

# **HIGH SECURITY DOOR LOCK SYSTEM**

*A Project Report*

*Submitted to the APJ Abdul Kalam Technological University*

*in partial fulfillment of requirements for the award of degree*

***Bachelor of Technology***

*in*

***Electronics and Communication Engineering***

*by*

**Sai Krishnan R (TRV20EC049)**

**Vinayak M (TRV20EC061)**

**S Karthikeyan (TRV20EC055)**

**Sharika Reghunath (TRV20EC052)**



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

**Government Engineering College Barton Hill**

**Trivandrum, KERALA**

**June 2023**

**DEPT. OF ELECTRONICS & COMMUNICATION ENGINEERING**

**Government Engineering College Barton Hill TRIVANDRUM**

**2023-24**



**CERTIFICATE**

This is to certify that the report entitled **HIGH SECURITY DOOR LOCK SYSTEM** submitted by **Sai Krishnan R** (TRV20EC049), **Vinayak M** (TRV20EC061), **S Karthikeyan** (TRV20EC055), **Sharika Reghunath** (TRV20EC052) to the APJ Abdul Kalam Technological University in partial fulfillment of the B.Tech. degree in Electronics and Communication Engineering is a bonafide record of the seminar work carried out by him under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

**Project Guide**

Prof. Jacob Mathew  
Assistant Professor  
Dept. of ECE, GECBH

**Project Coordinator**

Prof. Aparna S Thampy  
Assistant Professor  
Dept. of ECE, GECBH

**Project Coordinator**

Prof. Smitha S  
Assistant Professor  
Dept. of ECE, GECBH

**Head of Department:**

Dr Hari R  
Professor and HoD  
Dept. of ECE, GECBH

GEC Barton Hill, Trivandrum

**Date: 03-08-2023**

# Abstract

The RFID-based door lock system with multiple security measures offers a higher level of protection compared to traditional locks. It consists of an RFID reader placed at the door and a unique RFID card assigned to each individual. When a person approaches the door, they need to present their RFID card to the reader for identification. Once the card is successfully read by the reader, the second authentication process is activated. Each RFID tag corresponds to a unique PIN stored in a database. The person entering the room must enter their corresponding PIN for further verification. This dual authentication mechanism significantly enhances security, as it requires both the RFID card and the associated PIN for access. Moreover, the system includes a web application acting as a master lock, which grants full control over the system. This means that authorized personnel can completely shut down the system through the web application, preventing any unauthorized access to the room. The advantage of this multiple authentication RFID-based door lock system lies in its ability to deter malpractices, such as identity theft. By combining the unique RFID card and the corresponding PIN, the system ensures that only authorized individuals with both components can gain entry, providing a robust and reliable security solution.

# Acknowledgement

We take this opportunity to express my deepest sense of gratitude and sincere thanks to everyone who helped us to complete this work successfully. We express my sincere thanks to **Dr Hari R**, Head of Department, Electronics and Communication Engineering, Government Engineering College Barton Hill Trivandrum for providing me with all the necessary facilities and support.

We would like to express my sincere gratitude to **Prof Aparna S Thampy** and **Prof Smitha S**, department of Electronics and Communication Engineering, Government Engineering College Barton Hill Trivandrum for their support and co-operation.

We would like to place on record our sincere gratitude to our project guide **Prof Jacob Mathew**, Assistant Professor, Electronics and Communication Engineering, Government Engineering College Barton Hill for the guidance and mentorship throughout the course.

Finally, We thank our family, and friends who contributed to the successful fulfillment of this project work.

**Sai Krishnan R**

**Vinayak M**

**S Karthikeyan**

**Sharika Reghunath**

# Contents

<b>Acknowledgement</b>	<b>ii</b>
<b>List of Figures</b>	<b>vi</b>
<b>1 Introduction</b>	<b>1</b>
<b>2 Literature Review</b>	<b>4</b>
2.1 RFID Based Door Lock . . . . .	4
2.2 PIN Based Door Lock . . . . .	4
2.3 Fingerprint Based Door Lock . . . . .	5
2.4 OTP Based Door Lock . . . . .	5
2.5 Summary . . . . .	5
<b>3 Problem Statement</b>	<b>6</b>
3.1 Proposed System . . . . .	7
3.2 Objective . . . . .	8
3.3 Existing Solutions . . . . .	8
<b>4 System Design</b>	<b>12</b>
4.1 Components Description . . . . .	12
4.1.1 ESP32 DEV KIT V1 . . . . .	12
4.1.2 RC522 Reader Writer Module . . . . .	14
4.1.3 RFID TAG . . . . .	17
4.1.4 KEYPAD . . . . .	18
4.1.5 16 x 2 LCD DISPLAY . . . . .	19
4.1.6 I2C MODULE . . . . .	21

4.1.7	Relay Module . . . . .	22
4.1.8	Solenoid Lock . . . . .	23
4.1.9	Dot PCB Board . . . . .	25
4.1.10	Jumper Wires . . . . .	26
4.1.11	12V DC Adapter . . . . .	26
4.1.12	Header Pins . . . . .	27
4.1.13	Single Strand Wire . . . . .	28
4.1.14	Push Button . . . . .	28
4.1.15	7805 Voltage Regulator IC . . . . .	29
4.1.16	Capacitors . . . . .	30
4.2	System Architecture . . . . .	32
<b>5</b>	<b>Implementation and working</b>	<b>34</b>
5.1	Hardware . . . . .	34
5.2	Software . . . . .	36
5.2.1	Algorithm . . . . .	36
5.2.2	Flowchart . . . . .	38
5.2.3	Library Explanation . . . . .	38
5.2.4	Real Time Data Base . . . . .	41
5.2.5	Web Application . . . . .	42
5.2.6	Hashing using SHA-256 . . . . .	43
5.2.7	Network Time Protocol . . . . .	45
<b>6</b>	<b>Experiment and Results</b>	<b>46</b>
6.1	The scanned tag is valid and PIN entered is correct . . . . .	46
6.2	The scanned tag is valid and PIN entered is incorrect . . . . .	47
6.3	The scanned tag is invalid . . . . .	47
6.4	The system is in the lock state . . . . .	47
<b>7</b>	<b>Conclusion and Future Scope</b>	<b>49</b>
7.1	Conclusion . . . . .	49
7.2	Future Scope . . . . .	50



# List of Figures

3.1	Proposed System . . . . .	8
4.1	ESP32 DEV KIT V1 . . . . .	14
4.2	RC522 RFID Module . . . . .	16
4.3	RFID Tags . . . . .	18
4.4	4x4 Matrix Membrane Keypad . . . . .	19
4.5	LCD Display . . . . .	21
4.6	I2C Module . . . . .	22
4.7	Relay Module . . . . .	23
4.8	Solenoid Lock . . . . .	25
4.9	Dot PCB Board . . . . .	25
4.10	Jumper Wires . . . . .	26
4.11	12 V Adapter . . . . .	27
4.12	Header Pins . . . . .	28
4.13	Single strand wire . . . . .	28
4.14	Push Button . . . . .	29
4.15	LM7805 IC . . . . .	30
4.16	Capacitors . . . . .	31
4.17	Block Diagram . . . . .	32
5.1	Circuit Diagram . . . . .	35
5.2	Regulator Circuit . . . . .	35
5.4	Flowchart . . . . .	38
5.5	Real Time Database . . . . .	42
5.6	Web Application Page . . . . .	42



5.7	Web Login Page . . . . .	43
5.8	Hashing using SHA-256 . . . . .	44
6.1	Access Granted . . . . .	46
6.2	Access Denied . . . . .	47
6.3	Photograph of Circuit . . . . .	48
6.4	Hardware Photograph . . . . .	48

# Chapter 1

## Introduction

In today's rapidly advancing world, ensuring security and access control to buildings and restricted areas has become a paramount concern. Traditional key-based locks are prone to issues such as loss, theft, duplication, and inconvenience. Most of the existing systems just require an RFID card to access secured areas in an organization, this technique compromises the security. A unauthorized person could get hold of the RFID card and enter the restricted areas and could try to damage or steal proprietary information. An RFID based system can also be hacked easily, the hacker just needs a reader that reads the same frequency as the tag. To address these challenges, an innovative solution has emerged: an RFID-based door lock system with multiple security.

The RFID (Radio Frequency Identification) technology is a wireless communication system that uses electromagnetic fields to automatically identify and track objects equipped with RFID tags. It has found widespread use in various industries due to its reliability, ease of implementation, and enhanced security features. Leveraging this technology, our project aims to develop an efficient door lock system that provides a secure and convenient access control mechanism. The core functionality of our RFID-based door lock system revolves around the use of RFID cards or tags. Each authorized user will be issued a unique RFID card or tag that contains an embedded microchip. This microchip stores a unique identification number linked to the user's access privileges. Additionally, the system incorporates a unique PIN (Personal Identification

Number) for each user to provide an added layer of security.

When an authorized user approaches the RFID-based door lock, they need to present their RFID card or tag within proximity to the lock's reader. The reader then wirelessly communicates with the microchip on the card, verifying the user's identity and access privileges. Upon successful verification, the user will be prompted to enter their unique PIN on a keypad integrated into the lock system. The unique PIN acts as an additional authentication factor, ensuring that only authorized users with the correct RFID card or tag and the corresponding PIN can gain access. Once the correct RFID card and PIN combination are entered, the door lock system will grant access by unlocking the door, allowing the user to enter the secured area. The PIN along with all the details of the person is stored in an RTDB in Firebase which is authenticated with a username and password. The PIN is not stored as it is in the database, it is encrypted using the SHA-256 algorithm and stored in the database, this enhances the security, and the PIN cannot be misused under any circumstances.

Moreover, our RFID-based door lock system offers several advantages over traditional key-based locks. Firstly, the risk of key loss or theft is eliminated since the system relies on RFID cards or tags, which can be easily deactivated or reissued if needed. Secondly, the unique PIN adds an extra layer of security, reducing the likelihood of unauthorized access even if an RFID card or tag is stolen. Lastly, the convenience of the system is enhanced as users no longer need to carry a physical key but can simply present their RFID card or tag and enter their PIN.

