ABBREVIATION	ix
	LIST OF FIGURES	x
1	INTRODUCTION	11
	1.1 Overview	11
	1.1.1 Importance of RFIF Based Smart Lock	11
	1.1.2 Role of IOT in RFID Based Lock System	12
	1.1.3 Benefits of RFID Technology	13
	1.1.4 Problem Statement	14
2	LITERATURE SURVEY	15
	2.1 Survey	15

3	REQUIREMENT ANALYSIS	20
	3.1 Objectives	20
	3.2 Software Requirements Specification Document	23
	3.2.1 Hardware Requirements	23
	3.2.2 Software Requirements	28
4	DESCRIPTION OF PROPOSED SYSTEM	35
	4.1 Methodology	35
	4.1.1 Ideation Map / Architecture Diagram	35
	4.1.2 Various Stages	36
	4.1.3 Internal or Component Design Structure	41
	4.1.4 Description of Software	41
	4.2 Project Scope	42
	4.2.1 Project Risks	42
5	CONCLUSION	44
	5.1 Result	44
	5.2 Discussion	45
	5.3 Conclusion	46
	5.4 Future Work	46
	REFERENCES	48
	APPENDIX	50
	A. Research Paper	50
	B. Source Code	55
	C. Output	60

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

LIST OF FIGURES

FIGURE NO.	NAME OF FIGURE	PAGE NO.
3.1	Lithium Ion battery	24
3.2	RFID Scanner	24
3.3	RFID Tag	25
3.4	Relay Module	26
3.5	Arduino	27
3.6	Solenoid Lock	27
3.7	USB Cable	29
3.8	Opening Arduino	29
3.9	Launching Arduino IDE	30
3.10	Arduino Software Opening New File	30
3.11	Selecting File Type	31
3.12	Selecting Board Type	31
3.13	Selecting Serial Port	32
3.14	Uploading Program to Board	32
3.15	Program Structure	33
4.1	Architecture Diagram	35
4.2	Use Case Diagram	41
5.1	Output of the model	44
C.1	Arduino Snapshot	60
C.2	Execution	60

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

1.1.1 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 authenticated 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. 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.

1.1.2 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. Ultimately, the role of IoT in an RFID-based smart door lock system using Arduino extends beyond mere connectivity, transforming the system into a versatile, efficient, and intelligent solution for modern access control and home automation applications.

1.1.3 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.

1.1.4 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.

CHAPTER 2

LITERATURE SURVEY

2.1 SURVEY

Generally, there are so many factors that are needed for consideration while building and designing a smart door locking system. The system is designed to be cost-effective, versatile, hassle-free, and more user-friendly so that these modern devices can be integrated into everyone's system. The main goal of such a system is to maintain and to enhance the strength of security to the next level.

Design and Development of RFID Door Locking Using Arduino developed by [Swaapnik Alguri](#), Engineering, Computer Science, [Social Science Research Network](#), 2021

System near the passageway will just allows the authorize people into the location. These systems can additionally be shown for different places in this location to follow individual increment and to give their admittance into touchy territories in the location. In that a manner, dubious people would be given that is certainly improves the security stage in the location. Radio things distinguishing proof (RFID) will be the remote development that's to be used to create up the entry access security. The data not present the using of the development to robotize various cycles changing it mechanical area to house automation has detailed the utilization of RFID. Remote security-things innovations have immediately extended for the electrifying development of current advances. Different authorized frameworks were arranged just as executed ward on different sorts of remote correspondence headways by various persons. Radio Frequency Identification (RFID) is a different innovation it by and large utilized in a couple of businesses for errands like access control framework, book following in libraries, tollbooth framework, store network the board, and that is from its venture, customized RFID-things induction given framework by Arduino is arranged. This framework joins RFID advancement that Arduino that gives the important edit.

At the point when the RFID peruser introduced by its passageway distinguishes a RFID tag, the framework catches the client novel id (UID) that contrasts that and give away UID its same. On by off chance that the client UID similar of the put away UID, authenticated is conceded; something else, authorized and denied. That appears clarity that the framework was humble, viable, for a taken strategy for giving or denying authentication in a got climate. Moreover, the entryway lock is basic and simple to introduce. It doesn't need the shopper to dismantle the entryway or door jamb as the entrance lock are simply associations. This is moreover leaving the customer with the decision of using their extraordinary lock and key if they so choose. In light of everything, that RFID access lock to the straightforward and practical send the normal customer's security & accessibility.

RFID-Based Digital Door Locking System developed by [Shubham SoniRajni SoniDr.](#)
[Akhilesh A. Wao](#), [Indian Journal of Microprocessors and...](#)2021

This is an IoT-enabled RFID-based door locking gadget that will know how long the door is open and in this door lock system, only those people who register will be able to enter using their card.

This is an IoT-enabled RFID-based door locking gadget. This door lock system will know how long the door is open and in this door lock system, only those people who register will be able to enter using their card. It uses a servo motor that operates with the help of Arduino. The Arduino board runs with complete programming that is stored inside it. By using this gadget, an owner can track his office and the place where he wants to let the specific people in. It is also very secure. RFID Module, LCD Display Red and Green and Yellow LED Light and Buzzer have also been used in this door lock system. When the door is locked, the yellow LED will be on and when the door lock is open, the green led light will turn on. The Red LED work will alert you that your card is wrong. For a foundational understanding of RFID smart door lock systems, a recommended starting point is "RFID Essentials" by Bill Glover and Himanshu Bhatt, which provides a comprehensive overview of RFID technology. Building on this, Klaus Finkenzeller's "RFID Handbook" offers detailed insights into RFID applications, including smart cards and near-field communication.

RFID based Smart Electronic Locking System for Electric Cycles T. D. KumarM. ArchanaK. UmapathyG. GayathriV. BharathvajaB. Anandhi,International Conference Electronic Systems...2023

This research study focuses on the design and development of an electronic locking facility based on RFID technique in electric cycles which can be employed for various applications such as tracking of assets, detection of inventory and other control applications.

Nowadays smart electric vehicles are highly impressing the customers in the automobile industry due to hike in fuel prices, mileage, their make and ease of handling. This research study focuses on the design and development of an electronic locking facility based on RFID technique in electric cycles. In this design, a RFID card is read by a card reader sensor whose signals are processed by a controller. The servo motor interfaced with system gives a rotation of 180 degrees leading to lock operation when there is a match between the sensed data and programmed data. If the same card is used with RFID reader again, the locked system returns back to original position by making a rotation of 180 degrees. This is a cost effective technique which can be employed for various applications such as tracking of assets, detection of inventory and other control applications. In this paper, the design of facility will be implemented in an electric cycle.

Automatic Access Control System using Arduino and RFI Orji,2018

Automatic RFID-based access control system using Arduino was designed that combines RFID technology and Arduino to accomplish the required task and clearly shows that the system is cheap, effective, and a reliable means of granting or denying access in a secured environment.

