A

Project Report on

DEVELOPMENT OF GSM BASED ADVANCED DIGITAL LOCKING SYSTEM

Submitted

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

BACHELOR OF TECHNOLOGY

in

Electronics & Communication Engineering

by

B. KEERTHAN SAI REDDY – 18R11A0404

K. AKANKSHA – 18R11A0424

K. KIRAN BABU – 18R11A0426

under the supervision of
G. Aparna
Assistant professor

Department of Electronics & Communication Engineering
GEETHANJALI COLLEGE OF ENGINEERING AND TECHNOLOGY
(UGC Autonomous)
(Accredited by NAAC with ‘A’ & NBA, Approved by AICTE, New Delhi,& Affiliated to JNTUH)
Cheeryal (V), Keesara (M), Medchal Dist, Hyderabad– 501 301, Telangana State

2021-2022

GEETHANJALI COLLEGE OF ENGINEERING & TECHNOLOGY

Department of Electronics & Communication Engineering

CERTIFICATE

This is to certify that the project report titled *"Development of GSM based advanced digital locking system"* being submitted by **B. Keerthan Sai Reddy, K. Akanksha, K. Kiran Babu** bearing hall ticket numbers **18R11A0404, 18R11A0424, 18R11A0426** in partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology in ***Electronics & Communication Engineering*** is a record of bonafide work carried out under my supervision.

Mrs. G. Aparna
Assistant Professor

Dr. S. Suryanarayana
HoD

Internal Examiner

External Examiner

ACKNOWLEDGEMENTS

We, the students of ECE department of Geethanjali College of Engineering and Technology would like to convey heartfelt thanks to **Dr. S. Udaya Kumar**, Principal of the college for the inspiration and encouragement given to us to move ahead in the execution of this project.

We are highly grateful to **Dr. S. Suryanarayana**, Head of the Department of **Electronics and Communication Engineering** of **GCET** for the support extended.

We are very happy for being supervised by **G. Aparna**, Assistant professor for her/his able guidance during the completion of the proposed work successfully.

We are also thankful for the members of the project review committee for the timely suggestions which helped a lot to complete our project work as per schedule.

With Regards

B. KEERTHAN SAI REDDY (18R11A0404)
K. AKANKSHA (18R11A0424)
K. KIRAN BABU (18R11A0426)

CONTENTS PAGE NO.s

ABSTRACT

Security has become very important, but along with that, people also need a system that is highly secure and more reliable. As conventional door locks can be easily opened, this makes people vulnerable to security threats. This study attempts a comparative analysis of pre-existing researches, made in the field of security control system developed and improvised over the span of time with multifactor authentication technique's evolvement. Security systems or door locking mechanics have evolved from metallic door locks of primitive type keys to advanced controlling structure with up to four or five step authentications to ensure utmost safety.

Multifactor authentication is often used in situations where more strong security is required. In most cases, multifactor authentication is complex and not user-friendly because it requires additional steps as far as end users are concerned. With the advancement of technology, digital door locks have become very common these days. Digital lock doesn't require any physical key but it uses RFID, fingerprint, Face ID, pin, passwords, etc. to control the door lock system. For this project two factors i.e., Password and OTP are used for authentication. With this in addition to entering a password (first factor) users need to enter a Onetime Password (second factor) manually that they receive to their mobile phones that is generated by a hardware. So, introducing additional authentication factors greatly increases the level of security. Hence two factors are implemented for authentication.

Multi-factor authentication gives the best conveniency for better security. It also alerts the user whenever the wrong details are entered through notification. Buzzer is used to alert the neighbor's or people nearby. The security increases with this model. Resetting password is additional feature which is very useful.

LIST OF FIGURES

LIST OF TABLES

LIST OF SCREENS

SYMBOLS & ABBREVIATIONS

GSM	- Global System for Mobile Communication
LCD	- Liquid Crystal Display
LED	- Light Emitting Diode
OTP	- One Time password
IDE	- Integrated Development Environment
RFID	- Radio Frequency Identification
SDA	- Serial Data Line
SCL	- Serial Clock Line
USB	- Universal Serial Bus
I2C	- Inter-Integrated Circuit
SMS	- Short Message Service
OS	- Operating System
DC	- Direct Current

CHAPTER 1 - INTRODUCTION

1.1 GENERAL BACKGROUND

These days offices and houses need security since many faces threat of burglary, if individual is available or not at place. When it comes to security systems, it is one of the primary concerns in this busy competitive world, where human cannot find ways to provide security to his confidential belongings manually. Instead, an individual finds an alternative solution which provides better, reliable and atomized security. This is an era where everything is connected through network, where anyone can get hold of information from anywhere around the world. Thus, chances of one's info being hacked are a serious issue. Due to these risks it's very important to have some kind of personal identification to access one's own info. Now a day's personal identification is becoming an important issue all around. Among mainstream personal identification methods, mostly password and identification cards techniques are seen. But it is easy to hack password now-a-days and identification cards may get lost, thus making these methods quite unreliable. So, lengthy password with alphabets can be used. With this hacking time is very high but, tag is not effective so less used.

There are certain situations which are very annoying like when a person locks himself out of his house or office or he leaves his key inside or lost. These kinds of situations always trouble people who use manual door lock with keys. Although in some places people use smart cards, there might arise a situation when someone loses the card or keeps the card inside. Then in other scenarios there are caretakers for locking houses or offices and keeping the keys safe. But then again there are times when a person in charge of the keys might not be available or has gone to some emergency routine, which can cause unwanted delay for people who need the key straightaway. By the help of digitals locks these problems can be avoided. We need not carry any keys and simply unlock door by simple steps, even some unlock directly by face match, but with these there are some disadvantages too.

Figure 1.1 Digital Door Locks

1.2 PURPOSE

Automatic door system has become a standard feature on many different types of buildings and homes. And they are becoming popular every day to develop effective electronic devices which provide security. Home security has been a major issue because of the increase in crime rate and everybody wants to take proper action to prevent unauthorized user. Various control systems have been designed over the years to prevent access to unauthorized user. The main aim for providing locks for our home, school, office, and building is for security of our lives and property. It is therefore important to have convenient way of achieving this goal.

The purpose of this advanced digital locking system is to develop a unique system through mobile technology which can control various units of the houses, industries, and also provides a security system, the various appliances can be utilized by managing them remotely by using GSM technology, which enables the user to remotely control the operations of the appliances. Just by pressing keypad of remote telephone the user can perform ON/OFF operations on the appliances. Unlock the door by using pre-decided password. Increase the security level to prevent an unauthorized unlocking of the door. To prevent the opening of the door by unauthorized persons. Flexibility to the user to change or reset the password. More secure yet cost-efficient way of door locking-unlocking system.

1.3 METHOD

The first step of this project was to formulate the research questions. The next step was to gather information about advanced locking system. This was done by reading articles and investigating projects from previous years related to the subject. There were some projects where some demerits are present and solution were found in our project and make efficient locking mechanism. From the literature study, components that were needed for the prototype could be determined. We had multiple options to get some functionalities and compared all of them to find the accurate which fits our project well. A prototype was then made which looks like Figure 1.2 when implemented practically. When the construction was completed, the Arduino software Integrated Development Environment (IDE) was used to program the algorithm. Then whole setup is tested in all possible ways of implementation and then optimized for ease of operation and in most efficient manner.