To multiply the security, we have also introduced a web application, which acts as the master lock system. The person with access to the web application can completely shut down the system which restricts access via RFID too. The application is secured with a username and password which is linked with the authentication of the Firebase hence the application can only be accessed by the person who has access to the real-time database in Firebase.

In conclusion, the RFID-based door lock system with multiple security provides a

secure, efficient, and convenient access control solution for buildings and restricted areas. By leveraging RFID technology and incorporating a unique PIN for each user, our project aims to enhance security while improving the overall user experience. This project has the potential to revolutionize access control systems and contribute to creating safer environments in various domains, including residential, commercial, and industrial sectors.

# **Chapter 2**

## **Literature Review**

This literature review aims to provide insight into the existing door lock systems, although there are a lot of different systems we will be mainly looking into four types. By reading this review everyone could get an insight on why the proposed solution in this project was put forward. The information has been collected from various sources and websites of manufacturers of these door lock systems.

### **2.1 RFID Based Door Lock**

RFID (Radio Frequency Identification) door lock systems utilize RFID technology to control access to doors. These systems typically consist of RFID tags or cards that contain unique identification information and RFID readers installed near the doors. When a person with a valid RFID tag approaches the door, the reader wirelessly communicates with the tag, authenticates its identity, and grants or denies access accordingly. RFID door lock systems offer several advantages, including convenience, improved security, and the ability to track and record access events. They are commonly used in various settings, such as offices, hotels, hospitals, and residential buildings, to provide efficient and secure access control.

### **2.2 PIN Based Door Lock**

PIN-based door lock systems are a type of access control system that relies on personal identification numbers (PINs) for granting or denying access to doors. In this system,

users are assigned unique PINs that they enter on a keypad or touchscreen interface to gain entry. The PIN is compared against a stored database of authorized codes, and if the entered code matches an authorized PIN, the door is unlocked.

## **2.3 Fingerprint Based Door Lock**

Fingerprint-based door lock systems employ biometric technology to grant access to doors based on an individual's unique fingerprint pattern. These systems capture and store fingerprint images of authorized users in a database. When a person places their finger on the designated sensor, the system compares the captured fingerprint with the stored templates to authenticate the identity. If the fingerprint match is successful, the door is unlocked.

## **2.4 OTP Based Door Lock**

OTP (One-Time Password) based door lock systems utilize a dynamic password mechanism for access control. In this system, users are provided with a unique one-time password that expires after a single use or after a predefined time period. The OTP is typically generated and transmitted through a mobile app, SMS, or email. To unlock the door, users must enter the valid OTP on a keypad or input device.

## **2.5 Summary**

By studying these solutions and finding flaws in them we could develop a more robust and secure solution. The field of RFID door lock systems with unique PINs presents several areas for future research and development. Advancements in RFID technology, such as the use of more secure and tamper-resistant tags, can further enhance the security of these systems. Additionally, exploring the integration of other biometric authentication methods, such as fingerprint or facial recognition, could offer even stronger security measures.

# Chapter 3

## Problem Statement

The current state of door lock systems raises concerns about their effectiveness and vulnerability to unauthorized access in various establishments such as offices and banks. Common door lock systems, including RFID (Radio Frequency Identification) based locks, face several vulnerabilities that can be exploited by thieves and unauthorized individuals. One significant vulnerability is the ease with which RFID cards can be cloned. Attackers can intercept the radio signals between the RFID card and the reader, capture the card's information, and create duplicate cards for illicit access. This cloning process requires inexpensive equipment and basic technical knowledge, making it a serious concern.

Another issue is the weak or non-existent encryption used in many RFID door locks. This lack of encryption makes it simpler for attackers to intercept and decode the communication between the card and the reader. Consequently, the card's data can be easily stolen, enabling attackers to replicate or forge the card. Furthermore, some RFID door locks lack proper authentication mechanisms, relying solely on the presence of the card for access. This flaw makes them vulnerable to spoofing attacks, where unauthorized devices or fake cards can deceive the system into granting access.

### **3.1 Proposed System**

The RFID-based door lock system is designed to provide secure access control by combining RFID tags, unique PINs, a real-time database, and a web application. Each RFID tag is associated with a specific individual and has a corresponding unique PIN. These details, including the person's information, are stored in a real-time database.

The system operates by reading the RFID tag when it comes into proximity with the door lock. The unique PIN associated with the tag is then validated against the stored information in the real-time database. If the PIN matches, access is granted to the individual.

Additionally, a web application serves as a master lock, allowing authorized administrators to shut down the entire system if necessary. This web application provides an interface to manage the RFID tags, PINs, and person details stored in the database. By accessing the web application, administrators can disable or enable specific RFID tags, change PINs, or even deactivate the entire system temporarily.

By combining RFID technology, unique PINs, a real-time database, and a web application, this system ensures secure access control while providing administrators with the ability to manage and control the system effectively.



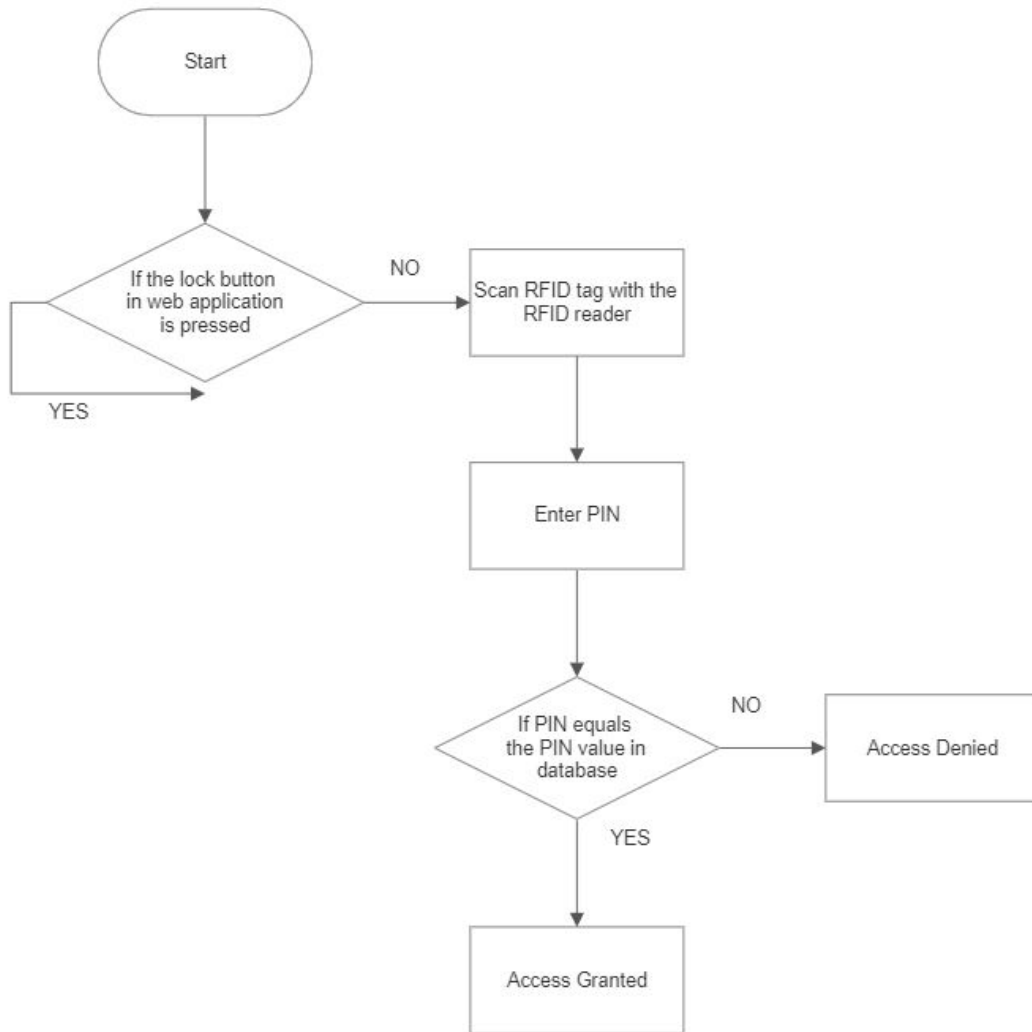


Figure 3.1: Proposed System

## 3.2 Objective

1. To design and implement a high-security door lock system with multiple layers of security.
2. To ensure robust resistance against RFID card hacking and unauthorized access.
3. To implement a low-budget high-security door lock system.

## 3.3 Existing Solutions

1. **RFID based door lock systems:-** An RFID-based lock is a type of electronic lock that utilizes Radio Frequency Identification (RFID) technology for access

control and security purposes. RFID enables wireless communication between a lock and RFID tags or cards that contain embedded microchips and antennas.

Here's how an RFID-based lock typically works:

1. **Lock Configuration:** The RFID lock is initially programmed or configured to recognize specific RFID tags or cards that are authorized for access. Each RFID tag or card is assigned a unique identification code.
2. **RFID Tags or Cards:** Authorized users are provided with RFID tags or cards that they need to carry or present to the lock for access. These tags or cards contain an embedded RFID chip and antenna.
3. **Proximity Verification:** To unlock the RFID-based lock, an authorized user presents their RFID tag or card within proximity to the lock's RFID reader. The RFID reader emits a radio frequency signal that powers the RFID tag or card and enables communication.
4. **Authentication and Authorization:** The RFID reader reads the unique identification code from the RFID tag or card. It then compares this code with the authorized codes stored in its memory. If a match is found, the lock proceeds to unlock.
5. **Unlocking:** Upon successful authentication, the RFID-based lock disengages, allowing physical access to the secured area. The lock may incorporate various unlocking mechanisms such as an electronically controlled latch, motorized bolt, or other mechanisms depending on its design.