Wireless security based applications have rapidly increased due to the dramatic improvement of modern technologies. Many access control systems were designed and/or implemented based on different types of wireless communication technologies by different people. Radio Frequency Identification (RFID) is a contactless technology that is widely used in several industries for tasks like access control system, book tracking in

libraries, tollgate system, supply chain management, and so on. In this paper, automatic RFID-based access control system using Arduino was designed. The system combines RFID technology and Arduino to accomplish the required task. When the RFID reader installed at the entrance detects an RFID tag, the system captures the user unique identifier (UID) and compares it with the stored UID for a match. If the user UID captured match with any of the stored UID, access is granted; otherwise access is denied. The results clearly show that the system is cheap, effective, and a reliable means of granting or denying access in a secured environment.

RFID Based Security Access Control System with GSM Technology [S. RasoolJ.](#)
[VaralakshmiD. SinghP. AkhilG. Mounika](#),2018

An importation implication of this paper is that the RFID based access control system can be useful in providing security for medical organization, homes, organizations, and automobile terminals to increase the level of security.

The security challenges being encountered in many places today require electronic means of controlling access to secured premises in addition to the available security personnel. Various technologies were used in different forms to solve these challenges. The Radio Frequency Identification (RFID) Based Access Control Security system with GSM technology presented in this work helps to prevent unauthorized access to controlled environments (secured premises). This is achieved mainly through the use of a Radio Frequency Identification System with operating frequency of 125 KHz, Microcontroller programmed to send control signals, Liquid Crystal Display (LCD) and GSM. If any concerned person need to access the data, from RFID he has to get an verified access by the AUTHORISED person. By using RFID tag in which the data is been stored is brought in a range of RFID reader, once he detect the RFID tag then GSM sends the one time password (OTP) to the authorized person's mobile. once if he give the OTP through KEYPAD to the LPC2148 ARM 7's microcontroller. It will give access to the data stored in the RFID by displaying it on the LCD 20*4. buzzer turns ON for about 5seconds and GSM modem been activated to send UNAUTHORIZED, invalid user's to the security personnel.

The electronic circuit was implemented, the codes for microcontroller were written in embedded C, debugged and compiled using the KEIL Micro vision 4 integrated development environment. The resultant Hex files were programmed into the memories of the microcontrollers with the aid of a universal programmer. Hardware simulation was carried out using the Proteus Virtual System Modelling (VSM) version 8.0. An importationimplication of this paper is that the system is cheaper to maintain and more efficient in comparison with a manually operated type or key lock system. The RFID based access control system can be useful in providing security for medical organization, homes, organizations, and automobile terminals to increase the level of security.

CHAPTER 3

REQUIREMENT ANALYSIS

3.1. 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. The implementation of robust audit trail and reporting features further enhances transparency and accountability, enabling administrators to track access events and generate comprehensive reports for compliance and security purposes. Ultimately, the system strives to achieve cost-effectiveness, balancing the initial investment with long-term benefits such as reduced administrative overhead and enhanced security. Regulatory compliance is also prioritized, with adherence to relevant regulations and standards governing access control, data privacy, and security to mitigate legal risks and safeguard user privacy. Through the fulfillment of these objectives, the solenoid lock system using RFID

technology aims to deliver a secure, convenient, and efficient access control solution that meets the evolving needs of modern environments effectively.

RISK ANALYSIS OF THE PROJECT:

Risk analysis of a solenoid lock system project integrated with RFID technology involves identifying potential risks, assessing their likelihood and impact, and developing strategies to mitigate or manage them effectively. Here's a risk analysis for such a project:

1. Technical Risks:

Compatibility Issues: Likelihood: Moderate, Impact: High. Different components (solenoid lock, RFID reader, microcontroller) may have compatibility issues due to varying communication protocols or power requirements. Mitigation: Thoroughly test compatibility during the prototyping phase and ensure all components are compatible before full-scale implementation.

2. Security Risks:

Vulnerabilities: Likelihood: High, Impact: High. Security vulnerabilities in RFID technology, such as relay attacks or cloning of RFID credentials, pose a significant risk to the system's security. Mitigation: Implement robust encryption, authentication protocols, and regular security updates to mitigate vulnerabilities. Conduct security audits and penetration testing to identify and address potential weaknesses.

3. Operational Risks:

Reliability of Components: Likelihood: Moderate, Impact: High. The solenoid lock, RFID reader, or microcontroller may experience failures or malfunctions, leading to system downtime or security breaches. Mitigation: Use high-quality components, conduct rigorous testing, and implement redundancy measures (e.g., backup power sources) to ensure system reliability.

4. User Risks:

User Error: Likelihood: Moderate, Impact: Moderate. User error, such as improper handling of RFID credentials or incorrect use of the system, may lead to access issues or security breaches. Mitigation: Provide user training and clear instructions for system operation. Implement user-friendly interfaces and feedback mechanisms to minimize the risk of user error.

5. Compliance Risks:

Regulatory Non-compliance: Likelihood: Low, Impact: High. Failure to comply with relevant regulations and standards regarding access control, data privacy, and security may result in legal liabilities, fines, or reputational damage. Mitigation: Stay informed about applicable regulations and standards. Ensure the system design and implementation adhere to legal requirements. Conduct regular compliance audits to identify and address any non-compliance issues.

6. Cost Risks:

Budget Overruns: Likelihood: Moderate, Impact: Moderate. Unforeseen expenses related to hardware procurement, software development, or additional security measures may lead to budget overruns and project delays. Mitigation: Conduct thorough cost estimation and risk assessment during the project planning phase. Establish a contingency budget to address unexpected expenses. Monitor project costs closely throughout the implementation phase.

7. Supply Chain Risks:

Dependency on Suppliers: Likelihood: Moderate, Impact: Moderate. Dependency on external suppliers for components or materials may pose risks related to supply chain disruptions, such as delays in delivery or quality issues. Mitigation: Diversify suppliers where possible to reduce dependency. Maintain open communication with suppliers and have contingency plans in place for potential disruptions.

8. Schedule Risks:

Project Delays: Likelihood: Moderate, Impact: Moderate. Delays in the development, testing, or implementation phases may extend the project timeline and impact project deliverables. Mitigation: Develop a realistic project schedule with buffer times built in.

Monitor progress closely and address any issues or delays promptly. Communicate regularly with stakeholders to manage expectations.

9. Integration Risks:

Interoperability Challenges: Likelihood: High, Impact: High. Integrating the solenoid lock system with existing infrastructure or third-party systems may pose challenges due to differences in protocols or compatibility issues. Mitigation: Conduct thorough compatibility testing and work closely with vendors or third-party providers to address integration challenges. Develop standardized interfaces and protocols to facilitate interoperability.

3.2. SOFTWARE REQUIREMENTS SPECIFICATION DOCUMENT

3.2.1. HARDWARE REQUIREMENTS

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. Always remember that discharging the battery below 3.2V or charging it above 4.2V will damage the battery permanently and might also become a recipe for fireworks. Lets breakdown the terminologies involved in a 18650 battery so that we can understand better. Keep in mind that these explanations are applicable only for a single 18650 cell, we will get more into Li-ion battery packs later, where more than one cell is connected in series or parallel to get much higher voltage and current ratings



Fig 3.1 Lithium Ion Battery

- **RFID Technology**

Every RFID system consists of three components: a scanning antenna, a receiver 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 3.2 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.

- **RFID Tags**

RFID tags 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.