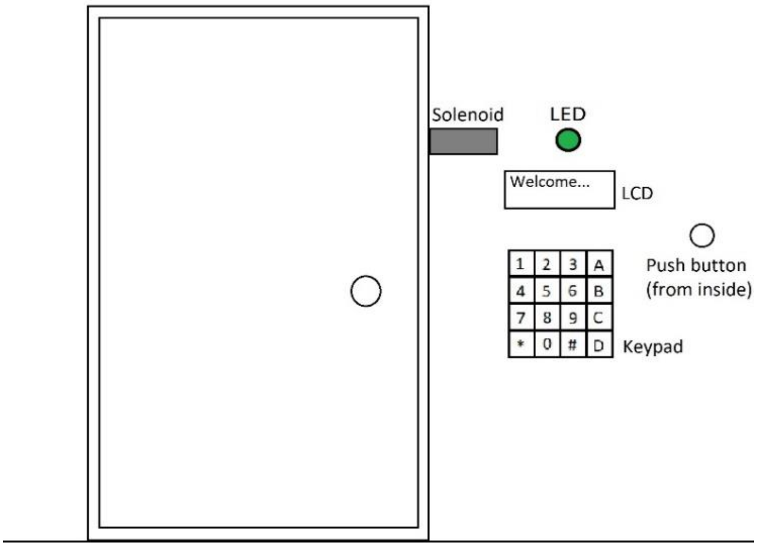


Figure 1.2 Schematic diagram of digital locking system

1.4 HARDWARE COMPONENTS

1.4.1 Arduino Uno

Arduino is an open-source physical computing platform based on a single microcontroller board. Arduino is used when there are interactions between inputs and outputs. It is used to control the output according to the inputs command such as controlling the light or motor by using a switch. The Arduino programming language uses an Integrated Development Environment (IDE), and a single board microcontroller. The language can be expanded through C libraries.

The advantages of using Arduino are

- ✓ Inexpensive – Compared to other microcontrollers, Arduino board is cheaper.
- ✓ Cross platform – Arduino software can run on Windows, Linux and other OS.
- ✓ Simple, clear programming environment – Arduino is easy to use by beginners and advanced users.

In our project Arduino UNO is used. It is microcontroller board based on the Microchip ATmega328P microcontroller and developed by Arduino.cc. The board is equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards and other circuits. The board has 14 digital I/O pins, 6 analog I/O pins, and is programmable with the Arduino IDE via a type B USB cable as shown in Figure 1.3. It can be powered by the USB cable or by an external 9-volt battery, though it accepts voltages between 7 and 20 volts. It is similar to the Arduino Nano and Mega with slight differences.

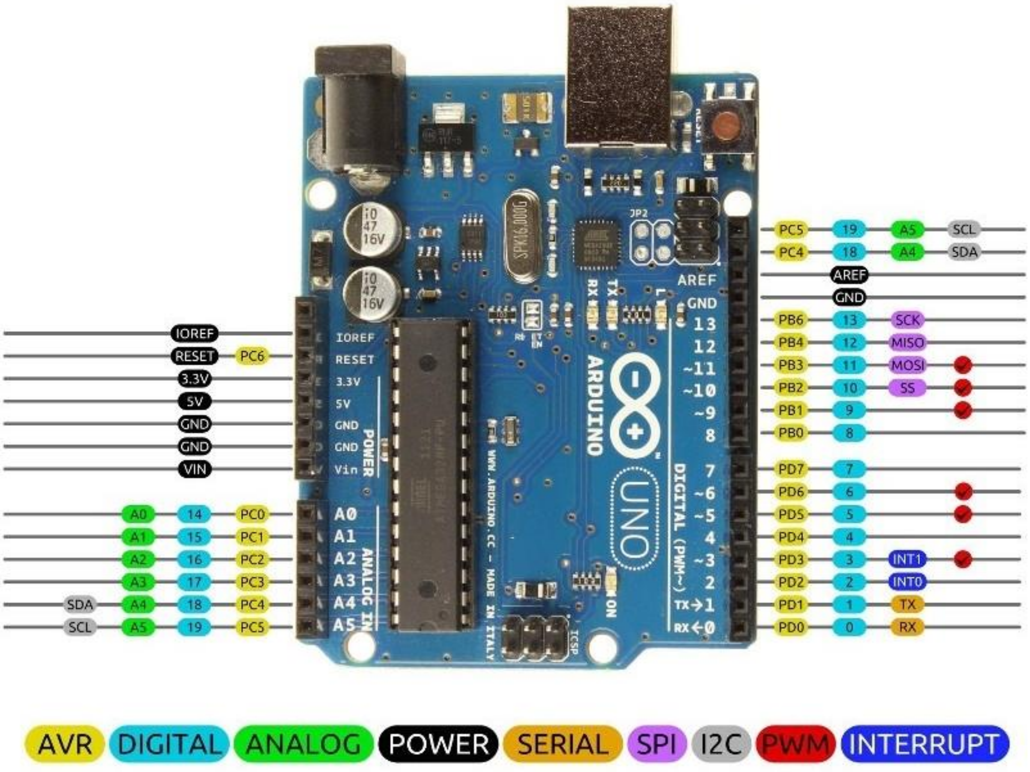


Figure 1.3 Arduino UNO Pinout

Parameter	Range/Value
Microcontroller	ATmega328P
Operating voltage	5 volts
Digital I/O pins	14(of which 6 has PWM output)
Analog I/O pins	6
Input voltage	7 to 20 volts
Flash memory	32 KB
SRAM	2 KB
EEPROM	1KB
Clock speed	16 MHz

Table 1.1 Arduino UNO Specifications

1.4.2 GSM Module

GSM modem or GSM module is a device that uses GSM mobile telephone technology to provide a wireless data link to a network. GSM modems are used in mobile telephones and other equipment that communicates with mobile telephone networks. They use SIMs to identify their device to the network.

A GSM module is a hardware device that uses GSM mobile telephone technology to provide a data link to a remote network. From the view of the mobile phone network, they are essentially identical to an ordinary mobile phone, including the need for a SIM to identify themselves to the network. It operates at either the 900 MHz or 1800 MHz frequency band.

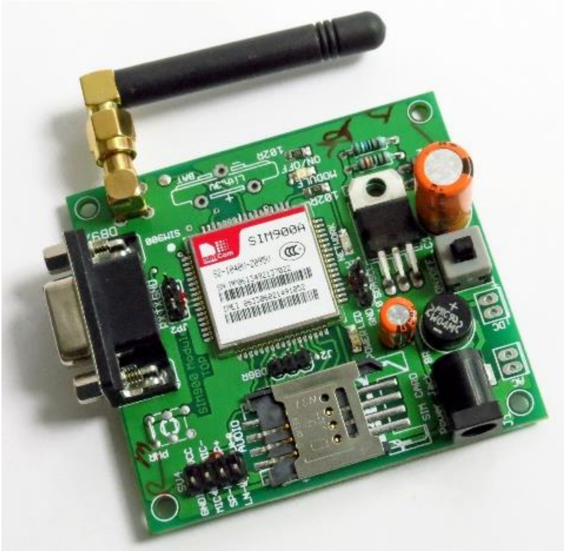


Figure 1.4 GSM Module

GSM Modules are one of the commonly used communication modules in embedded systems. A GSM Module is used to enable communication between a microcontroller (or a microprocessor) and the GSM Network. Here, GSM stands for Global System for Mobile Communication. It allows microcontrollers to have a wireless communication with other devices and instruments. Such wireless connectivity of microcontroller opens up to wide range of applications like Home Automation, Home Security Systems, Disaster Management, Medical Assistance, Vehicle Tracking, Online Banking, E – Commerce etc. to name some.

1.4.3 16x2 LCD

An electronic device that is used to display data and the message is known as LCD 16×2. As the name suggests, it includes 16 Columns & 2 Rows so it can display 32 characters in total & every character will be made with 5×8 (40) Pixel Dots. So, the total pixels within this LCD can be calculated as 32 x 40 otherwise 1280 pixels. 16 X2 displays mostly depend on multi-segment LEDs. There are different types of displays available in the market with different combinations such as 8×2, 8×1, 16×1, and 10×2, however, the LCD 16×2 is broadly used in devices, DIY circuits, electronic projects due to less cost, programmable friendly & simple to access.

Parameter	Range/Value
Operating voltage	4.7V to 5.3V
Display Bezel size	72 x 25mm
Operating current	1mA
Controller	HD47780
Number of columns and rows	16 & 2
Total Characters	32

Table 1.2 Specifications of LCD

Figure 1.5 16x2 LCD

1.4.4 I2C Module

I2C module is a synchronous, multi slave, multi master packet switched, single-ended serial bus. i.e., multiple chips can be connected to the same bus. I2C uses only two bidirectional open collector or open drain lines, Serial Data Line (SDA) and Serial Clock Line (SCL), pulled up with resistors.

I2C Module has an inbuilt PCF8574 I2C chip that converts I2C serial data to parallel data for the LCD display. These modules are currently supplied with a default I2C address of either 0x27 or 0x3F. If there are 3 sets of pads labelled A0, A1, & A2 then the default address will be 0x3F. If there are no pads the default address will be 0x27. The module has a contrast adjustment pot on the underside of the display. This may require adjusting for the screen to display text correctly as shown below.