RFID-based locks offer several benefits, including convenience, flexibility, and security. Users can quickly access the lock by presenting their RFID tag or card, eliminating the need for physical keys or PINs. The lock can also be programmed to recognize multiple authorized RFID tags or cards, enabling access for multiple users.

Additionally, RFID-based locks provide an audit trail of access events, as each entry can be recorded with the associated RFID tag or card identification. This can be useful for security monitoring and tracking access history.

It's important to note that RFID-based locks typically operate within a limited

range, usually a few centimeters to a few meters. This range ensures that the lock only responds to RFID tags or cards that are in close proximity, enhancing security by preventing unauthorized access from a distance.

2. **Pin Based Lock** A pin-based lock, also known as a combination lock or a numeric lock, is a type of lock that uses a series of digits or numbers to unlock it. Instead of using a physical key, the lock is opened by correctly inputting the predefined numeric code.

Here's how a typical pin-based lock works:

1. **Dialing Mechanism:** The lock consists of a dial or a keypad that has numbers (usually from 0 to 9) printed or embossed on it. It may also include additional symbols or buttons for specific functions like "Enter" or "Clear."
2. **Predefined Code:** The lock has a predetermined numeric code, often set by the lock owner. This code serves as the key to open the lock.
3. **Entering the Code:** To unlock the lock, the user needs to input the correct numeric code. This is done by rotating the dial or pressing the keypad buttons corresponding to the numbers in the correct sequence.
4. **Alignment and Verification:** As the user inputs the code, the lock's internal mechanisms align based on the code sequence. Once the correct code is entered, the lock's internal components (such as pins or tumblers) align in a specific pattern, allowing the lock to disengage.
5. **Unlocking:** When the correct code is entered and the internal components are correctly aligned, the lock can be opened by turning the dial or operating a separate latch or lever mechanism.

Pin-based locks are commonly used in various applications, such as lockers, safes, briefcases, luggage, and even some doors. They offer a convenient and keyless method of securing items or spaces, provided that the user knows the correct numeric code. It's important to choose a strong and unique code to ensure the security of the lock.

3. **NFC based door lock system:-** An NFC-based lock is a type of electronic lock that utilizes Near Field Communication (NFC) technology for unlocking and

securing access. NFC is a short-range wireless communication technology that enables devices to exchange data over a close proximity.

Here's how an NFC-based lock typically works:

1. **Lock Configuration:** The NFC lock is initially configured by assigning access privileges and permissions to specific NFC devices or tags. These NFC devices or tags are programmed with unique identification information.
2. **NFC-enabled Devices or Tags:** Users who are authorized to access the lock are given NFC-enabled devices, such as smartphones, keycards, or dedicated NFC tags. These devices have an embedded NFC chip that allows them to communicate with the lock.
3. **Proximity Verification:** To unlock the NFC-based lock, the user brings their NFC-enabled device or tag within close proximity to the lock. The lock's NFC reader detects the presence of the NFC signal and initiates communication.
4. **Authentication and Authorization:** The NFC reader verifies the authenticity of the NFC device or tag by checking its unique identification information. If the device or tag is recognized and authorized, the lock proceeds to unlock.
5. **Unlocking:** Upon successful authentication, the NFC-based lock disengages, allowing physical access to the secured area. This can be achieved through an electronically controlled latch, motorized mechanism, or other unlocking mechanisms depending on the lock design.

NFC-based locks offer several advantages, including convenience, ease of use, and enhanced security. They eliminate the need for physical keys, as users can simply tap or bring their authorized NFC device close to the lock for access. Additionally, access permissions can be easily managed and updated by reprogramming or reconfiguring the NFC devices or tags.

It's worth noting that NFC-based locks require both the lock and the NFC-enabled device or tag to be within close proximity for communication, typically within a few centimeters. This proximity requirement ensures that the lock cannot be unlocked from a distance, enhancing security.

# Chapter 4

## System Design

The components description and the system architecture is explained below:

### 4.1 Components Description

#### 4.1.1 ESP32 DEV KIT V1

The ESP32 is a series of low-cost and low-power systems on a Chip (SoC) microcontrollers that include Wi-Fi and Bluetooth wireless capabilities and dual-core processors. It is a low-cost microcontroller that consumes very less power and the processing speed is high when compared to ESP8266.

##### **Pinout**

The ESP32 chip comes with 48 pins with multiple functions. Not all pins are exposed in all ESP32 development boards, and some pins should not be used. Out of the 48 pins only 36 are exposed GPIOs which can be used for connecting peripherals.

- **Power Pins:** The ESP32 board comes with 3.3V, Ground and Vin Pin which can be used to power the board.
- **GPIO Pins:** The ESP32 peripherals include:
  - 18 Analog-to-Digital Converter (ADC) channels
  - 3 SPI interfaces

- 3 UART interfaces
  - 2 I2C interfaces
  - 16 PWM output channels
  - 2 Digital-to-Analog Converters (DAC)
  - 2 I2S interfaces
  - 10 Capacitive sensing GPIOs The ESP32 is a series of low-cost and low-power System on a Chip (SoC) microcontrollers that include Wi-Fi and Bluetooth wireless capabilities and dual-core processor. It is a low cost microcontroller which consumes very less power and the processing speed is high when compared to ESP8266.
- GPIOs 34 to 39 are GPIOs – input only pins. These pins don't have internal pull-up or pull-down resistors. They can't be used as outputs, so use these pins only as inputs.
  - GPIO 6 to GPIO 11 pins are connected to the integrated SPI flash on the ESP-WROOM-32 chip and are not recommended for other uses

The ESP32 has 10 internal capacitive touch sensors. These can sense variations in anything that holds an electrical charge, like the human skin. So they can detect variations induced when touching the GPIOs with a finger. These pins can be easily integrated into capacitive pads and replace mechanical buttons.

The ESP32 LED PWM controller has 16 independent channels that can be configured to generate PWM signals with different properties. All pins that can act as outputs can be used as PWM pins (GPIOs 34 to 39 can't generate PWM).

To set a PWM signal, you need to define these parameters in the code:

- Signal's frequency
- Duty cycle
- PWM channel

- GPIO where you want to output the signal

Some GPIOs change their state to HIGH or output PWM signals at boot or reset. This means that if you have outputs connected to these GPIOs you may get unexpected results when the ESP32 resets or boots.

- GPIO 1
- GPIO 3
- GPIO 5
- GPIO 6 to GPIO 11 (connected to the ESP32 integrated SPI flash memory – not recommended to use).
- GPIO 14
- GPIO 15

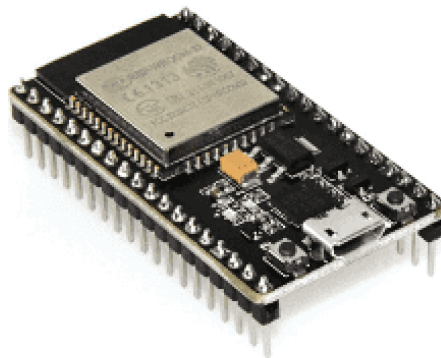


Figure 4.1: ESP32 DEV KIT V1

#### **4.1.2 RC522 Reader Writer Module**

An RFID or radio frequency identification system consists of two main components, a tag, and a reader. The reader consists of a radio frequency module and an antenna that generates a high-frequency electromagnetic field. Whereas the tag is usually a passive device (it does not have a battery). It consists of a microchip that stores and processes information, and an antenna for receiving and transmitting a signal. When the tag is

brought close to the reader, the reader generates an electromagnetic field. This causes electrons to move through the tag's antenna and subsequently powers the chip. The chip then responds by sending its stored information back to the reader in the form of another radio signal. This is called backscatter. The reader detects and interprets this backscatter and sends the data to a computer or microcontroller.

The RC522 RFID reader module is designed to create a 13.56MHz electromagnetic field and communicate with RFID tags (ISO 14443A standard tags). The reader can communicate with a microcontroller over a 4-pin SPI with a maximum data rate of 10 Mbps. It also supports communication over I2C and UART protocols. The RC522 RFID module can be programmed to generate an interrupt, allowing the module to alert us when a tag approaches it, instead of constantly asking the module "Is there a card nearby?"

The module's operating voltage ranges from 2.5 to 3.3V, but the good news is that the logic pins are 5-volt tolerant, so we can easily connect it to an Arduino or any 5V logic microcontroller without using a logic-level converter.

### **Pinout**

- **VCC** supplies power to the module. This can be anywhere from 2.5 to 3.3 volts.
- **RST** is an input for reset and power-down. When this pin goes low the module enters power-down mode. In which the oscillator is turned off and the input pins are disconnected from the outside world. Whereas the module is reset on the rising edge of the signal.
- **GND** is the ground pin
- **IRQ** is an interrupt pin that alerts the microcontroller when an RFID tag is in the vicinity.
- **MISO (Master In Slave Out) / SCL / Tx** pin acts as master-in-slave-out when the SPI interface is enabled, as a serial clock when the I2C interface is enabled, and as serial data output when the UART interface is enabled.



- **MOSI (Master Out Slave In)** is the SPI input to the RC522 module.
- **SCK (Serial Clock)** accepts the clock pulses provided by the SPI bus master.
- **SS / SDA / Rx** pin acts as a signal input when the SPI interface is enabled, as serial data when the I2C interface is enabled, and as a serial data input when the UART interface is enabled. This pin is usually marked by encasing the pin in a square so that it can be used as a reference to identify other pins.

SPI is a synchronous communication protocol used to communicate with micro-controllers. One unique benefit of SPI is the fact that data can be transferred without interruption. Any number of bits can be sent or received in a continuous stream.

UART stands for Universal Asynchronous Receiver/Transmitter. Its main purpose is to transmit and receive serial data. UARTs transmit data asynchronously, which means there is no clock signal to synchronize the output of bits from the transmitting UART to the sampling of bits by the receiving UART.