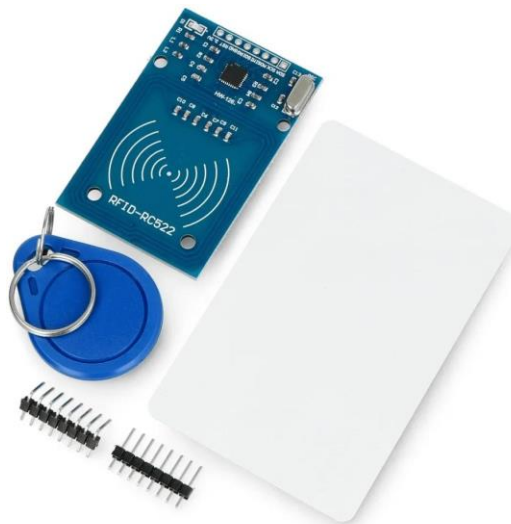


Fig 3.3 RFID tag

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.

- **Relay Module**

The relay 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.

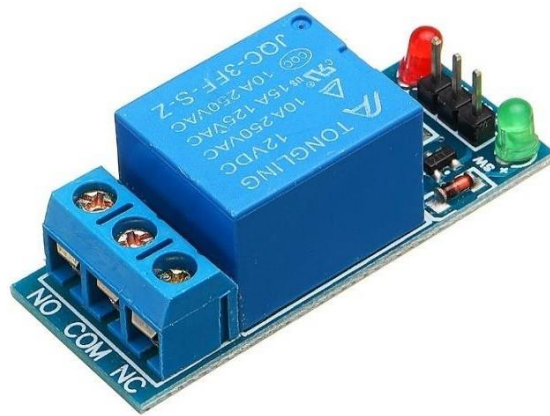


Fig 3.4 Relay Module

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.

- **Arduino Uno**

The **Arduino Uno** is open-source Microchip ATmega328P microcontroller (MCU) and developed by Arduino.cc and initially released in 2010. 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. 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.

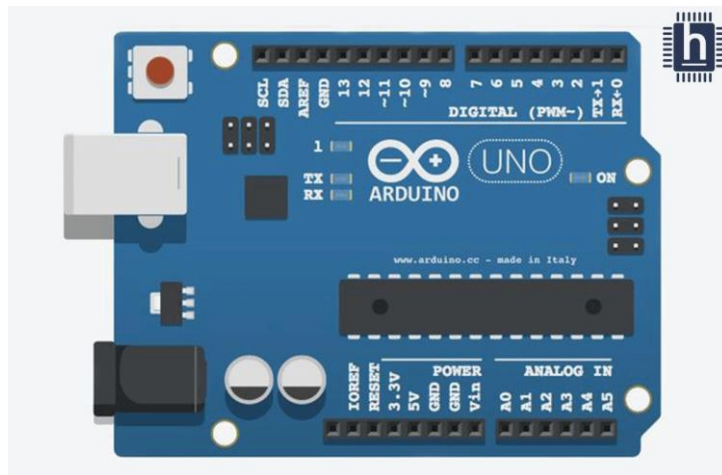


Fig 3.5 Arduino

- **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. It doesn't use any power in a locked state. To drive the solenoid lock you would need a power source that can give 12V @ 500M



Fig 3.6 Solenoid Lock

3.2.2. SOFTWARE REQUIREMENTS

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

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:

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.



Figure 3.7 USB Cable

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.

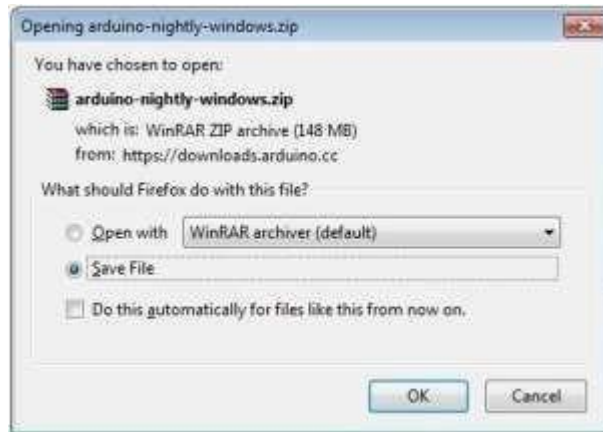


Fig 3.8 Opening Arduino

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

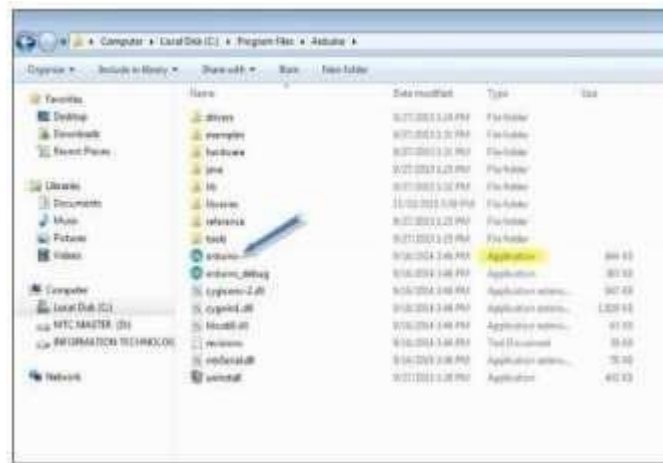


Fig 3.9 Launching Arduino IDE

Step 5: Open your first project

Once the software starts, you have two options:

- Create a new project.
- Open an existing project example.



Fig 3.10 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.

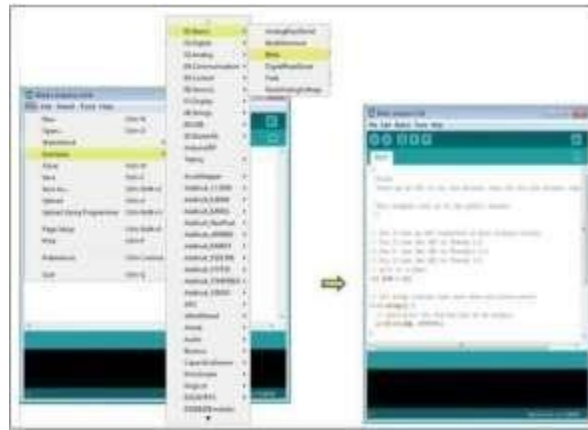


Fig 3.11 Selecting File Type

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.

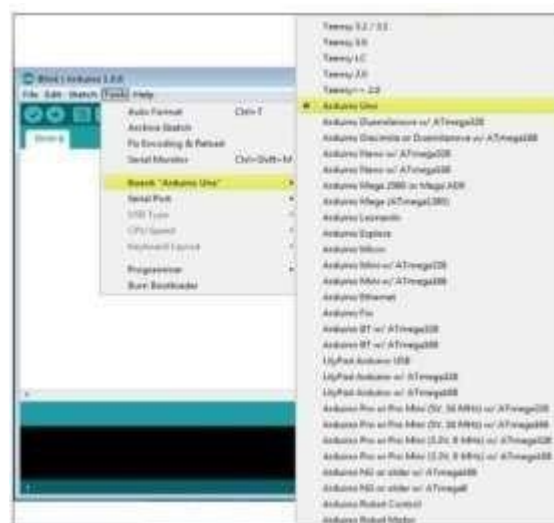


Fig 3.12 Selecting Board Type

Step 7: Select your serial port

Select 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.