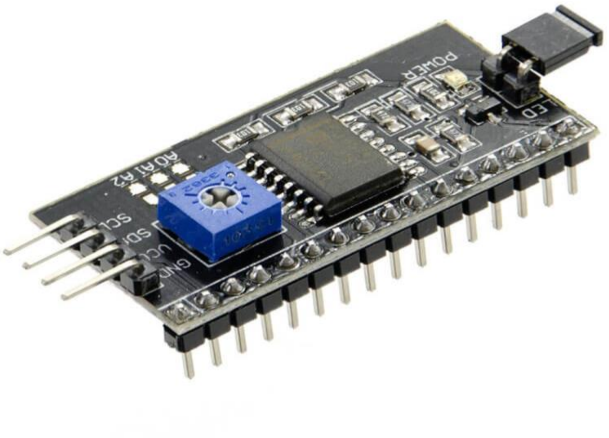


Figure 1.6 I2C Module

Features of I2C Module: -

- Operating Voltage: 5V
- Backlight and Contrast is adjusted by potentiometer
- Serial I2C control of LCD display using PCF8574
- Come with 2 IIC interface, which can be connected by Dupont Line or IIC dedicated cable
- Compatible for 16x2 LCD
- This is another great IIC/I2C/TWI/SPI Serial Interface
- With this I2C interface module, you will be able to realize data display via only 2 wires.

1.4.5 Solenoid

This DC 12V Cabinet Door Lock Electric Lock Assembly Solenoid can be used for locking sell-machine, storage shelf, file cabinet and etc. The hidden way of unlocking can be used for an emergency. The lock works as the circuits disconnects, and it will unlock as the instant power-on. It is steady, durable, and energy-saving and had a long lifespan. In the anti-theft and shockproof design, the lock is better than other kinds of locks. After connecting the wires and when the current is available, the electric lock can control the door’s opening and closing. Whenever power is supplied the electro-magnet inside solenoid gets magnetized. Since to latch is made of metal it gets pulled inside thus lock opens. If the supply is stopped then simply magnetism is lost and the latch is released. It just needs Phase and ground and can be given to any pin since magnetization can be done in any direction.

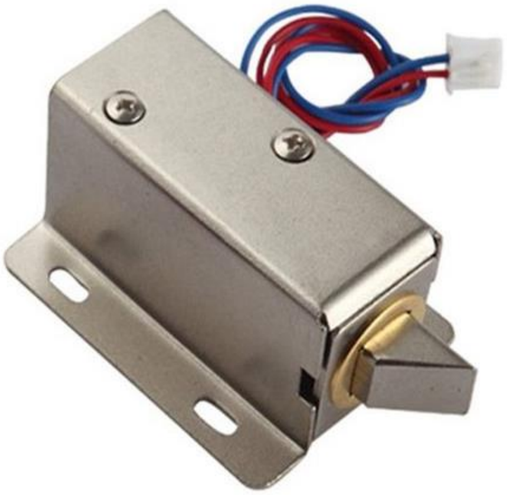


Figure 1.7 Solenoid

Parameter	Range/Value
Model	DC 12V Door Lock
Rated Operating Voltage (VDC)	12
Rated Current (mA)	0.80A.
Power Consumption (Watt)	9.6
Holding Force (N)	2.45
Unlocking Time	1 sec

Table 1.3 Solenoid specifications

1.4.6 Relay

A relay is an electromagnetic switch operated by a relatively small current that can control much larger current. This module is designed for switching only a single high-powered device from your Arduino. It has a relay rated up to 10A per channel at 250VAC or 30VDC. There are three channels of the relay broken out to blue screw pin terminals. The channels are labeled for their function: common (COM), normally closed (NC), and normally open (NO).

On the other side of the module, there are three pins – a Ground pin and a VCC pin to power the module and an input pin IN to control the relay. The input pin is active LOW, meaning relay will not be activated and it will become active when pin is HIGH.

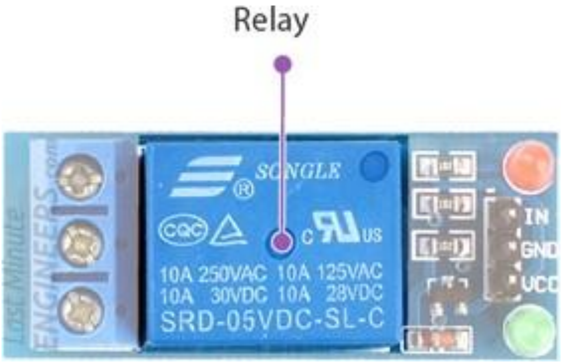


Figure 1.8 One channel relay

There are two LEDs on the relay module indicating the position of the relay as shown in Figure 1.9

- The Power LED will light up when the module is powered.
- The Status LED will light up when the relay is activated.

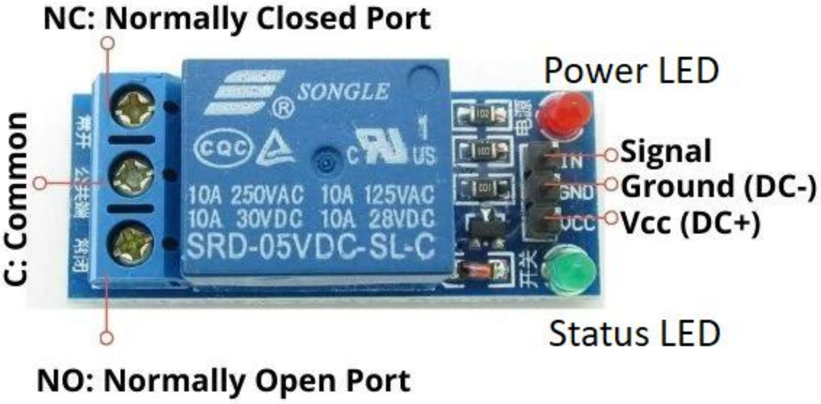


Figure 1.9 Relay description

1.4.7 4x4 Keypad

Keypad is used as an input device to read the key pressed by the user and to process it. It is a block or pad of buttons set with an arrangement of digits, symbols, or alphabetical letters. Pads mostly containing numbers and used with computers are numeric keypads. Keypads are found on devices which require mainly numeric input such as calculators, television remotes, push-button telephones, vending machines, ATMs, Point of Sale devices, combination locks, and digital door locks. Keypad is used to enter character and integer that is required to access the door. In this project, keypad is implemented for getting password, used to get OTP and so on.

This 4x4 matrix keypad has 16 built-in pushbutton contacts connected to row and column lines. A microcontroller can scan these lines for a button-pressed state. In the keypad library, the Propeller sets all the column lines to input, and all the row lines to input. 4x4 keypad consists of 4 rows and 4 columns. Switches are placed between the rows and columns as shown in Figure 1.11. A key press establishes a connection between the corresponding row and column, between which the switch is placed.

The advantage of a matrix keypad is that the use of it will allow the programmer to reduce the number of pins to be used. In a 4×4 matrix keypad, there are four rows and four columns connected to 16 push button switches.

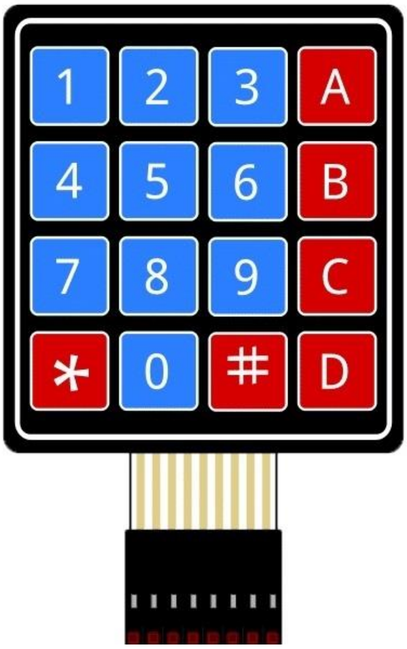


Figure 1.10 4x4 Keypad

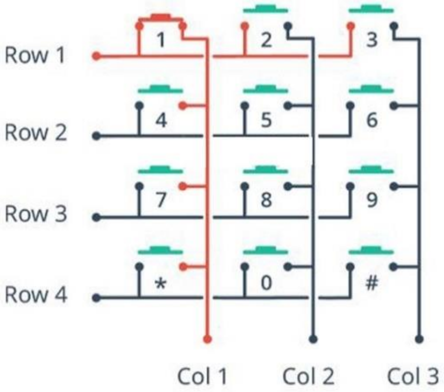


Figure 1.11Internal diagram of keypad

1.5 ARDUINO IDE

The Arduino IDE is an open-source software, which is used to write and upload code to the Arduino boards. The IDE application is suitable for different operating systems such as Windows, Mac OS X, and Linux. It supports the programming languages C and C++. Here, IDE stands for Integrated Development Environment.