I2C is a serial communication protocol, so data is transferred bit by bit along a single wire (the SDA line). Like SPI, I2C is synchronous, so the output of bits is synchronized to the sampling of bits by a clock signal shared between the master and the slave. The clock signal is always controlled by the master.



Figure 4.2: RC522 RFID Module

### **4.1.3 RFID TAG**

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. These radio waves transmit data from the tag to a reader, which then transmits the information to an RFID computer program. An RFID tag may also be called an RFID chip.

An RFID tag works by transmitting and receiving information via an antenna and a microchip — also sometimes called an integrated circuit or IC. The microchip on an RFID reader is written with whatever information the user wants.

#### **Types of RFID Tags**

- Battery-operated RFID tags contain an onboard battery as a power supply. Battery-operated RFID tags might also be called active RFID tags.
- Passive RFID tags are not battery-powered and instead work by using electromagnetic energy transmitted from an RFID reader.

Passive RFID tags use three main frequencies to transmit information: 125 – 134 KHz, also known as Low Frequency (LF), 13.56 MHz, also known as High Frequency (HF) and Near-Field Communication (NFC), and 865 – 960 MHz, also known as Ultra High Frequency (UHF). The frequency used affects the tag’s range.

When a passive RFID tag is scanned by a reader, the reader transmits energy to the tag which powers it enough for the chip and antenna to relay information back to the reader. The reader then transmits this information back to an RFID computer program for interpretation.

There are two main types of passive RFID tags: inlays and hard tags.

- Inlays
- Hard Tags

Active RFID tags use one of two main frequencies — either 433 MHz or 915 MHz — to transmit information. They contain three main parts, including a tag, antenna, and interrogator. The battery in an active RFID tag should supply enough power to last for 3-5 years. When it dies, the unit will need to be replaced, as the batteries are not currently replaceable. There are two main kinds of active RFID tags: beacons and transponders.



Figure 4.3: RFID Tags

#### **4.1.4 KEYPAD**

The 4×4 matrix keypad is an input device, usually used to provide input value in a project. It has 16 keys in total, which means it can provide 16 input values. It uses only 8 GPIO pins of a microcontroller. Underneath each key is a pushbutton, with one end connected to one row, and the other end connected to one column.

In order for the microcontroller to determine which button is pressed, it first needs to pull each of the four columns (pins 1-4) either low or high one at a time, and then poll the states of the four rows (pins 5-8). Depending on the states of the columns, the microcontroller can tell which button is pressed. For example, say your program pulls all four columns low and then pulls the first row high. It then reads the input states of each column, and reads pin 1 high. This means that a contact has been made between column 4 and row 1, so button ‘A’ has been pressed

A 4X4 keypad will have 8 terminals. In them four are rows of a matrix and four are

columns of a matrix. These 8 pins are driven out from 16 buttons present in the module. Those 16 alphanumeric digits on the module surface are the 16 buttons arranged in matrix formation 3

### Specifications

- Maximum Rating: 24 VDC, 30 mA
- Interface: 8-pin access to 4x4 matrix
- Operating temperature: 32 to 122 °F (0 to 50°C)
- Dimensions: Keypad, 2.7 x 3.0 in (6.9 x 7.6 cm)



Figure 4.4: 4x4 Matrix Membrane Keypad

### 4.1.5 16 x 2 LCD DISPLAY

The term LCD stands for liquid crystal display. It is one kind of electronic display module used in an extensive range of applications like various circuits devices like mobile phones, calculators, computers, TV sets, etc.

#### Pinout

- **PIN 1** (Ground/Source Pin): This is a GND pin of display, used to connect the GND terminal of the microcontroller unit or power source.
- **PIN 2** (VCC/Source Pin): This is the voltage supply pin of the display, used to connect the supply pin of the power source

- **PIN 3** (V0/VEE/Control Pin): This pin regulates the difference of the display, used to connect a changeable POT that can supply 0 to 5V
- **Pin4** (Register Select/Control Pin): This pin toggles among the command or data register, used to connect a microcontroller unit pin and obtains either 0 or 1 (0 = data mode, and 1 = command mode).
- **Pin5** (Read/Write/Control Pin): This pin toggles the display among the read or writes operation, and it is connected to a microcontroller unit pin to get either 0 or 1 (0 = Write Operation, and 1 = Read Operation).
- **Pin 6** (Enable/Control Pin): This pin should be held high to execute the Read/Write process, and it is connected to the microcontroller unit constantly held high.
- **Pins 7-14** (Data Pins): These pins are used to send data to the display. These pins are connected in two-wire modes like 4-wire mode and 8-wire mode. In 4-wire mode, only four pins are connected to the microcontroller unit like 0 to 3, whereas in 8-wire mode, 8-pins are connected to microcontroller units like 0 to 7.
- **Pin15** (+ve pin of the LED): This pin is connected to +5V
- **Pin 16** (-ve pin of the LED): This pin is connected to GND

The features of this LCD mainly include the following:

- The operating voltage of this LCD is 4.7V-5.3V.
- It includes two rows where each row can produce 16-characters.
- The utilization of current is 1mA with no backlight.
- Every character can be built with a 5×8 pixel box.
- The alphanumeric LCDs alphabets numbers.
- Is display can work on two modes like 4-bit 8-bit.
- These are obtainable in Blue Green Backlight.

- It displays a few custom generated characters

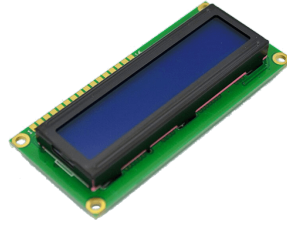


Figure 4.5: LCD Display

#### 4.1.6 I2C MODULE

Commercially available LCD display modules like 16x2 LCD display and 20x4 LCD display are great to be used with a microcontroller like Arduino, Raspberry Pi, PIC, etc. to display the data but a standard 16x2 LCD even when operating at 4-bit mode takes about 8 GPIO pins from the microcontroller to display information on it and in the projects where GPIO pins are at a premium, it is a lot. That is why we need a serial to parallel data adapter so that we can reduce the number of pins needed to drive the LCD display modules. This LCD I2C adapter module is designed to fit directly below the standard 16x2 LCD display. Then through this module, the LCD can communicate through I2C protocol which requires only 2 pins from the controller side and then uses the PCF8574 IC to receive data from I2C and display them on the LCD screen. It can be used to drive Robotics projects, 3D printers, Quadcopters, etc.

##### Specifications

- 5V power supply
- Serial I2C control of LCD display using PCF8574
- Backlight of the LCD display can be enabled or disabled via a jumper on the board
- Contrast of the LCD screen control via a potentiometer
- Can have 8 modules on a single I2C bus (change address via solder jumpers)

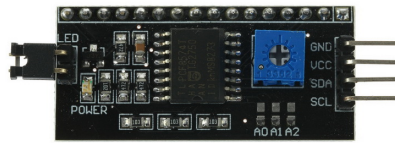


Figure 4.6: I2C Module

### 4.1.7 Relay Module

Relays are used to switch high power loads using a low power control signal, providing electrical isolation between the control circuit and the load. They are often used to control lights, motors, and other high-power devices, and can be controlled by a variety of signals, such as switches, sensors, or microcontrollers. Relays are also used to switch different loads independently, and to protect sensitive electronic components from high voltages and currents.

A 1-channel relay has a single switch or channel, which means it can only control one load or circuit at a time. This type of relay is typically used in simple applications where only one load needs to be switched, such as turning a single light on or off.

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.

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.

## Specifications

- Digital output controllab.
- Rated through-current: 10A (NO) 5A (NC)
- Control signal: TTL level
- Max. switching voltage 250VAC/30VDC
- Max. switching current 10A
- Size: 43mm x 17mm x 17mm

## Pinout

- **Pin 1** - Relay trigger - Input to activate the relay
- **Pin 2** - Ground
- **Pin 3** - VCC
- **Pin 4** - Normally open
- **Pin 5** - Common
- **Pin 6** - Normally closed

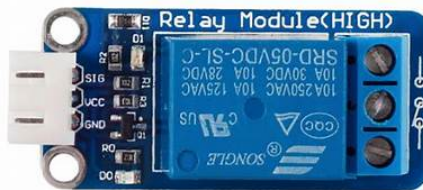


Figure 4.7: Relay Module

### 4.1.8 Solenoid Lock

Solenoids are basically electromagnets made of a big coil of copper wire with an armature (a slug of metal) in the middle. This DC 12V Solenoid lock is used for locking shell-machine, storage shelf, file cabinet, etc. This solenoid lock



features steady, durable, energy-saving, and has a long lifespan with an anti-theft and shockproof design. A 12v solenoid lock consists of a slug with a slanted cut and a good mounting bracket. Under normal conditions, it does not use any power. So the lock is active and can't open the door because the solenoid slug is in the way. When a 9-12v dc is applied to the solenoid lock, the slug pulls in. As a result, it doesn't stick out. Thus the doors can be opened.

The slug is pulled into the center of the coil when energized. Hence the solenoid is able to pull from one end. The slanted slug in the solenoid can be opened using head screws by rotating it 90, 180, or 270 degrees so that it matches the door you want to use it with. It is very important to check polarity while connecting the solenoid lock. The red wire should be connected to the positive and the Black wire to the negative. A power transistor and a diode are used in order to drive the solenoid lock.

The solenoid lock is basically a latch for electrical locking and unlocking. This power-on type enables unlocking only while the solenoid is powered on. Thus a door of this type is locked and not opened in case of power failure or wire disconnection, ensuring excellent safety.