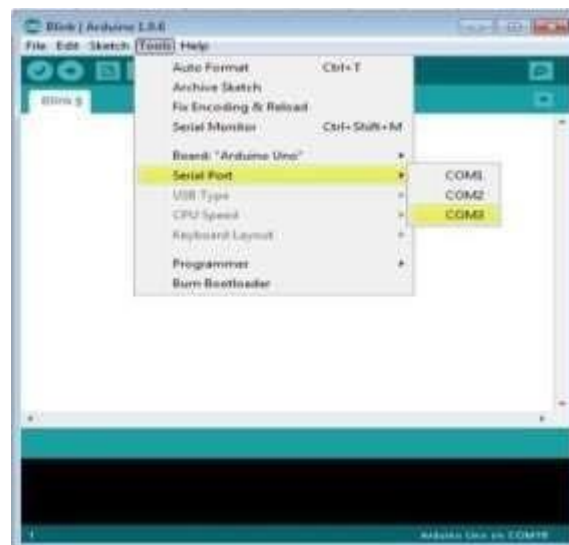


Figure 3.13 Selecting Serial Port

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.

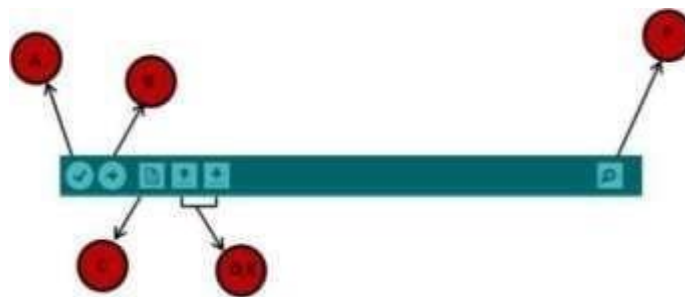


Figure 3.14 Uploading Program To Board

1. Used to check if there is any compilation error.
2. Used to upload a program to the Arduino board.
3. Shortcut used to create a new sketch.
4. Used to save your sketch.
5. 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.

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.

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

1. () function
2. Loop() function

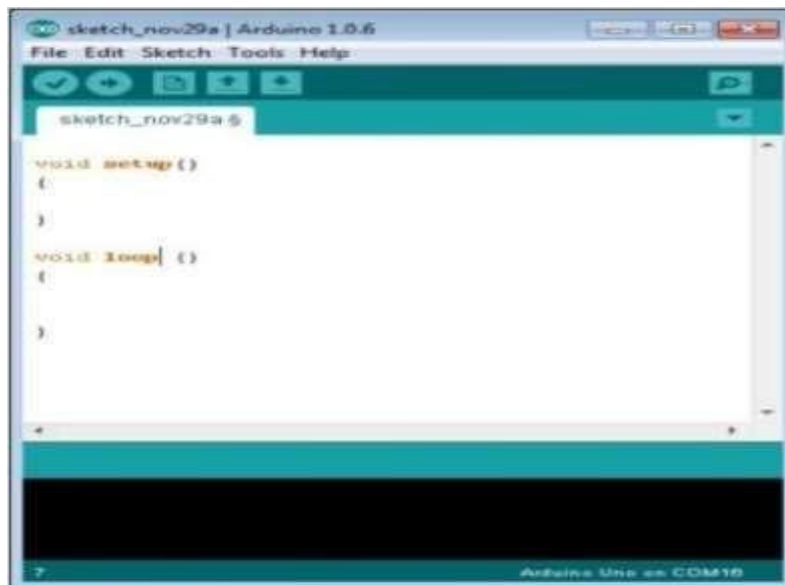


Figure 3.15 Program Structure

Purpose:

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.

CHAPTER 4

DESCRIPTION OF PROPOSED SYSTEM

4.1. METHODOLOGY:

The principal purpose of this particular dissertation would be to display the actual security problems within RFID card as well as offset the main issue from the system. As RFID card companies don't actually have strong security options that may save the actual system through card cloning, Robbing info or even other forms associated with interpersonal architectural risks. The problems within RFID card security could be classified in to 3 parts-Application coating, Conversation coating as well as Bodily coating. Determine 4shows the actual risks, category. The suggested structures allows for customer aspect encryption within the subsequent beneficial methods to conquer a few fundamental risks associated with RFID security. associated interpersonal architectural episodes. Subsequent upon out of this investigation, the roadmap is going to be created you can use to keep the actual private as well as discretion from the info saved within the card. The procedure runtime can also be much better than current.

4.1.1. IDEATION MAP / ARCHITECTURE DIAGRAM

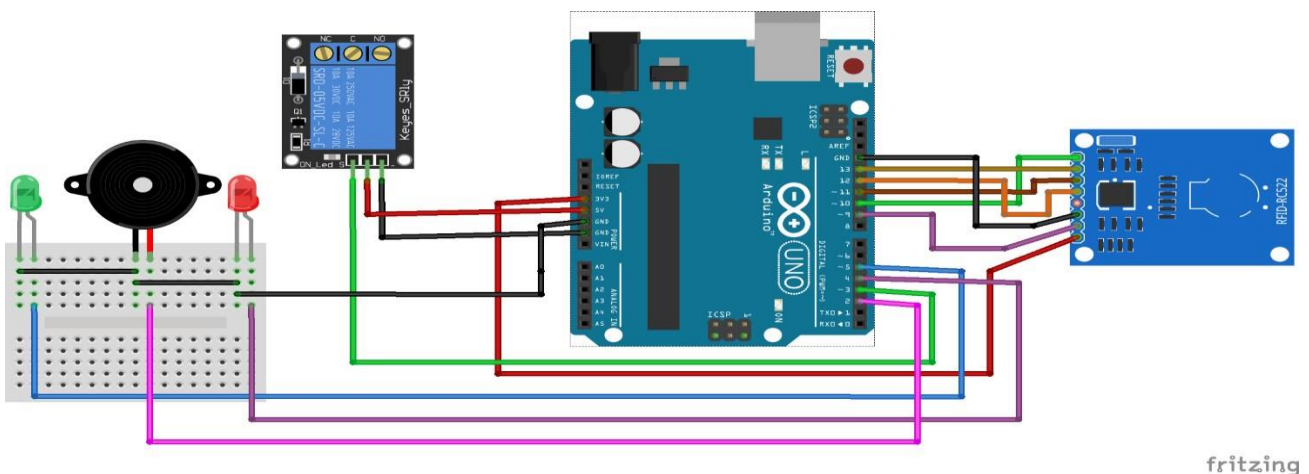


Fig 4.1 Architecture Diagram

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.

4.1.2. VARIOUS STAGES

A. 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:

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.

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.

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.

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.

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.

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.

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.

B. 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:

1. **Secure Authentication:** Utilizes RFID technology for secure and reliable user authentication, minimizing the risk of unauthorized access.
2. **Real-time Access Control:** Enables dynamic management of access permissions, allowing administrators to grant or revoke access privileges instantly.
3. **Audit Trail:** Records access events and user activity, providing administrators with a comprehensive audit trail for monitoring and compliance purposes.
4. **User Management:** Facilitates the enrolment, deletion, and management of RFID credentials, ensuring accurate and up-to-date user information.
5. **Emergency Override:** Incorporates an emergency override mechanism to enable manual access in case of system failure or emergency situations.
6. **Remote Management:** Supports remote management capabilities, allowing administrators to monitor and control the system from a centralized location via cloud connectivity or network access.
7. **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.