The program or code written in the Arduino IDE is often called as sketching. We need to connect the Genuino and Arduino board with the IDE to upload the sketch written in the Arduino IDE software. The sketch is saved with the extension '.ino.'

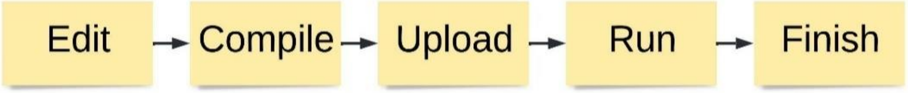
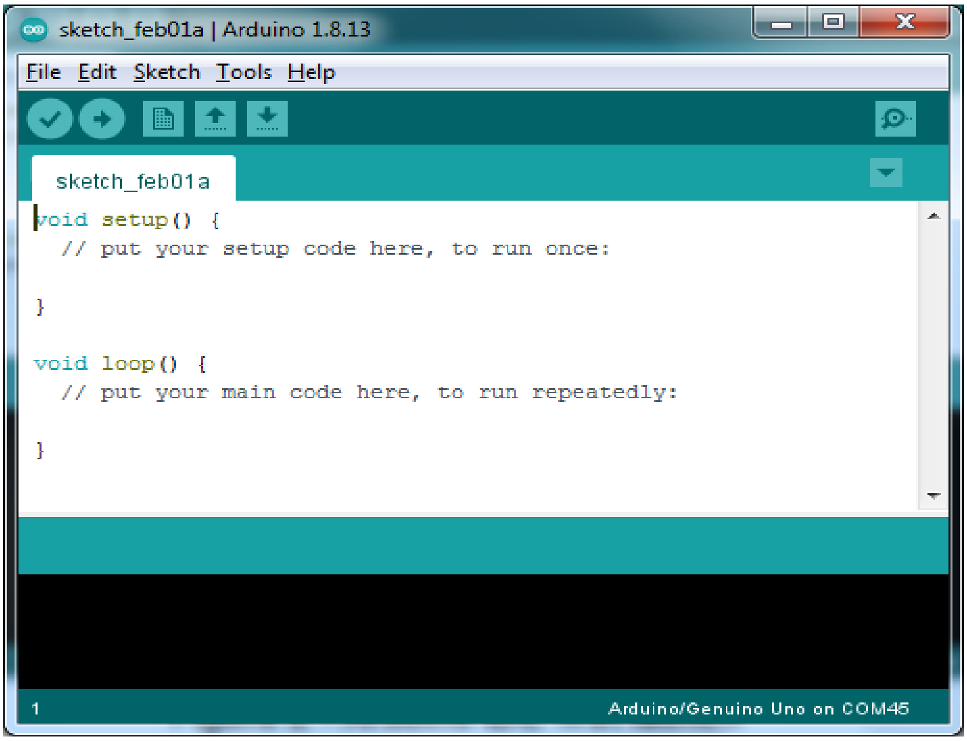


Figure 1.12 Arduino code development flow


sketch_feb01a | Arduino 1.8.13
File Edit Sketch Tools Help
sketch_feb01a
1
Arduino/Genuino Uno on COM45

```
void setup() {
  // put your setup code here, to run once:

}

void loop() {
  // put your main code here, to run repeatedly:

}
```

Figure 1.13 Initial Arduino IDE interface

In the above interface code is edited. Setup is run only once. The Loop is the function which runs as long as power is supplied. Code is written and run in there. While uploading board type need to be chosen and port number and other specifications in tool bar. Serial monitor is where we can see the board output.

CHAPTER 2 - LITERATURE SURVEY

2.1 EXISTING SYSTEMS

This study has analyzed current lock systems that are used in houses and offices at present. It has been found that although these methods are helpful in the initial days, eventually they become outdated and pose much threat to security issues. They have also been identified as quite expensive. Below is a discussion on the pros and cons of the existing systems.

2.1.1 Deadbolt System

Security protocol followed in this system was “Single key for a single lock” as shown in Figure 2.1. For a few days, it was satisfactory but at one time it was proved wrong by the fact that multiple keys can be easily made for a single lock. Hence this system is considered vulnerable and outdated in current times.

Figure 2.1 Bolt locking system

2.1.2 Password-Authentication

This system stores the password of authenticated users for the purpose of validation which provides considerable security to the users. Power consumption is efficient and usage is user-friendly. However, unauthorized users can easily acquire passwords through different methods (hacking, guessing and so on.). These problems can be reduced by long passwords and hiding password while entering.

2.1.3 RFID reader authentication

Radio Frequency Identification (RFID) is a fundamental and inexpensive technology that enables wireless data transmission as shown in Figure 2.2. With RFID, wireless automatic identification takes a very specific form: the object, location, or individual is marked with a unique identifier code contained with an RFID tag, which is in some way attached to or embedded in the target. This system has some advantage like the data on a RFID card is readable only with special equipment, keeping the data recorded on the chip secure. RFID systems can be easily duplicated or cards can fall into the wrong hands, even we may lose the tag.

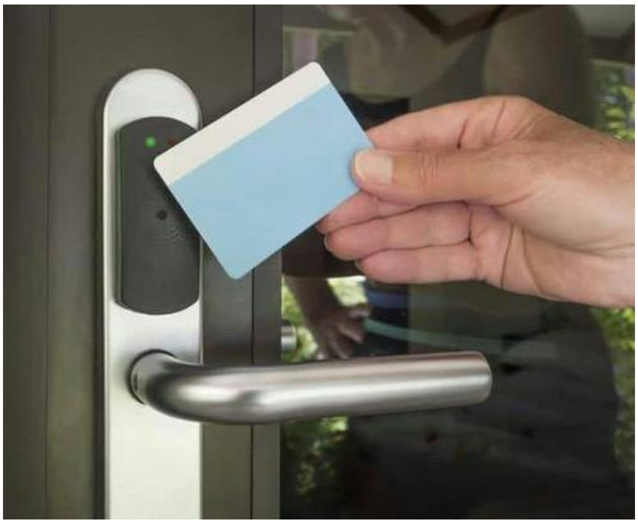


Figure 2.2 RFID based door lock

2.1.4 Face detector lock

These systems have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. It is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence. Sometimes system will detect face on screens like photos or mobiles and unlocks the door.

2.1.5 Retinal scanner

The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. The image acquisition requires a person to peep into an eye piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. This device is frequently used for security purpose. The false acceptance and rejection rates are lower in this device. But the problem of this device is, it is not user- friendly and the equipment cost is very high.

2.1.6 Iris scanner

Iris recognition is a method of biometric authentication, based on extraction features of the iris of an individual’s eyes. Each individual has a unique iris; the variation even exists between identical twins and between the left and right eye of the same person. The advantage of using iris scanner is, it has very high accuracy and the accuracy of iris scanners can be affected by changes in lighting. As iris is a small target and a scanner cannot be performed properly for multiple people of different heights. The main shortcomings with iris recognition technology, is that the iris scanners are very expensive and requires a lot of memory to store data.

2.1.7 Voice recognition

Voice recognition or speaker recognition is the problem of identifying a speaker from a short utterance. This biometric technology uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style). A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise.

2.2 DIGITAL DOOR LOCKING SYSTEM

Smart doors have been implemented using different methods such as Radio frequency identification (RFID) and Biometric lock to unlock and lock door. Both the RFID and biometric lock are really ideal and smart ways to make a door smart, due to necessity and limitations such as cloning of biometric prints or card. Also, on the other hand the biometric readers are expensive and initialization is length process. We need to read the biometrics for more than twice to register.