### **Specification**

- Operating Voltage: 12V.
- Rated Current: 0.8 A.
- Power: 9.6 Watt
- Dimensions: 54 x 42 x 28 mm
- Draws 650mA at 12V, 500 mA at 9V when activated

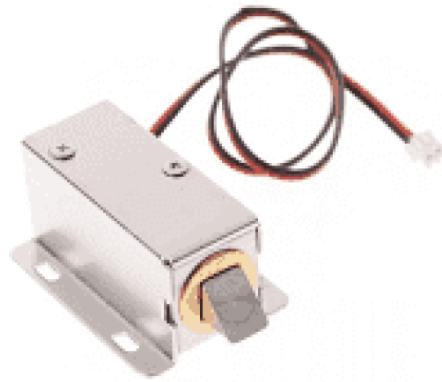


Figure 4.8: Solenoid Lock

#### 4.1.9 Dot PCB Board

Perfboard is a material for prototyping electronic circuits (also called DOT PCB). It is a thin, rigid sheet with holes pre-drilled at standard intervals across a grid, usually a square grid of 0.1 inches (2.54 mm) spacing. These holes are ringed by round or square copper pads, though bare boards are also available. Inexpensive perfboard may have pads on only one side of the board, while a better quality perfboard can have pads on both sides (plate-through holes). Since each pad is electrically isolated, the builder makes all connections with either wire wrap or miniature point to point wiring techniques. Discrete components are soldered to the prototype board such as resistors, capacitors, and integrated circuits. The substrate is typically made of paper laminated with phenolic resin (such as FR-2) or a fiberglass-reinforced epoxy laminate (FR-4).



Figure 4.9: Dot PCB Board

#### 4.1.10 Jumper Wires

A jump wire (also known as jumper, jumper wire, DuPont wire) is an electrical wire, or group of them in a cable, with a connector or pin at each end (or sometimes without them – simply "tinned"), which is normally used to interconnect the components of a breadboard or other prototype or test circuit, internally or with other equipment or components, without soldering.

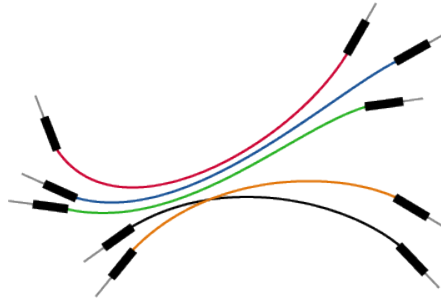


Figure 4.10: Jumper Wires

#### 4.1.11 12V DC Adapter

##### Specifications

- Input - 100-240 VAC 50/60Hz
- Category - Switch Mode Power Adaptor (SMPS)
- Output Type - DC
- Output - 12 Volt, 2Amp



Figure 4.11: 12 V Adapter

#### 4.1.12 Header Pins

Pin headers are stiff metallic connectors that are soldered to a circuit board and stick up to receive a connection from a female socket. While pin headers (often called PH, or headers) are male by definition, female equivalents are also quite common, and we refer to them as female headers (FH) or header connectors.

A plastic structure holds these sets of pin headers together. This structure is often designed to snap apart as needed, though female headers are generally manufactured with a set number of pins.

We define headers by combining:

- The number of pins in a row.
- "X."
- How many pins wide it is

So an 8x2 header would stack eight pins in a row, with two rows of pins attached beside each other, for 16 connections in total.

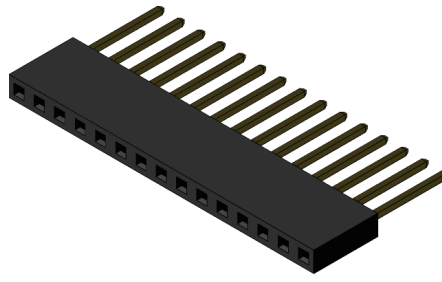


Figure 4.12: Header Pins

#### 4.1.13 Single Strand Wire

Solid wire, also called solid-core or single-strand wire, consists of one piece of metal wire. Solid wire is useful for wiring breadboards. Solid wire is cheaper to manufacture than stranded wire and is used where there is little need for flexibility in the wire. Solid wire also provides mechanical ruggedness; and, because it has relatively less surface area which is exposed to attack by corrosives, protection against the environment.



Figure 4.13: Single strand wire

#### 4.1.14 Push Button

Push Buttons are normally-open tactile switches. Push buttons allow us to power the circuit or make any particular connection only when we press the button. Simply, it makes the circuit connected when pressed and breaks when released. A push button is also used for triggering the SCR by the gate terminal. These are the most common buttons which we see in our daily life electronic equipment.

## Features

- Mode of Operation: Tactile feedback
- Power Rating: MAX 50mA 24V DC
- Insulation Resistance: 100Mohm at 100v
- Operating Force:  $2.55 \pm 0.69$  N
- Contact Resistance: MAX 100mOhm
- Operating Temperature Range: -20 to +70 °C
- Storage Temperature Range: -20 to +70 °C



Figure 4.14: Push Button

### 4.1.15 7805 Voltage Regulator IC

A voltage regulator IC maintains the output voltage at a constant value. 7805 Voltage Regulator, a member of the 78xx series of fixed linear voltage regulators used to maintain such fluctuations, is a popular voltage regulator integrated circuit (IC).

#### Pinout

- INPUT : In this pin of the IC positive unregulated voltage is given in the regulation.

- **GROUND** : In this pin where the ground is given. This pin is neutral for equally the input and output.
- **OUTPUT** : The output of the regulated 5V is taken out at this pin of the IC regulator.

7805 voltage regulator is not very efficient and has drop-out voltage problems. A lot of energy is wasted in the form of heat. So an appropriate heatsink is used to disperse this heat.

If the voltage regulator is situated more than 25cm (10 inches) from the power supply, capacitors are needed to filter residual AC noise. Voltage regulators work efficiently on a clean DC signal being fed. The bypass capacitors help reduce AC ripple. Essentially, they short AC noise from the voltage signal and allow only DC voltage into the regulator.

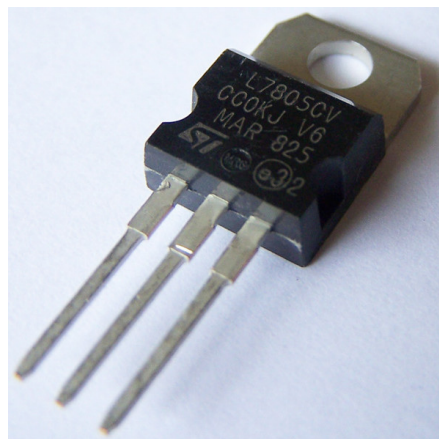


Figure 4.15: LM7805 IC

#### **4.1.16 Capacitors**

A capacitor is a two-terminal electrical device that can store energy in the form of an electric charge. It consists of two electrical conductors that are separated by a distance. The space between the conductors may be filled by a vacuum or with an insulating material known as a dielectric. The ability of the capacitor to store charges is known as capacitance.

It consists of two parallel plates separated by a dielectric. When we connect a DC voltage source across the capacitor, one plate is connected to the positive end (plate I) and the other to the negative end (plate II). When the potential of the battery is applied across the capacitor, plate I become positive with respect to plate II. The current tries to flow through the capacitor at the steady-state condition from its positive plate to its negative plate. But it cannot flow due to the separation of the plates with an insulating material.

An electric field appears across the capacitor. The positive plate (plate I) accumulates positive charges from the battery, and the negative plate (plate II) accumulates negative charges from the battery. After a point, the capacitor holds the maximum amount of charge as per its capacitance with respect to this voltage. This time span is called the charging time of the capacitor.

When the battery is removed from the capacitor, the two plates hold a negative and positive charge for a certain time. Thus, the capacitor acts as a source of electrical energy.



Figure 4.16: Capacitors



## 4.2 System Architecture

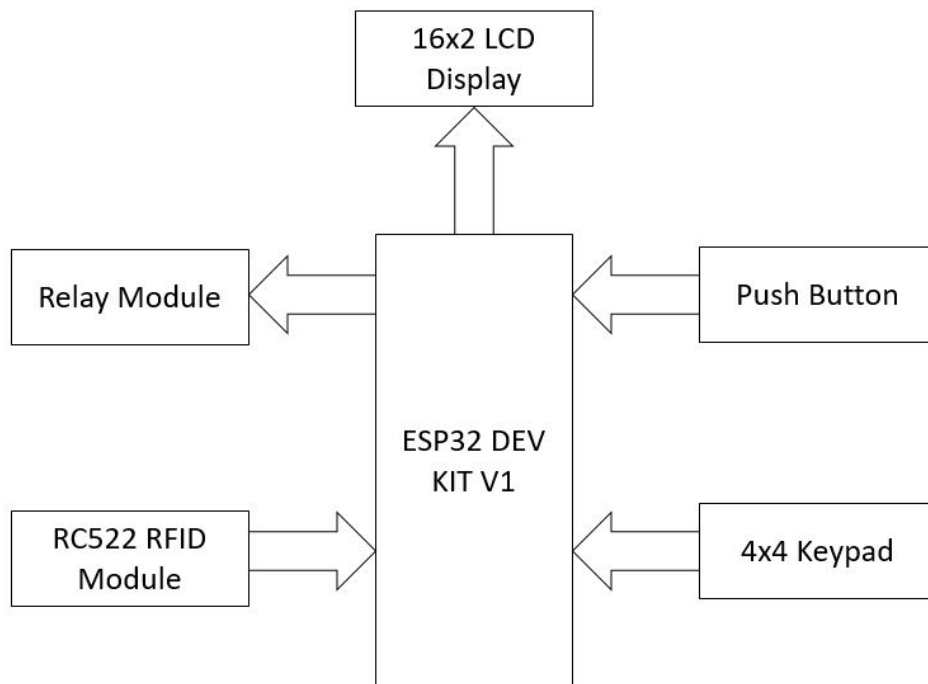


Figure 4.17: Block Diagram

The block diagram above illustrates the complete architecture of the system. It utilizes various modules, including the RC522 RFID Module, 4x4 Keypad, Push Button, Relay, Solenoid Lock, and 16x2 LCD Display, all interfaced with the ESP32 DEV KIT V1 microcontroller. The system takes inputs from the RFID Module, Push Button, and Keypad while providing output to the display and relay module.