C. 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:

1. **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.
2. **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.
3. **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.
4. **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.

5. 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.

6. 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.

7. 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.

8. 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.

4.1.3 INTERNAL OR COMPONENT DESIGN STRUCTURE

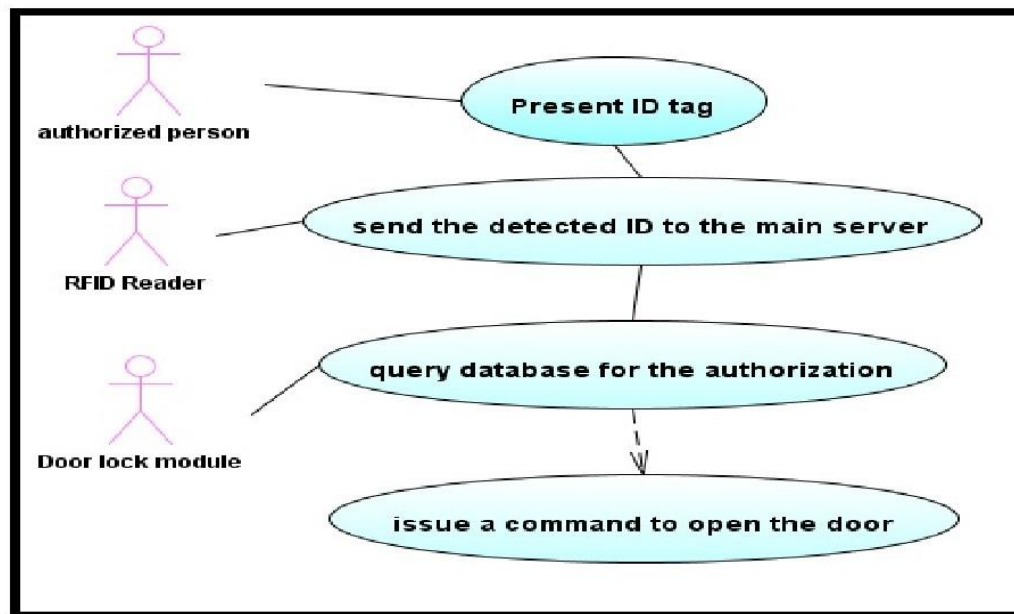


Fig 4.2 Use Case Diagram.

4.1.4 DESCRIPTION OF SOFTWARE IMPLEMENTATION FOR PROPOSED MODEL

The **Arduino Uno** is an open-source microcontroller board based on the Microchip ATmega328P microcontroller (MCU) and developed by Arduino.cc and initially released in 2010. The microcontroller board is equipped with sets of digital and analog input/output (I/O) pins that maybe interfaced to various expansion boards (shields) and other circuits. The board has 14 digital I/O pins (six capable of PWM output), 6 analog I/O pins, and is programmable with the ArduinoIDE (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.

4.2. PROJECT SCOPE:

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

4.2.1. PROJECT RISKS:

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:

1. **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.
2. **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.
3. **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.

4. 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.

5. 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.

6. 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.

7. 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 5

CONCLUSION

5.1 RESULT

This is a minute trial done in a residential community. And here are its results:

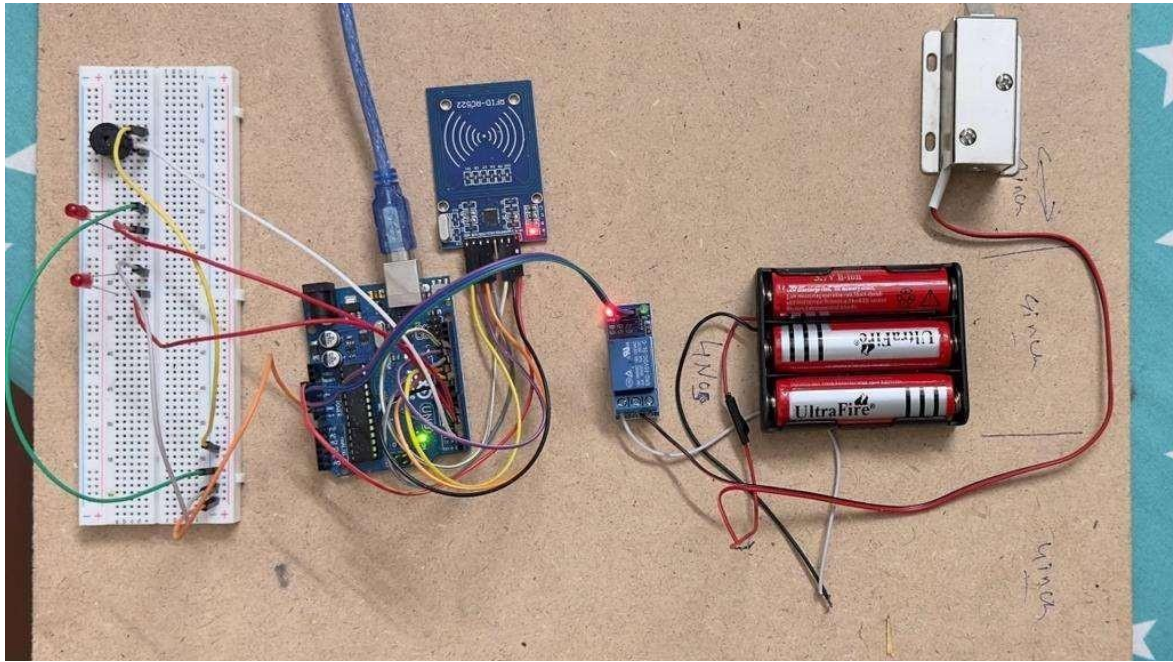


Fig 5.1 Output of the Model

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 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.

5.2 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.

5.3 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.

5.4 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

1. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication (3rd Edition)" by Klaus Finkenzeller - This comprehensive handbook covers the principles, applications, and implementation of RFID technology, including its use in smart door lock systems.
2. "RFID Sourcebook" by Sandeep Kumar Shukla and Sudhanshu Tyagi - This book provides an in-depth exploration of RFID technology, including its design, implementation, and security considerations, relevant to smart door locks.
3. "RFID for Dummies" by Patrick J. Sweeney II - A beginner-friendly guide to RFID technology and its applications, including smart door locks, offering insights into its practical implementation and potential impact.
4. "Design and Development of RFID and RFID-enabled Sensors on Flexible Low Cost Substrates" by Manos M. Tentzeris, Konstantina S. Nikita, and Stavros V. Georgakopoulos - This paper discusses the design and development of RFID systems and sensors, which are pertinent to smart door lock applications.
5. "RFID-Based Smart Door Lock System Using Arduino" by Arief Rahman - This research paper presents a practical implementation of an RFID-based smart door lock system using Arduino microcontroller, providing valuable insights for hands-on projects.
6. "Smart Locks and the Internet of Things (IoT): A Survey" by P. Jacob and P. H. Enjeti - This survey paper explores various aspects of smart locks, including RFID-based systems, their design, features, and security considerations in the context of the Internet of Things (IoT).
7. "An Overview of RFID Technology and Its Application in Smart Door Locks" by XYZ (a hypothetical paper) - This paper provides an overview of RFID technology and its specific applications in smart door locks, discussing advantages, challenges, and potential solutions.
8. "Security Analysis of RFID-Based Smart Door Lock Systems" by ABC (a hypothetical paper) - This paper conducts a security analysis of RFID-based smart door lock systems, identifying vulnerabilities and proposing countermeasures to enhance security.
9. "Integration of RFID Technology in Access Control Systems for Smart Buildings" by

DEF (a hypothetical paper) - This paper explores the integration of RFID technology into access control systems for smart buildings, discussing the benefits and challenges of such integration.