Also, previously there were some digital door locks based on password. There were some limitations in these like we need call company if we forget our password. So, to overcome these limitations we developed our model.

Figure 2.3 Digital Locks in market

2.3 LITERATURE REVIEW

S. Umbarkar implemented an electronic door lock system using the Arduino Platform using three different modes i.e., Keypad, Bluetooth and GSM modules. These three modules operated on a 4-digit password through a keypad matrix. The Bluetooth module was used to establish connection between smart phone and door lock Bluetooth kit and then the password is entered to open the door. The GSM module was used to enter the password on his mobile phone via a text message to open or close the door. It also sent a text message through this module in case of three failed attempts to enter the password and used a buzzer as warning of unauthorized intrusion. Motor is used to close and open door. LCD is used to communicate with user.

Steeven Zeiss proposed a method of “gesture-based door lock security system using capacitive sensors” to detect human presence over a distance and there is no physical contact between the door and the human required to lock/unlock the door. This helps in preventing health sanitation issues such as contagious diseases from spreading due to several people touching the door knob by their bare hands such as in case of public toilets or hospitals. When a swipe gesture is performed, only the vertical and horizontal gesture sensors are active.

Shilpi Banerjee has implemented an “Automatic Password Based Door Lock System”. This system works on pre- decided password. It increases the security level to prevent an unauthorized access done by the attacker. In case the user forgets the passwords, certain privileges are given to the user to change or reset the password. This automatic password-based lock system gives user more secure way of locking/unlocking the system.

Somjit Nath designed and developed a door unlocking system that can be used in Laboratory or library. The system was developed using a central server to gather and store all the useful information and the access to authorized personnel was provided through RFID technology. Wireless transmitter and receiver were also used in the system. The system is based on Arduino Uno. All the users are assigned a serial no. which is burnt into their RFID tag that can be read by the reader when the user needs to unlock the door. All the information about the user is stored in the central server.

Meera Mathew and Divya R S built a door lock system with RFID technology. It also provided authentication from passwords. The system provided better efficiency and reliability. They implemented multiple encryption schemes using Java. The two important features of the system are: key matching and encryption scheme in Java. An android app was used to store the secret key set for encryption called the Secure Wallet. User could change the keys as per their convenience. The user had a login id and password to login to the app and update the secret key based on which the OTP will be received by the user and entered while unlocking the door. to unlock the door, the user has to place his RFID tag close to the reader. The reader retrieves the information associated with the tag and the data is matched with the stored information. When the information matches with the stored data, an OTP is sent to the user on his smart phone. This OTP is entered on the keypad by the user and is verified.

"Door – Automation System Using Bluetooth" was implemented by Lia Kamelia, Alfin Noor Hassan S.R. Mada Sanjaya and W.S., Edi Mulyana. This implementation was on Android platform, so the implementation cost is less and affordable by a common user. With the use of wireless Bluetooth connection, the system installation is more easy way.

Muhammad Sabirin Hadis developed a door lock security system that can be unlocked or locked by entering a password by a remote device to control the same. The system also makes use of Bluetooth technology with low power which is available for all gadgets. The system also indirectly encourages the program of United Convention of Right People with disabilities. This system can be used by people with disability due to its ability to unlock the door when the authorized person is in the vicinity of the door lock system using the Bluetooth technology. This Bluetooth technology acts as a communication protocol between the user and the door lock system. The system is low power as it consumes less power than the Wi-Fi. The system consists of four components: Door Lock, Lock Control System, Server and a Device with Bluetooth Technology.

2.4 SUMMARY

Sl No.	Author	Title	Advantages	Limitations
1	A. Hemalatha G.Gandhimathi	RFID, Password & OTP based Door Lock	Higher security	Tag may be lost No reset password feature
2	S. Umbarkar	Electronic door lock system using Arduino	Error notification Buzzer alert	No password recovery option Password length is fixed
3	Steeven Zeiss	Gesture-based door lock security system using capacitive sensors	Contactless opening Helpful in hospitals	No security measures Can be accessed by anyone
4	Somjit Nath	Door unlocking system based on RFID	Central server holds much more data	RFID may be lost No data backup
5	Muhammad Sabirin Hadis	Remote door lock security system	Low power usage Remote Unlocking access	Bluetooth has small range

Table 2.1 Summary of literature survey

CHAPTER 3 - PROPOSED ALGORITHM

3.1 INTRODUCTION

Previously there were some digital locks based on GSM. Along with that there are some locks which works on password only. These are some disadvantages with this like someone might steal the mobile and then unlock the lock easily with OTP or password may be forgot. There were some other problems with this old system like mobile may be lost where OTP is received, we may forget our password, unlock door from inside and so on. So, we made sure that the issues in the old system are solved. So, the multi-factor or two factor locking system is implemented with some enhanced features which helps user to much more extent.

So, with the help of new system we can solve these problems. The option of sending OTP to multiple persons makes easy to unlock even when battery dies in one of the mobile or even the mobile is lost. Also, to solve the issue of forgetting password. We provided a solution for that so that password can be reset if forgot. Reset password has a security question to make sure we can’t change password directly with help of OTP only which reduces the level of security. If any wrong character in password or OTP is entered it can be removed or in security question, this helps to make changes and not start the process from the start, this can be seen in Figure 3.2.

To make it easy to unlock from inside, installation of a push button is done which unlocks the door with a small push. To make it easy to understand weather the door is locked or unlocked we added LED, which indicates status of door lock. To alert security guard or neighbors buzzer which rings whenever wrong details entered while unlocking is added. All these components are connected and shown in Figure 3.1. Along with these features the power consumption is also quiet less.