Here's how the system works: Initially, the ESP32 DEV KIT V1 microcontroller reads the input from the push button. If the input is low, the microcontroller expects input from the RFID Module. The LCD Display shows the message "Swipe Tag," indicating that the RFID module is ready to read data from the tag. The person requesting access must then present their tag to the module. The module reads the data stored within the tag's chip and communicates it back to the microcontroller. If the tag is valid, the LCD will display the message "Enter Your Pin." Once this message appears, the person is expected to enter their PIN using the 4x4 keypad. The ESP32 DEV KIT V1 microcontroller is now ready to accept input from the keypad. It compares the

entered PIN with the PIN stored in the database (details of the PIN comparison will be explained in the software section). If the PIN comparison is successful, the LCD displays "Access Granted," and the relay module is activated for 5 seconds. The relay acts as a switch, activating the Solenoid Lock. However, if the comparison fails, the LCD will display "Access Denied."

In the event that the ESP32 DEV KIT V1 reads a high input from the push button, the relay and Solenoid Lock will be activated for 5 seconds. This push button is used inside the cabin, allowing someone inside to open the door. To power the microcontroller, a 1000mAh power bank is employed in the project. This power bank supplies a voltage of 5V, which is sufficient for the ESP32 microcontroller. However, the Solenoid Lock operates only at voltages equal to or above 12V, so a 12V adapter is used specifically to power the lock.

# Chapter 5

## Implementation and working

This chapter describes the detailed working of the High security door lock system.

### 5.1 Hardware

The whole circuit is controlled by ESP-32 Development module and the RC-522 RFID reader here uses SPI Protocol instead of UART Protocol because of the features of SPI protocol. The SCK pin of the RFID reader is connected to GPIO18 of ESP-32 and MOSI(Master-out-slave-in) and MISO(Master-in-slave-out) pins of the RFID reader are connected to SPI pins. The RST port is connected to GPIO 22 of ESP-32, Vcc and ground to corresponding pins in ESP-32.

The sixteen pins of the 16x2 LCD Display module are connected to the I2C Module. There are four pins in the I2C Module. The SCL, SDA pins of I2C are connected to 16 and 17 pins respectively. The LCD works on following I2C protocol. Whenever the RFID reader reads a card, the update will be displayed in the LCD Screen.

Coming to the data entering part, i.e., the keypad. Here we used a 4x4 Keypad which consists of 8 data pins representing each key value. The 8 pins are connected to 13, 12, 14, 27, 26, 25, 33, 32 pins of ESP-32 respectively. The value entered in the keypad will be displayed in the LCD screen.

The next comes to the Lock System, where we used an optocoupler relay module

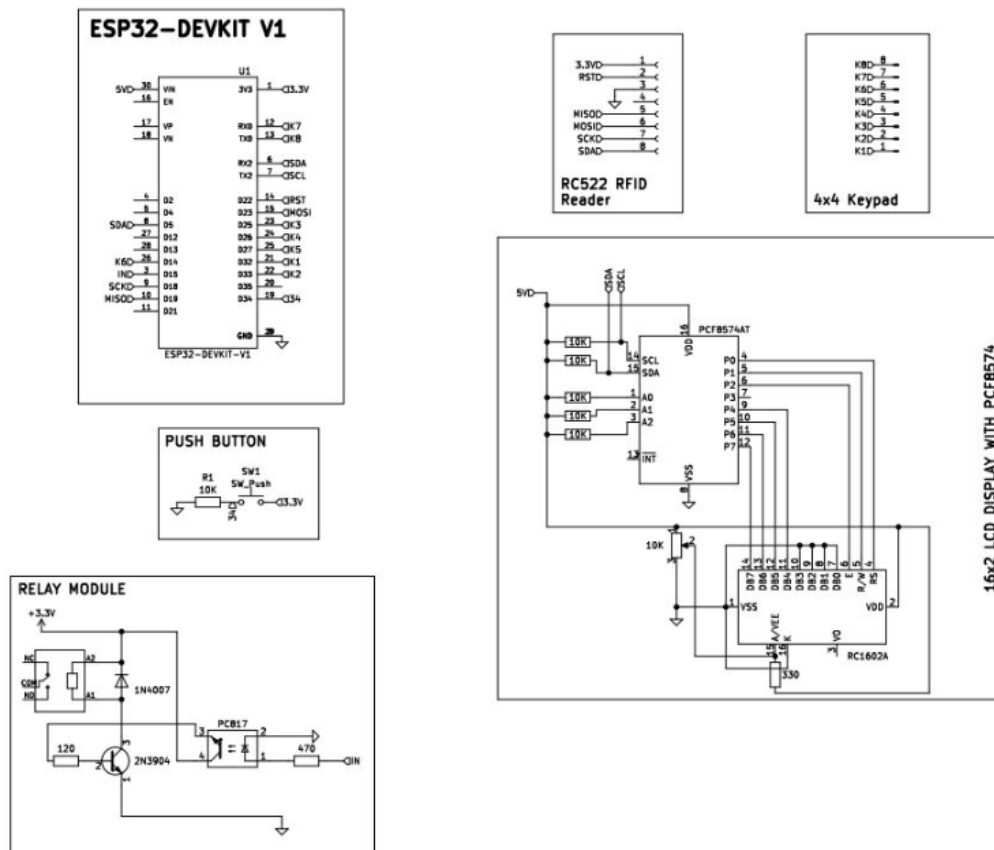


Figure 5.1: Circuit Diagram

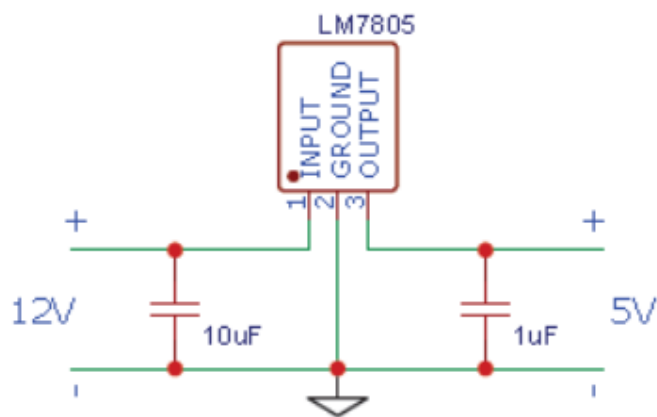


Figure 5.2: Regulator Circuit

to control the 12V solenoid lock. An optocoupler consists of an LED coupled with a photoresistor, it's used in relay modules to convert different signal levels or to isolate

one signal from another and it allows more power. The positive port of the relay module is connected to the positive pin of the 12V adapter jack and the GND of the jack is connected to the negative pin of the solenoid lock. The input(IN) pin of the relay is connected to GPIO 15 of ESP-32.

For opening the door from inside the room we used a push button of 5V or less than that. The Vcc of the button is connected to the Vcc of the ESP module and the ground is connected to the ground of ESP-32 through a 10K pulldown resistor and to the GPIO 34. The pull down resistor is used to carry out the entire current during the opening and closing of the button.

Components	Description
ESP32 DEV KIT V1	Microcontroller for the project
RC522 RFID Module	Reads the data stored in RFID tag and communicates with the microcontroller
4x4 Keypad	Used to input the PIN
Relay Module	Acts as a switch and controls the opening and closing of the lock.
Solenoid Lock	The lock used in the project
12V adapter	Powers the lock
16x2 LCD Display	Displays the required outputs

## 5.2 Software

### 5.2.1 Algorithm

1. Start
2. Set up pin modes, connect to wifi, configure the firebase, set up RFID, and configure ntp protocol to calculate real-time.
3. Enters the void loop function.
4. The read function is called.

5. Reads the data within the output node and if value is 1, jumps back to void loop else push button function is called.
6. If push button state is high the relay function is called and if it is low the rfid function is called. When the swiped tag is read by the reader, the keypad function and print local time function is called and a unique string is stored in the uid variable.
7. Keypad function expects the pin to enter.
8. After 4 keys are pressed, the readdata function is called.
9. In the readdata function, ESP reads the data stored within the corresponding uid variable
10. The hash function is then called. Within the hash functions, the pin which is in the form of an array is combined to a single string.
11. And this string is then hashed with an inbuilt library `mbdhtls/md.h`
12. This hashed value is then compared with the hash string stored within the database that was read in the previous function
13. If they are equal, access is granted and the relay function and write data function is called. Else access is denied and the write data function is called
14. In the relay function, the relay is switched ON and after 5 seconds it is switched OFF.
15. In the write data function, a node is created with the key value as the time that was identified by print local time function
16. Within this node, the name of the user, RFID uid, and whether the access granted or not is stored
17. Returns to void loop.
18. Stop