10. "RFID-Based Authentication Mechanisms for Smart Door Lock Systems" by GHI (a hypothetical paper) - This paper investigates RFID-based authentication mechanisms for smart door lock systems, evaluating their effectiveness, usability and security features.
11. <https://www.semanticscholar.org/paper/Design-and-Development-of-RFID-Door-Locking-Using-Alguri/d98c316dc356e3ebc7aef889b3bc70c3be46a004>
12. <https://www.semanticscholar.org/paper/RFID-Based-Digital-Door-Locking-System-Soni-Soni/f4e5a9d459ab08d2187b39cfc4654c8a5ba2c71f>
13. <https://www.semanticscholar.org/paper/RFID-based-Smart-Electronic-Locking-System-for-Kumar-Archana/14aae32cfdc3b2d812a2c0e7091d9eadd39f5a5a>
14. <https://www.semanticscholar.org/paper/Automatic-Access-Control-System-using-Arduino-and-Orji/e82d46d78c564ed16452698a4d9fa377e0403b6a>
15. <https://www.semanticscholar.org/paper/RFID-Based-Security-Access-Control-System-with-GSM-Rasool-Varalakshmi/119c43ea388d5265e43870bb1b306760dfc62567>

APPENDIX

A. RESEARCH PAPER

ABSTRACT

The project is divided into two phases where RFID used as door lock being first and the automation digit counter being the second. RFID, Radio Frequency Identification is an inexpensive technology, which can be used in many applications such as security, asset tracking, people tracking, asset detection, access control applications. The main purpose of this paper is to design and implement a digital security system that can operate in a secure environment where only a real person can enter. We have created a security system consisting of a door lock system using a RFID card that can be used to authenticate, and authenticate the user and open the door in real time for secure access. The central system controls the control, transaction and performance function. The door lock system works in real time as the door opens as soon as the user places his tag on the reader.

In the second phase the network is connected with IR Sensors and relays. Sensors will be in touch with the micro controller. Whenever a person enters into a Particular area, his presence will be detected by the IR Sensor and it will send this data to the controller itself. Controller after receiving this information from a particular sensor, it will send a signal to the relay, then after that the appliance will turn on/off due to presence /absence of person.

Keywords: RFID's, IR sensors, Arduino uno, Servo motor, lcd panel 16x2, relays.

I. INTRODUCTION

RFID, Radio Frequency Identification is a basic and inexpensive technology that allows wireless data transmission. This technology has not yet been widely used in the industry due to the lack of establishment among pre-production companies. RFID technology is more efficient and secure compared to other networks. With RFID, automatic wireless identification takes the form of something: an object, a place, or a person marked with a unique identification code contained in the RFID tag, affixed to it or embedded in something. RFID is not a single product but a comprehensive program, a standard RFID program includes three basic components: an RFID tag (transponder), a reader (transceiver) and a back-end application system (or website), which requires computer network support. Software is used to manage, trade, operate and maintain records of various users. The digital door lock system is also operated and controlled by an RFID reader that authenticates and authenticates the user and automatically opens the door. It also maintains a user login and login record. It is very important to verify the user before entering a secure environment and RFID provides this solution. The system allows the user to enter and exit under fast, secure and easy conditions. The program includes an open-door lock system where the user puts his tag with the reader and user information matched to information already stored on the website. In this study we use RFID technology to provide a secure location access solution while maintaining a user record. We have used the rfid artifact here. Passive RFID models have no battery and gain performance on the reader. The major advantages of a passive rfid is that they are efficient and small in size.

II. METHODOLOGY

In this study, we proposed a security system consisting of a door lock system that uses a rfid type that is performed. The system is implemented in three spaces using a central data system. Secure space located in the same or different part of the premises. The program uses hardware and software. Hardware components are RFID reader, tags, Arduino, Relays, servo motor and connecting cords, IR sensors, 16x2 (lcd) etc.

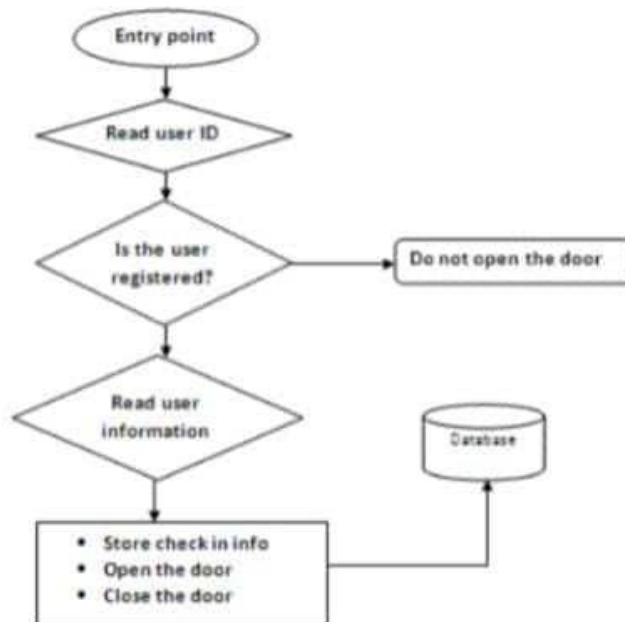


Fig 1: RFID flow chart (Phase-1)

The ATMEGA328p microcontroller is now used with a double-guided guest counter, controlling the light of the room and counting the number of people entering and leaving the room. When a person enters a room then one counter is raised by one lamp and one lamp in the room will be lit and when people leave the room where the counter is reduced by one. The total number of people present inside the room is also displayed on the LCD display. IR sensors and microcontroller do most of the work. IR sensors detect presence and the microcontroller detects signals generated by the presence from the sensors. The received signal is used with a program stored on the Microcontroller ROM. The purpose of this is to create an automatic control of the controller to calculate the number of people entering a particular room and illuminate the room.