3.2 BLOCK DIAGRAM

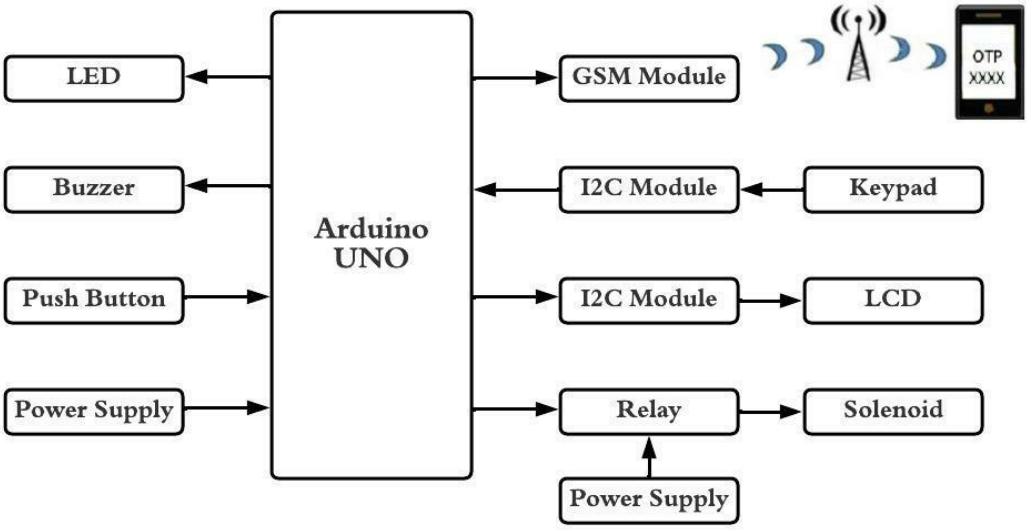


Figure 3.1 Block diagram of Door Lock

3.3 FLOWCHART

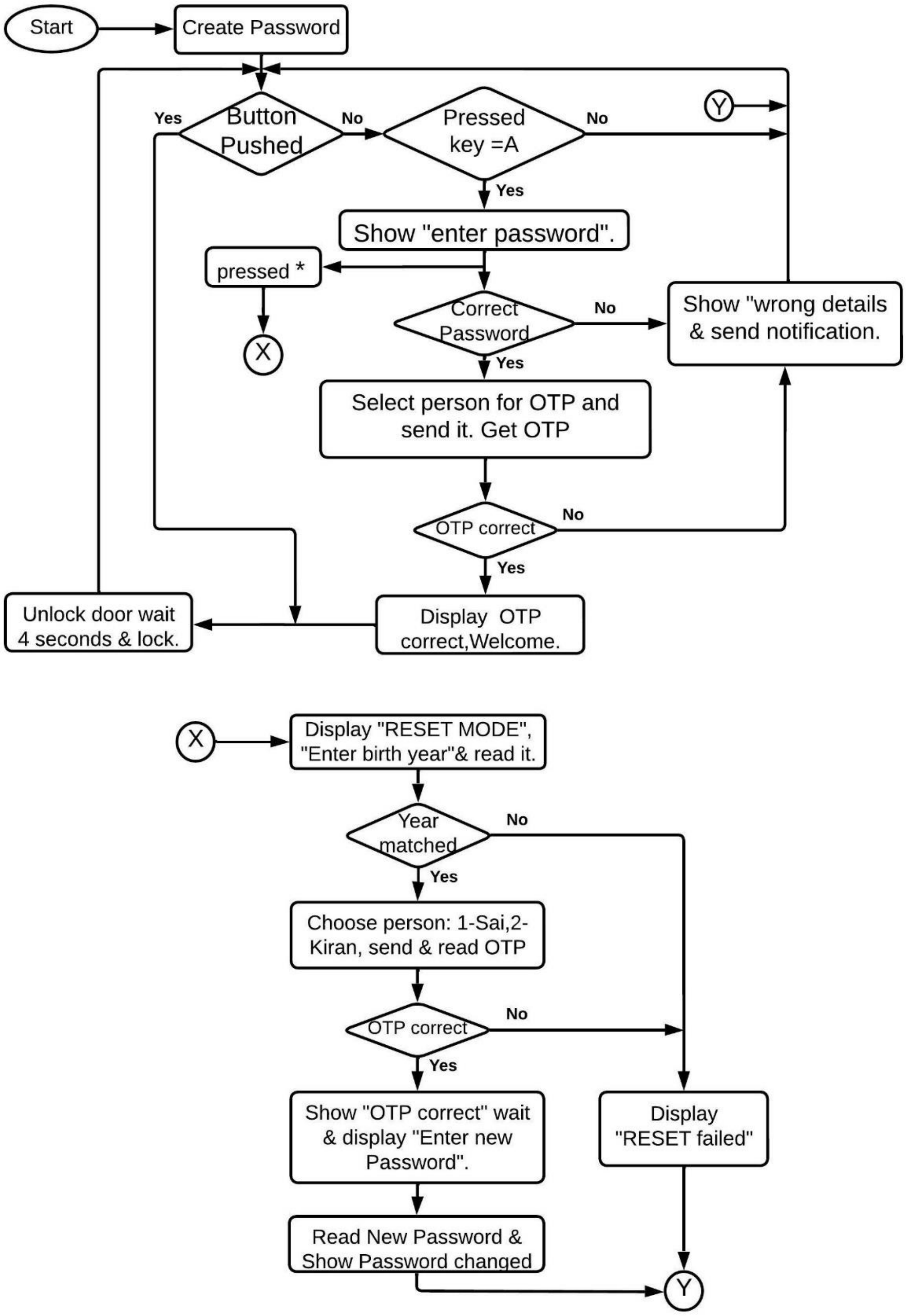

Start
Create Password
Button Pushed
Yes
No
Pressed key =A
No
Y
Yes
Show "enter password".
pressed *
X
Correct Password
No
Show "wrong details & send notification.
Yes
Select person for OTP and send it. Get OTP
OTP correct
No
Yes
Unlock door wait 4 seconds & lock.
Display OTP correct,Welcome.
X
Display "RESET MODE", "Enter birth year"& read it.
Year matched
No
Yes
Choose person: 1-Sai,2-Kiran, send & read OTP
OTP correct
No
Yes
Show "OTP correct" wait & display "Enter new Password".
Display "RESET failed"
Read New Password & Show Password changed
Y

Figure 3.2 Flowchart of system

3.4 CIRCUIT DIAGRAM

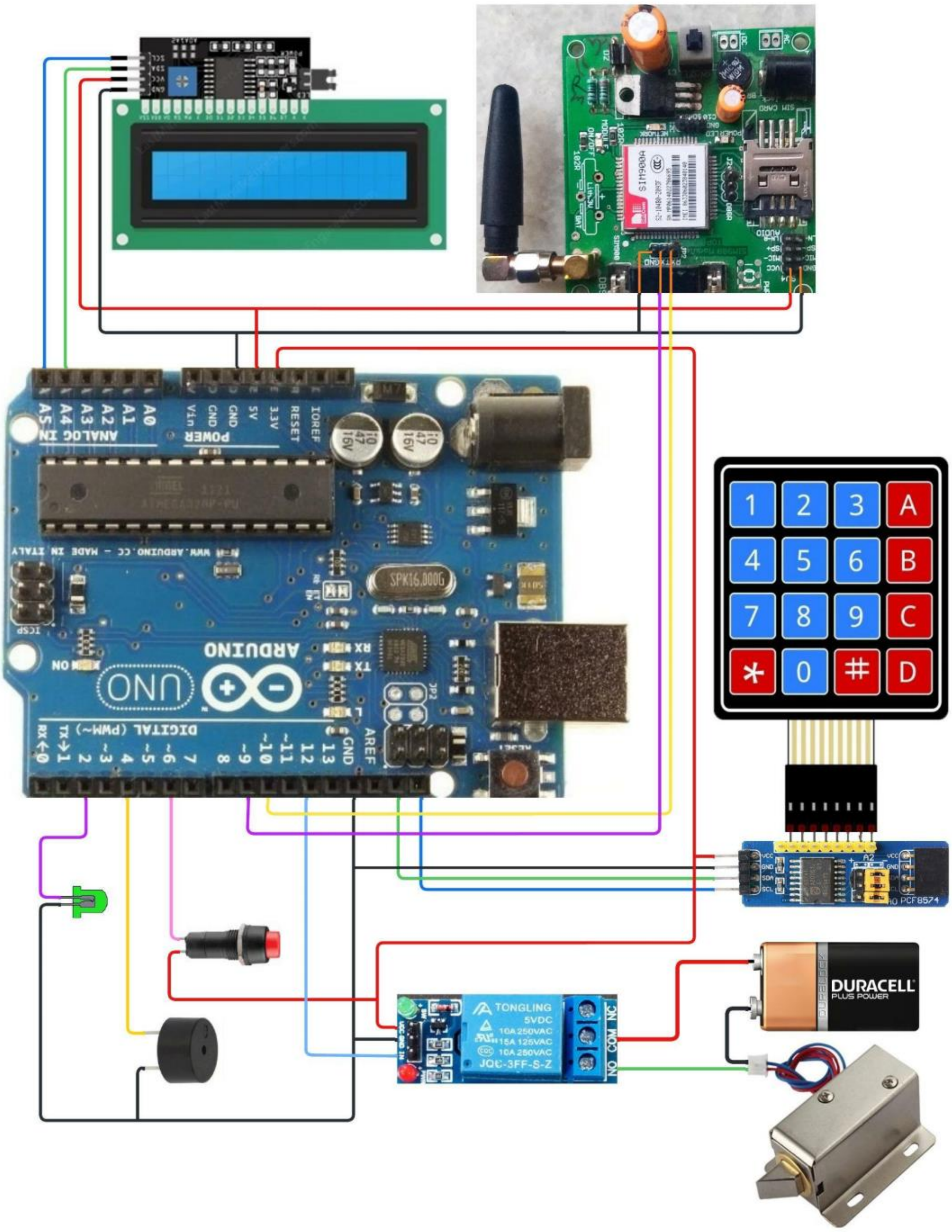


Figure 3.3 Circuit diagram

3.5 BASIC DESIGN UNITS

These are components used in designing the locking system. Each part has its own work to do. Based on the functionality they are divided into three categories. Input, Output and processing units. Input gets data from the user and output is used to instruct the user and also indicate status to user. The processing unit is used process the inputs given based on the loaded algorithm and generate output. This output is delivered to user by output devices.