## 5.2.2 Flowchart

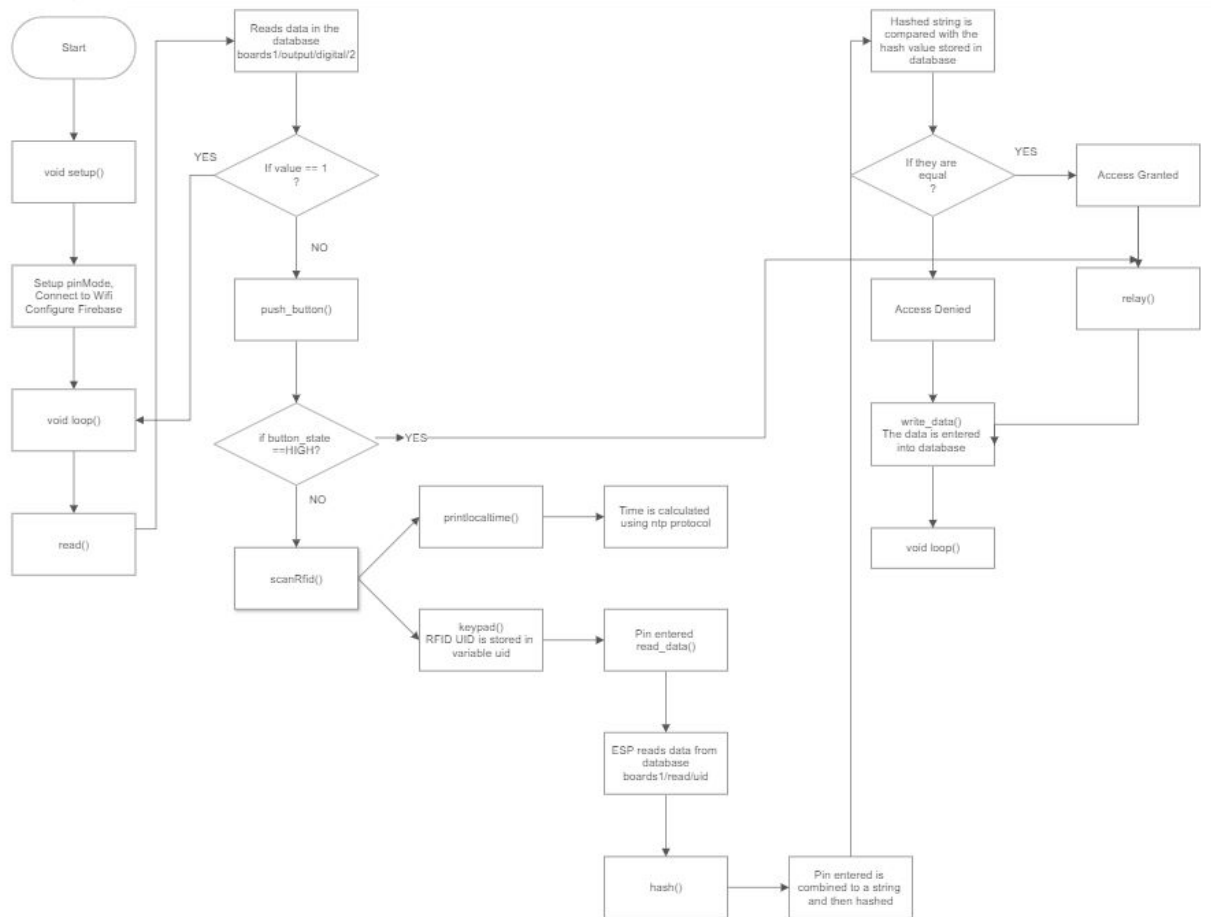


Figure 5.4: Flowchart

## 5.2.3 Library Explanation

**Arduino.h** The arduino.h library is a header file that provides access to various functions and features of the Arduino platform. It is automatically included in Arduino sketches when you create a new project using the Arduino IDE. The arduino.h library includes definitions and functions that allow you to interact with the hardware components connected to the Arduino board, such as digital and analog pins, timers, interrupts, communication interfaces (such as UART, I2C, SPI), and other utility functions.

**WiFi.h** The WiFi.h library is used to connect the ESP32 DEV KIT V1 to the Wifi.

The WiFi.h library allows you to perform tasks such as connecting to a Wi-Fi network, configuring network settings, and sending and receiving data over a Wi-Fi connection. In this project the ESP needs to be connected to the WIFI so that it can interact with the RTDB in firebase and also helps to detect the present time using the NTP protocol.

**Firebase\_ESP\_Client.h** The details of all the members with access along with their PINs are stored in the RTDB of firebase. This library is used in order to configure the firebase and helps to interact with the firebase services. This library provides a set of functions and classes to interact with Firebase Realtime Database, Firebase Authentication, and Firebase Cloud Messaging services.

**SPI.h** The SPI.h library is a header file that provides functions and classes for using the Serial Peripheral Interface (SPI) communication protocol on ESP32. It allows you to communicate with other devices, such as sensors, display modules, or other microcontrollers, using the SPI protocol. In this project we are using SPI protocol to communicate with the RC522 RFID Reader. The SPI protocol is a synchronous serial communication interface that enables full-duplex communication between a master device and one or more slave devices. It uses a clock signal (SCK) and separate data lines for transmission (MOSI - Master Out Slave In) and reception (MISO - Master In Slave Out). Additionally, it often includes a chip select (CS) line to select the specific slave device for communication. The SPI.h library provides functions and classes to configure the SPI hardware on the ESP32 board, send and receive data using the SPI protocol, and manage communication settings.

**MFRC522.h** The MFRC522.h library is a header file that provides functions and classes for interacting with the MFRC522 RFID reader. The MFRC522 module is a popular RFID reader that can read and write RFID tags based on the ISO/IEC 14443A/MIFARE standard. The MFRC522.h library allows you to perform tasks such as reading RFID tag data, writing data to RFID tags, and controlling the behavior of the MFRC522 module. It provides an abstraction layer that simplifies the process of using the MFRC522 module, making it easier to integrate RFID functionality into the project.



**Keypad.h** The Keypad.h library is a header file that provides functions and classes for interfacing with matrix keypads. Matrix keypads are commonly used input devices that consist of multiple buttons arranged in rows and columns. The Keypad.h library simplifies the process of reading input from these keypads. In this project the keypad is used to input the PIN. The Keypad.h library allows you to define the keypad's layout, including the number of rows and columns, and provides functions to detect button presses and releases.

**LiquidCrystal\_I2C.h** The LiquidCrystal\_I2C.h library is a header file that provides functions and classes for controlling LCD displays that use the I2C communication protocol in Arduino projects. It is commonly used when working with LCD displays that have an I2C backpack or module attached to reduce the number of required I/O pins. The LiquidCrystal\_I2C.h library allows you to initialize and control LCD displays with just a few lines of code. It abstracts the low-level I2C communication details, making it easier to interface with the LCD display and display text, numbers, and custom characters.

**Wire.h** GPIO 21 and 22 are the default I2C pins for the ESP32 DEV KIT V1 but in this project, these pins are already in use for the interfacing of RC522 RFID with ESP32 using SPI protocol. The Wire. h library is used to change the default I2C pins using the wire. begin().

**time.h** In this project, we are required to calculate the time in which the tag is swiped. The time is calculated using the ntp protocol and time. h is an inbuilt library to calculate the time.

**mbdtdls/md.h** To enhance the security system we are using the hashing algorithm (SHA-256). The hashed value of the PIN is stored in the real-time database. When the PIN is entered, the entered PIN is converted into its hash value and then compared with the string in the database. The mbedtdls/md.h is an in-built library used to convert the value to its corresponding hashed value.

**string.h** The string.h library provides functions to manipulate the strings. It includes functions for operations such as copying, concatenating, comparing, and searching within strings.

## **5.2.4 Real Time Data Base**

A real-time database is a type of database system that is designed to process and manage data in real-time or near real-time. It is optimized for handling data that needs to be updated and accessed instantly as it changes, providing instantaneous responses to queries and updates. Traditional databases, such as relational databases, are typically optimized for handling batch processing or handling data that is not expected to change frequently. In contrast, real-time databases are designed to handle high-speed data streams and provide real-time data updates to multiple users or applications simultaneously. Real-time databases are commonly used in applications that require instant data availability and synchronization across multiple devices or users. They are prevalent in various domains, including financial systems, stock market trading, monitoring and control systems, online gaming, collaborative applications, and more.

In this project, we have used Firebase which is a popular real-time database. Firebase is a comprehensive platform provided by Google that offers a wide range of back end services and tools for building and managing web and mobile applications. It provides developers with a set of ready-to-use services that handle tasks such as data storage, user authentication, real-time database management, hosting, cloud functions, and more.

In this project, we use Firebase to store the unique pin and the information about who has swiped their RFID tag, the timing, and whether access was granted or not to them. The pin is stored in the hashed form which is a 32-character string. In real-time we can learn who has unlocked the door and add or delete users from the database to enhance the security of that area.



Figure 5.5: Real Time Database

### 5.2.5 Web Application

In this project, the web application acts as the master lock which completely shuts the system down. The application is linked with the real-time database in Firebase and only those user authenticated to use the database will be able to access the web application. This application is linked with the Output node in the Firebase and when the lock button in the application is pressed the value in the output node changes from 0 to 1. The ESP32 continuously monitors the changes in the value of the node and when it reads the value '1' the complete system is shut down that is there is no way any user will be able to gain access to the room. This web application was introduced as an extra security measure.

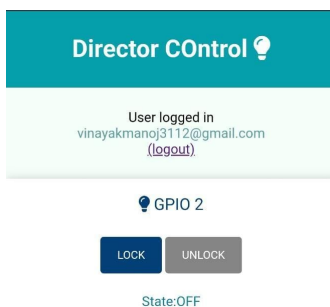


Figure 5.6: Web Application Page

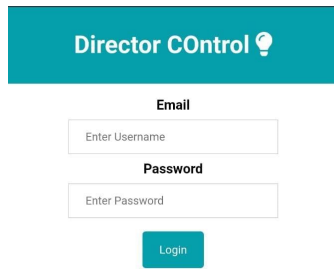
The image shows a web login page for 'Director Control'. At the top, there is a teal header bar with the text 'Director Control' and a lightbulb icon. Below the header, the word 'Email' is centered above a text input field with the placeholder 'Enter Username'. Underneath that, the word 'Password' is centered above another text input field with the placeholder 'Enter Password'. At the bottom of the form, there is a teal button with the text 'Login' in white.

Figure 5.7: Web Login Page

## 5.2.6 Hashing using SHA-256

Hashing is a process of transforming input data into a fixed-size string of characters, which is typically a hash value or hash code. It is commonly used in computer science and cryptography for various purposes, such as data integrity verification, password storage, and indexing.

The algorithm used for hashing in this project is SHA-256. Here is how SHA-256 works:

1. Input processing: SHA-256 operates on input data in blocks of 512 bits. If the input message is longer, it is divided into multiple blocks. Padding is applied to the last block to ensure it is a complete 512-bit block.
2. Message expansion: Each 512-bit block is further divided into 16 words of 32 bits each. These words go through a series of transformations and are expanded to create 64 words.
3. Initialization: SHA-256 uses a set of constant initial values known as "initial hash values" or "state." These values are predefined and serve as the starting point for the hash computation.
4. Compression function: The compression function is the core of the SHA-256 algorithm. It operates on each 512-bit block of the input message and updates the state based on the block's contents.
5. Iterative process: The compression function is executed in multiple rounds, with each round performing a series of logical operations, including bitwise

operations (AND, OR, XOR), modular addition, and logical functions (bit shifting, rotations). These operations mix the input data and update the state at each step.