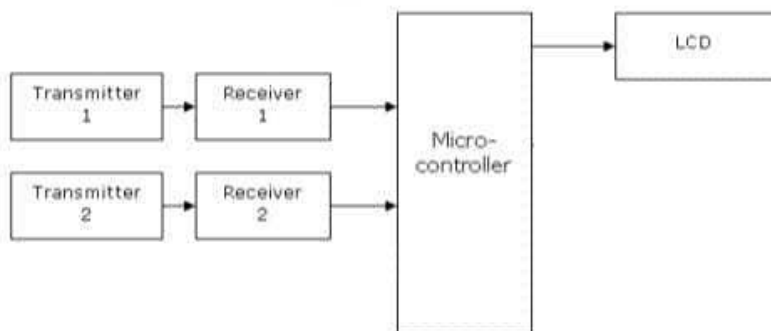


Fig 2: Flow chart of Digit Counter(Phase-2)

Methodology and Analysis

The program consists of a hardware module, Arduino Uno and a program called Arduino IDE. The application is called Arduino IDE which is the main application of Arduino and the is used to write codes. Hardware module are RFID marker, as well as RFID reader, display unit, Arduino uno, servo motor, proximity sensor, relay switch, and power supply unit. The RFID marker returns the information contained in the marker as it reaches a distance of a few millimeters from the reader, after receiving the marking information, the system generates a corresponding port control signal that controls the opening and closing of the door with a servo motor. When the door is opened, the door sensor will hear and activate the relay switch to open like a magnetic switch, and a message will immediately be sent to the user stating "The door is currently open". If the user exceeds the proximity sensor it will calculate the number of people logged in and will change the network connection. The power supply provides the voltage and still needed to operate the system effectively. This supply is pressed to a 12V DC power source and controlled before being fed into the system. The components used are:

- **Relay:** We use a 12-volt relay. The relay driver circuit is used to open the relay. Using this transfer user can control any AC or DC device.
- **Buzzer:** We use a piezoelectric buzzer. This is a warning / indication that an invalid attempt is being made to gain access to the system.
- **DC motor:** Will be used to display the door display or gate opening.
- **Servo motor:** Servo motor is widely used in high-tech devices in the industrial system as automated technology. It is an independent electrical device that surrounds parts of the machine with high efficiency and high accuracy. The output shaft of this motor can be rotated at a certain angle. Servo motors are widely used in home electronics, toys, cars, planes, etc.
- **Proximity Sensor:** Proximity Sensor is used to detect objects and obstacles before sensing. The sensor constantly transmits infrared light and when any object is approached, it detects the sensor by monitoring the light emanating from the object. It can be used on robots to avoid obstacles, automatic doors, parking aid equipment or security alarm systems.
- **LCD Display:** 16 by 2 Liquid Crystal Display (LCD) will be used for this project. Displays 2 rows each containing 16 characters. The LCD display has 16 numbers of processor working pins. RS is a line of instruction or data selection. This PIN is kept up or down by the microcontroller to display command line or data bytes on the db0-db7 data bus. A special feature of this LCD module allows reading of data bytes stored in RAM.

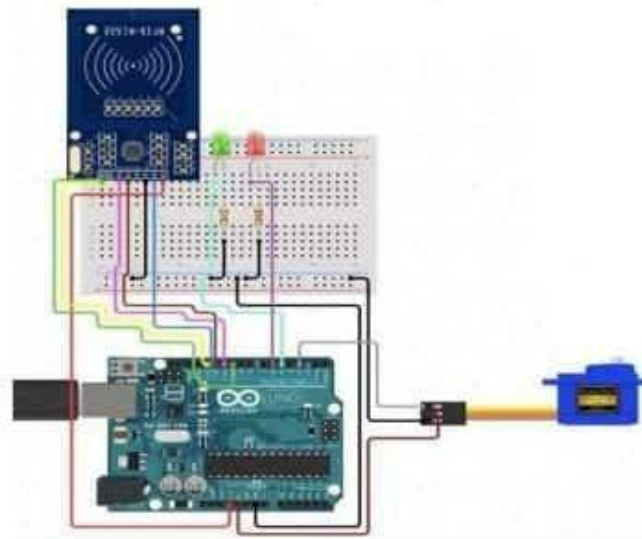


Figure 3: Circuit Diagram For Phase-1.

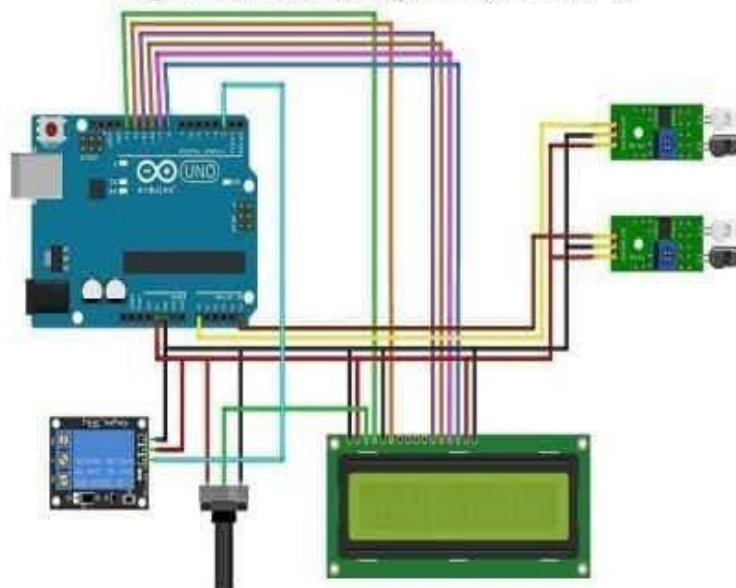


Figure 4: Circuit Diagram for Phase-2.

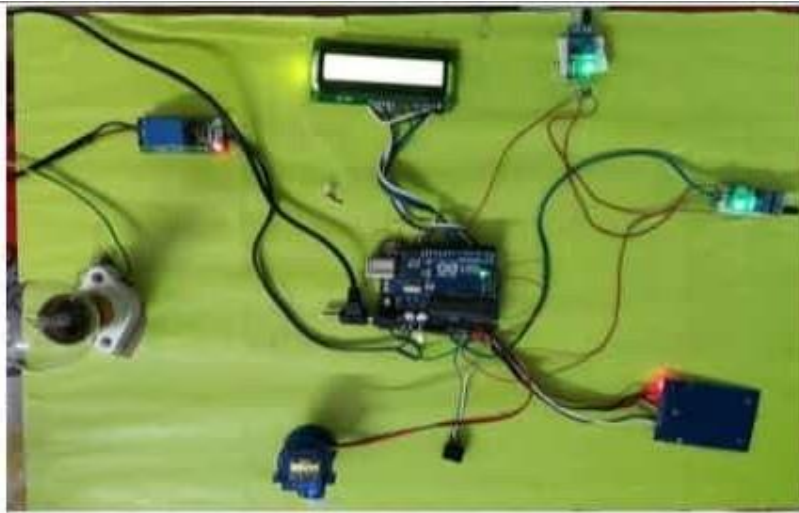


Figure 5: Project Model

III. RESULTS AND DISCUSSIONS

The connections of the RFID reader, the LCD, the servo motor, the proximity sensor, the relay switch, and power supply to the Arduino uno were done, and then checked for consistency. After running the Arduino code successfully. Fig 5 and 6 show, the flow chart of the system phases simultaneously, Fig 7 and Fig 8. The circuit diagram of the system, Fig3.3. The working model of the system, the instruction was displayed on the LCD screen, it means the system is prepared to read the RFID tag. After scanning the RFID master tag, some of the RFID tags were added. One of the tags was brought to about 5cm in front of the reader, a response "Access Granted" was displayed on the LCD and the servo motor opened the door, and the door was closed after 5 seconds. After that when the user crosses the proximity sensors the connected equipment's lightens up and when everyone exits the room and count becomes zero lights switches off.