Components	Class	Functionality
Keypad	Input	It gets data entered by user
Push button		Unlock door when pushed
12V Battery/Adaptor		Power the system
LCD	Output	Display progress of system
LED		Show status of door
Buzzer		Alert the security
Solenoid		Works as lock to close
GSM		Sends OTP and notifications
Arduino	Processing	Brain of the system
I2C module		Convert parallel data to serial
Relay		Control the solenoid lock

Table 3.1 Design units' classification

3.5.1 Input Unit

This is the unit in which command is given to start the execution of a program and in this project button A on keypad serves the purpose of sending command as input. After this the process of unlocking starts from outside the door. Here inputs like password and OTP details entered by user are needed. So, one of the input units is keypad. To reduce number pins from 8 to 2, a serial data converter called I2C module is used. Along with that one of the other inputs in push button. This push button is used to send a signal that it is pushed. It uses power supply of 3.3V to do this function. These are the two input units. Along with this power supply is needed. Arduino needs at least 5V but it can accept 12V. So, we simply used one adaptor to power both Arduino and Solenoid.

3.5.2 Output Unit

The system has many output components which serves different functionality. Mainly GSM is used to interface with mobile, that is to send OTP to mobile or error notification. It needs a network card to send these SMS's. LCD is used to display the instructions to the user. It is an important component because it is display where we can see the position of the current step. Apart from these LED is used to indicate the status of the door weather unlocked or locked. Buzzer is used to alert the security nearby whenever wrong details are entered. Command is sent to relay whenever the door needs to be unlocked. These are the output units in the system.

3.5.3 Processing Unit

The data from inputs is processed here to generate output. There will be a preloaded code which is used to process data. Generally, it is the brain of the system. Here Arduino is one of the processing devices which compiles the code. It runs on an infinite loop if power is supplied. All data from input devices is given to this and this Arduino generates an output. Along with this I2C Module is used to convert parallel data into serial one. Here it consists of SDL and SCL lines. SDL transfers data and SCL is clock for data to be sent as shown in Figure 3.4. By usage of this I2C module the number of pins connected to Arduino is reduced.

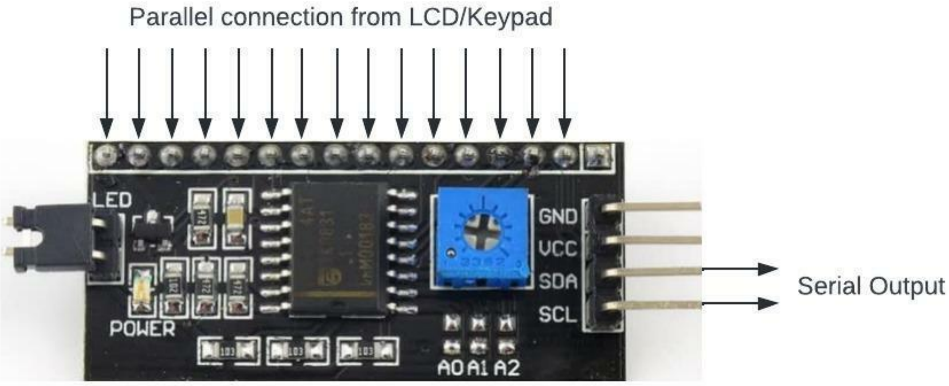


Figure 3.4 Parallel to serial conversion by I2C

CHAPTER 4 - SOFTWARE CODE

```
#include <SoftwareSerial.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <Keypad_I2C.h>
#define green 2                                  //green led pin
#define buzzer 4                                 //buzzer pin
#define buttonPin 6                              //Push Button pin
#define relay 12                                 //relay pin
String master;
String otpstring;
String security = "2000";
String esecurity;
String eotp;
String edata;
String substr;
char customkey;
SoftwareSerial mySerial(9, 10);                  //connection to gsm(tx,rx)
int x,f=0;
const byte ROWS = 4;
const byte COLS = 4;
char keys[ROWS][COLS] ={
{'1','2','3','A'},
{'4','5','6','B'},
{'7','8','9','C'},
{'*','0','#','D'}};
byte rowPins[ROWS] = {0, 1, 2, 3};
byte colPins[COLS] = {4, 5, 6, 7};
Keypad_I2C myKeypad(makeKeymap(keys), rowPins, colPins, 4,4, 0x20, PCF8574);
LiquidCrystal_I2C lcd(0x27, 16, 2);
void setup()
{
    Wire.begin();
    myKeypad.begin(makeKeymap(keys));
    Serial.begin(9600);
    mySerial.begin(9600);                        //initializing GSM
    delay(100);
    lcd.init();
    lcd.clear();
    lcd.backlight();
    newpassword();
    lcd.setCursor(0,0);
    lcd.print("New Password Set");
    delay(1000);
    lcd.clear();
    lcd.setCursor(1,0);
    lcd.print("Lock Activated");
    delay(1000);
    lcd.clear();
    lcd.noBacklight();
    pinMode(relay, OUTPUT);
    pinMode(green, OUTPUT);
    pinMode(buzzer, OUTPUT);
    pinMode(buttonPin, INPUT);
    digitalWrite(relay, LOW);
    digitalWrite(green, LOW);
    digitalWrite(buzzer, LOW);
}
void loop()
{
        customkey = myKeypad.getKey();
        if(digitalRead(buttonPin)){
                digitalWrite(relay, HIGH);
                delay(3000);
                digitalWrite(relay, LOW);
        }
        else if(customkey == 'A'){
                lcd.backlight();
                lcd.setCursor(1, 0);
                lcd.print("Enter Password");
                readpassword();
                if(f==1){
                        f=0;
                        esecurity="";
                        goto alpha;
                }
                if(checkpassword()){
                        lcd.clear();
                        lcd.setCursor(0, 0);
                        lcd.print("PASSWORD CORRECT");
                        delay(1000);
                        sendotp();                              //sending otp function
                        readotp();                              //read otp entered by user
                        if(checkotp()){
                                allok();
                        }
                        else    {
                                lcd.clear();
                                lcd.setCursor(0, 0);
                                lcd.print("OTP WRONG");
                                digitalWrite(buzzer, HIGH);
                                gsmerror();
                                digitalWrite(buzzer, LOW);
                        }
                }
                else{
                        lcd.clear();
                        lcd.setCursor(0, 0);
                        lcd.print("PASSWORD WRONG");
                        digitalWrite(buzzer, HIGH);
                        gsmerror();
                        digitalWrite(buzzer, LOW);
                }
                alpha:lcd.clear();
                lcd.noBacklight();
                edata = "";
                eotp = "";
        }
}
void readpassword()                             //gets password from user
{
        x=0;
        customkey = myKeypad.waitForKey();
        while(customkey != '#'){
                if(x == 0 && customkey == '*'){
                        resetpassword();
                        f=1;
                        return;
                }
                else if(x > 0 && customkey == '*'){
                        x--;
                        substr="";
                        substr+=edata.substring(0,x);
                        edata="";
                        edata+=substr;
                        lcd.setCursor(x,1);
                        lcd.print(" ");
                }
                else if(customkey != '*'){
                        edata = edata + customkey;
                        lcd.setCursor(x, 1);
                        lcd.print("*");
                        x++;
                }
                customkey = myKeypad.waitForKey();
        }
}
void readsecurity()                                     //gets security code
{
        x=0;
        customkey = myKeypad.waitForKey();
        while(customkey != '#'){
                if(x > 0 && customkey == '*'){
                x--;
                substr="";
                substr+=esecurity.substring(0,x);
                esecurity="";
                esecurity+=substr;
                lcd.setCursor(x,1);
                lcd.print(" ");
        }
        else if(customkey != '*'){
                esecurity = esecurity + customkey;
                lcd.setCursor(x, 1);
                lcd.print("*");
                x++;
        }
        customkey = myKeypad.waitForKey();
        }
}
void readotp()                                          //reads OTP entered
{
        x=0;
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Enter OTP");
        customkey = myKeypad.waitForKey();
        while(customkey != '#'){
                if(x > 0 && customkey == '*'){
                        x--;
                        substr="";
                        substr+=eotp.substring(0,x);
                        eotp="";
                        eotp+=substr;
```

```
            lcd.setCursor(x,1);
            lcd.print(" ");
        }
        else if(customkey != '*'){
            eotp = eotp + customkey;
            lcd.setCursor(x, 1);
            lcd.print("*");
            x++;
        }
        customkey = myKeypad.waitForKey();
    }
}
void resetpassword()                    //resets password
{
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("RESET Mode");
    delay(750);
    lcd.setCursor(0, 0);
    lcd.print("Your Birth Year?");
    readsecurity();
    if(checksecurity){
        sendotp();
        readotp();
        if(checkotp()){
            newpassword();
            lcd.clear();
            lcd.setCursor(0, 0);
            lcd.print("Password Changed");
        }
        else{
            goto beta;
        }
    }
    else{
        beta : lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("RESET Failed");
    }
    delay(1000);
}
void newpassword()                      //stores new password
{
    lcd.clear();
```

```
        lcd.setCursor(0, 0);
        lcd.print("Set New Password");
        master = "";
        x=0;
        customkey = myKeypad.waitForKey();
        while(customkey != '#'){
                if(x > 0 && customkey == '*'){
                        x--;
                        eotp.setCharAt((master.length()-1), '\0');
                        lcd.setCursor(x,1);
                        lcd.print(" ");
                }
                else if(customkey != '*'){
                        master = master + customkey;
                        lcd.setCursor(x, 1);
                        lcd.print(customkey);
                        x++;
                }
                customkey = myKeypad.waitForKey();
        }
}
int checkpassword()                          //checks if password is correct or not
{
        if (edata.equals(master)){
                return 1;
        }
        else{
                return 0;
        }
}
int checksecurity()                          //checks entered security
{
        if (esecurity.equals(security)){
                return 1;
        }
        else{
                return 0;
        }
}
int checkotp()                               //checks OTP entered
{
        if (eotp.equals(otpstring)){
                return 1;
        }
        else{
                return 0;
        }
}
void allok()                                    //unlocks door
{
        digitalWrite(relay, HIGH);
        digitalWrite(green, HIGH);
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Door Unlocked");
        lcd.setCursor(0, 1);
        lcd.print("Welcome...");
        delay(4000);
        digitalWrite(relay, LOW);
        digitalWrite(green, LOW);
}
void sendotp()                                  //sends OTP
{
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Choose Person:");
        lcd.setCursor(0, 1);
        lcd.print("1-Sai,2-Kiran");
        customkey = myKeypad.waitForKey();
        while(customkey != '1' && customkey != '2'){
                customkey = myKeypad.waitForKey();
        }
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("OTP Sending...");
        x = random(1000,9999);
        otpstring = String(x);
        if(customkey == '1'){
        gsm1();
        }
        else if(customkey == '2'){
                gsm2();
        }
        delay(2000);
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("OTP Sent");
        delay(750);
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Enter OTP");
        return;
}
void gsm1()                                        //send otp to mobile 1
{
        mySerial.println("AT+CMGF=1");             //Sets GSM in Text Mode
        delay(1000);
        mySerial.println("AT+CMGS=\"+918106688767\"\r");    // mobile number
        delay(1000);
        mySerial.println("OTP - "+otpstring);         // The SMS text to send
        delay(100);
        mySerial.println((char)26);                // ASCII code of CTRL+Z
        delay(1000);
        Serial.println(otpstring);
}
void gsm2()                                                //sends OTP to mobile 2
{
        mySerial.println("AT+CMGF=1");
        delay(1000);
        mySerial.println("AT+CMGS=\"+918106896122\"\r");
        delay(1000);
        mySerial.println("OTP - "+otpstring);
        delay(100);
        mySerial.println((char)26);
        delay(1000);
        Serial.println(otpstring);
}
void gsmerror()                            //sends error notification
{
        mySerial.println("AT+CMGF=1");
        delay(1000);
        mySerial.println("AT+CMGS=\"+918106688767\"\r");
        delay(1000);
        mySerial.println("Wrong details entered.");
        delay(100);
        mySerial.println((char)26);
        delay(1000);
        Serial.println(otpstring);
}
```