6. Final hash value: After processing all the blocks, the final state is obtained. It consists of a 256-bit hash value, which represents the unique fingerprint of the input data.

We introduced hashing in this project with just one concern: “What if someone gets hold of the data inside the real-time database?”. The pin that is stored in the database is in the hashed form. It is impossible to retrieve the original data back from the hashed form. In our door lock system when someone enters their pin it is first hashed using the SHA-256 algorithm and is compared with the string inside the database if it matches then access is granted else denied.

## SHA256

SHA256 online hash function

1103

Input type

Hash ☒ Auto Update

f0d588a225e6e6ba0501a3f787230abf579f6db2dd55be0fa3450f8acd54e6f3

Figure 5.8: Hashing using SHA-256

### **5.2.7 Network Time Protocol**

The Network Time Protocol (NTP) is a system for synchronizing the clocks of hosts and clients across the Internet. NTP is a protocol intended to synchronize all computers participating in the network within a few milliseconds of Coordinated Universal Time (UTC). The core of the protocol is NTP's clock discipline algorithm that adjusts the local computer's clock time and tick frequency in response to an external source — such as another trusted NTP server, a radio or satellite receiver, or a telephone modem. A core problem in NTP is establishing the trust and accuracy of nodes in the NTP network. This is done through a combination of selection and filtering algorithms to choose from the most reliable and accurate peer in the synchronization network.

NTP uses a hierarchical network architecture that forms a tree structure. Each level of this hierarchy is called a stratum and is assigned a number starting with zero representing reference hardware clocks. A level one server is synchronized with a level zero server, and this relationship continues so that a server synchronized to a stratum  $n$  server runs at stratum  $n+1$ . The stratum number, therefore, represents the distance from an accurate reference clock. In general, the stratum of a node in the server is an indication of quality and reliability but this is not always the case; it is common to find stratum three-time sources that are higher quality than other stratum two-time sources.

In order to collect the data about when a person has used their RFID tag local time is needed this is done using the NTP protocol and updates into the real-time database.

# Chapter 6

## Experiment and Results

This chapter deals with various experiments conducted to ensure proper working of the system and the results obtained.

### 6.1 The scanned tag is valid and PIN entered is correct

In this experiment, a valid RFID tag was shown to the reader and after the reader reads the tag, the correct PIN was entered using the Keypad.

**Result** The tag was successfully read by the reader, LCD prints the message "Enter Your PIN". On entering the accurate PIN, access was granted. The LCD prints "Access Granted", the relay switches ON, and the solenoid lock was unlocked.

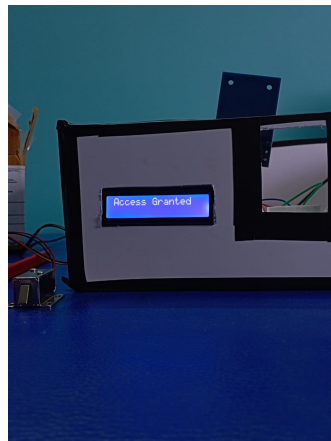


Figure 6.1: Access Granted

## 6.2 The scanned tag is valid and PIN entered is incorrect

In this experiment, a valid RFID tag was shown to the reader and after the reader reads the tag, the incorrect PIN was entered using the Keypad.

**Result** The tag was successfully read by the reader, LCD prints the message "Enter Your PIN". On entering the inaccurate PIN, access was denied. The LCD prints "Access Denied", and the relay remains OFF.

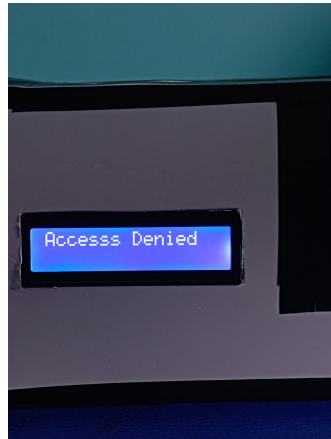


Figure 6.2: Access Denied

## 6.3 The scanned tag is invalid

In this experiment, an invalid RFID tag was shown to the reader.

**Result** The tag was successfully read by the reader, and LCD prints the message "Invalid tag". The system returns back to the initial stage.

## 6.4 The system is in the lock state

In this experiment, the lock button in the web application is pressed and different tags were shown to the reader.

**Result** The system enters the lock state and completely shuts down. The RFID reader does not read any cards which are shown to it.



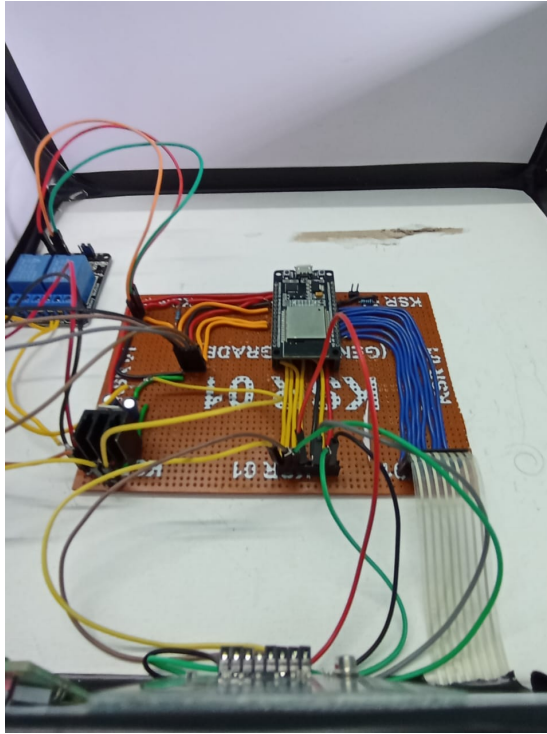


Figure 6.3: Photograph of Circuit



Figure 6.4: Hardware Photograph

# **Chapter 7**

## **Conclusion and Future Scope**

### **7.1 Conclusion**

The proposed RFID-based door lock system offers a secure and efficient solution for access control. Each RFID tag is assigned a unique PIN, adding an extra layer of security to the authentication process. This combination of RFID technology and PIN verification ensures that only authorized individuals can gain access to restricted areas.

The system's integration with a real-time database enables the storage of crucial user information and PINs. This centralized database allows for efficient management of access permissions, with administrators able to easily update, add, or remove users. The real-time nature of the database ensures that any changes made are immediately reflected, enhancing system responsiveness.

Additionally, a web application serves as a master lock, providing convenience and control. Administrators can remotely monitor and manage the system, as well as initiate a complete shutdown if needed. This feature is especially useful in emergencies or during maintenance, allowing for seamless control over the entire system.

Compared to traditional lock and key mechanisms, the RFID-based system offers several advantages. It eliminates the need for physical keys, which can be lost, stolen, or duplicated. RFID tags also improve access speed and ease, as individuals only need

to present their tag for verification. This streamlined process enhances user experience and reduces bottlenecks at entry points.

In conclusion, the proposed system provides a comprehensive solution for secure access control. The combination of RFID technology, unique PINs, real-time database integration, and a web application as a master lock ensures efficient and reliable operation. By leveraging these technologies, organizations can enhance security protocols, improve access control management, and maintain a higher level of protection for their premises and assets.

## **7.2 Future Scope**

1. Rechargeable batteries can be implemented as a backup power source to ensure uninterrupted operation during power outages or interruptions. These batteries can be connected to the system's main power supply, acting as a secondary power source. This feature ensures that the door lock system remains operational even when the primary power source is temporarily unavailable, maintaining security and access control functionality.
2. A mobile application can be developed to send instant notifications to authorized users whenever a door access event occurs, providing them with real-time updates on who accessed the door and when.
3. To address the issue of system shutdown when there is no Wi-Fi connection for the ESP device to interact with Firebase, the cache memory can provide a solution. By utilizing the EEPROM (Electrically Erasable Programmable Read-Only Memory) in the ESP, the database can be temporarily stored in the cache memory. This allows the ESP to access and retrieve necessary information even without an active Wi-Fi connection, ensuring the system remains operational and functional even in the absence of internet connectivity.

# References

- [1] Shafin, Kishwar Kabir, KaziLutful Hasan, Nazmul Mouri,Israt Islam, Samina Ansari,Lazima Karim, Md Hossain,Md. (2015). Development of anRFID Based Access Control Systemin the Context of Bangladesh.10.1109/ICIIECS.2015.7193024
- [2] S. Shepard, “RFID Radio Frequency Identification”, USA, ISBN: 0-07-144299-5, 2005.
- [3] Zhang, L., “An Improved Approach to Security and Privacy of RFID application System”, Wireless Communications, Networking and Mobile Computing. International Conference. pp 1195- 1198, 2005.
- [4] [randomnerdtutorials.com/esp32-firebase-realtime-database/](http://randomnerdtutorials.com/esp32-firebase-realtime-database/)
- [5] [randomnerdtutorials.com/esp32-firebase-web-app/](http://randomnerdtutorials.com/esp32-firebase-web-app/)
- [6] [firebase.google.com/docs/database/web/read-and-write/](https://firebase.google.com/docs/database/web/read-and-write/)
- [7] [randomnerdtutorials.com/esp32-firebase-realtime-database/](http://randomnerdtutorials.com/esp32-firebase-realtime-database/)
- [8] [randomnerdtutorials.com/esp32-data-logging-firebase-realtime-database/](http://randomnerdtutorials.com/esp32-data-logging-firebase-realtime-database/)
- [9] [www.movable-type.co.uk/scripts/sha256.html](http://www.movable-type.co.uk/scripts/sha256.html)