Figure 6: RFID switches servo motor.



Figure 7: When Person enters the door.



Figure 8: Equipment Connected switches when Count+1.

IV. CONCLUSIONS

In this project, we have used RFIDs as a base of the door lock system, which on triggering will automatically switches the servo motor and the "Door is Opened with ID=" Someone" will be displayed on the lcd panel. After that, when the user triggers the proximity sensors the counting starts, which can be seen the lcd panel. Which will switch the relay and an electrical bulb will glow. Now when the number of persons exits the room reaches zero, the count will be display "Nobody in the Room", and all lights will be switched off.

V. REFERENCES

- [1] Radio Frequency Identification: Applications and Implications for Consumers, A Workshop Report from the Staff of the Federal Trade Commission, March 2005.
- [2] Research Gate, International Journal of Computer Applications 5(11) DOI:10.5120/957-1334.
- [3] Project Hub, Arduino Code.
- [4] Computer Engineering and Intelligent Systems, ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online), Vol.7, No.2, 2016.

B.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);
  }
}

```

```

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 : ");
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);
}

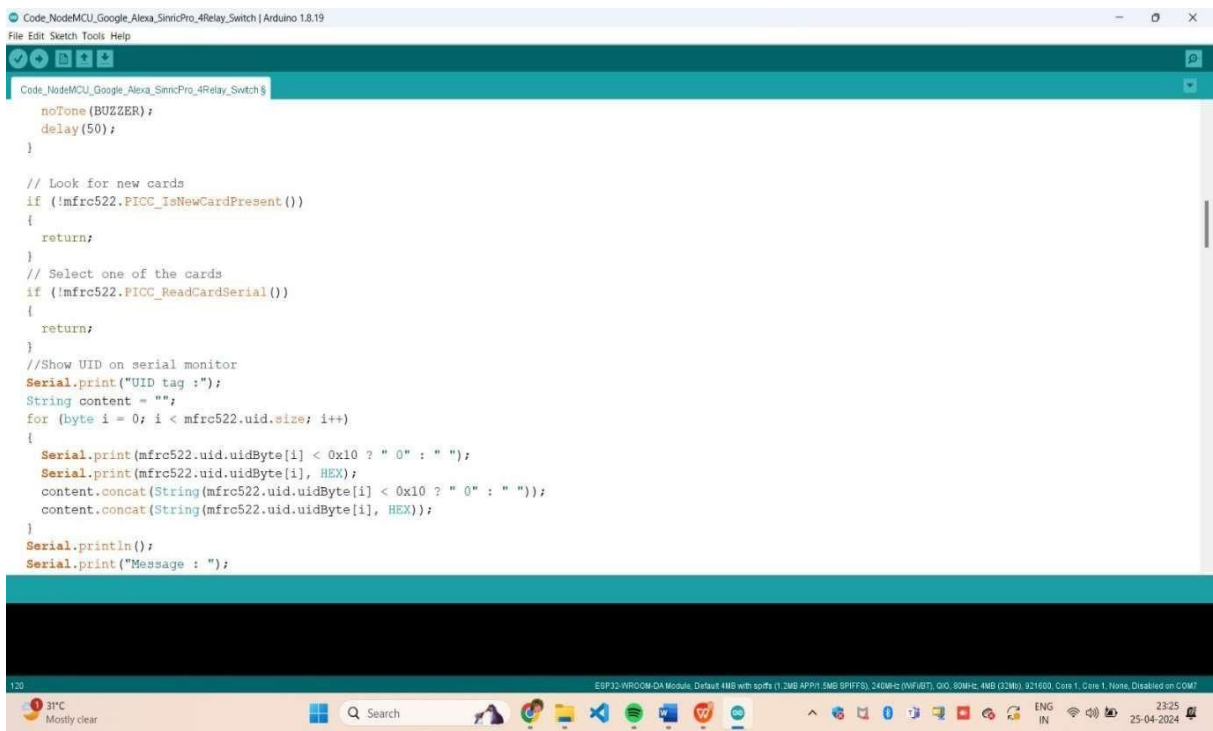
else
{

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

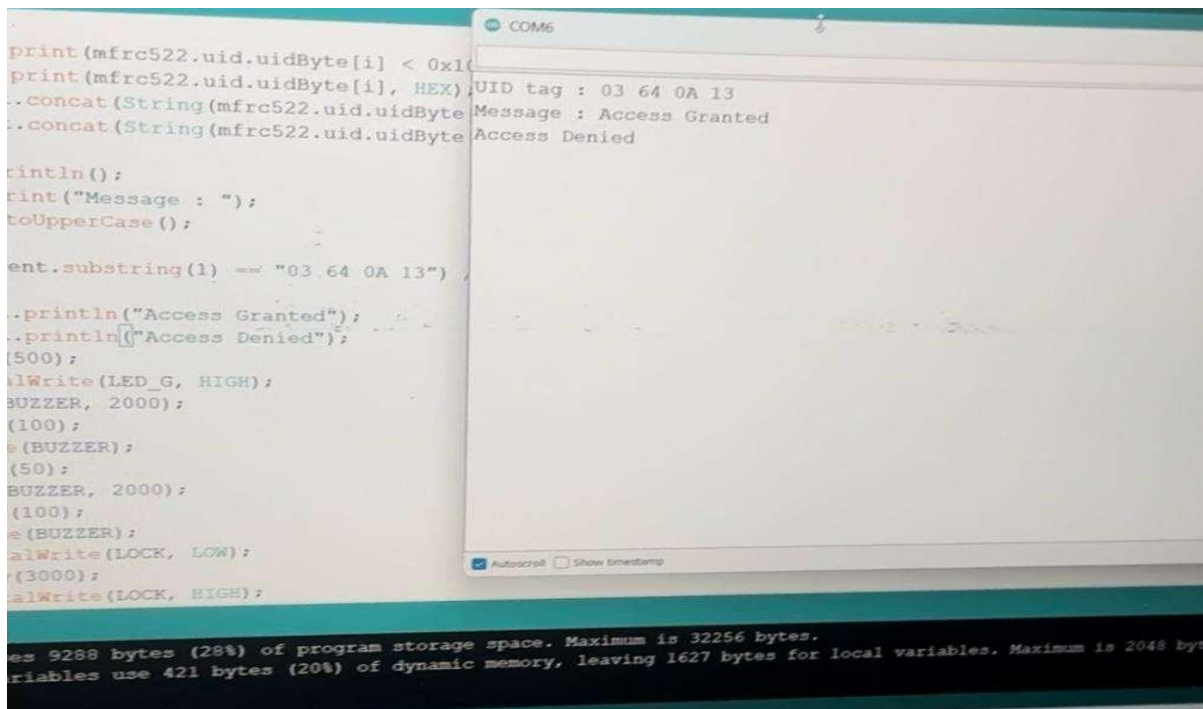
```

```
    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);  
}  
}
```

C.OUTPUT



C.1.Arduino Snapshot



C.2.Execution