CHAPTER 5 - RESULTS

We surveyed many smart door locking systems. We found that these locking products are expensive. Some of the implementations mentioned in the literature survey are very cost effective in implementation but do not provide multi user or multi-level functionalities. We identified these requirements and thought to develop a system which is cost effective in implementation and having more advanced features like multi user and multilevel. These features are the need of time and such functionalities will make the system more useful.

The GSM Based Digital Door Lock Security System was designed and implemented successfully and it looks like Figure 4.1 from front to the user. On basis of detailed analysis and trials, we could conclude that the system was stable and can be an emerging product in field of security systems for both residential and commercial applications.

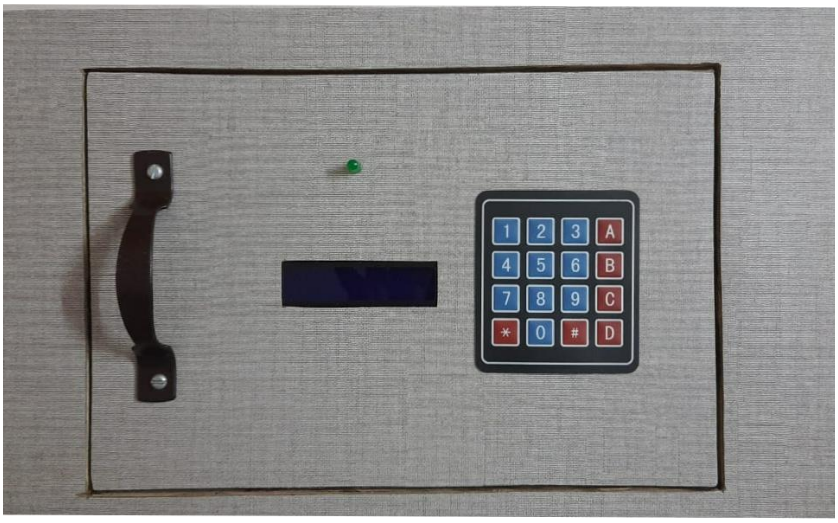


Figure 5.1 Front view of the project

The locking system developed has overcome the following problems

- ✓ Physical is not necessary
- ✓ If one mobile gets discharged or lost, other mobiles can be used.
- ✓ Cost is comparatively less than present digital locking systems.
- ✓ Password can be reset in case forgot without anyone’s help.

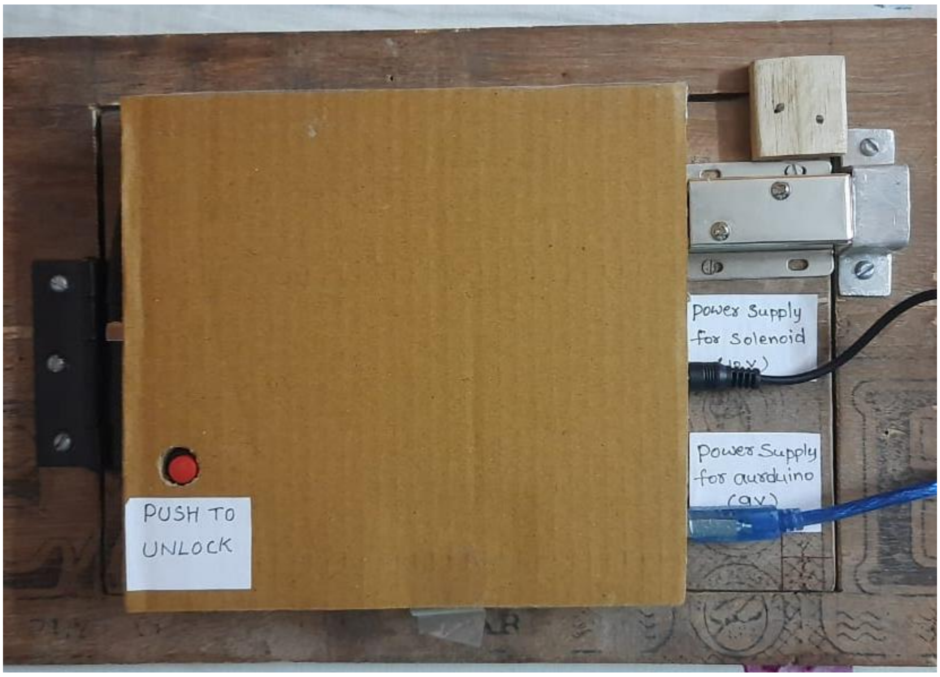
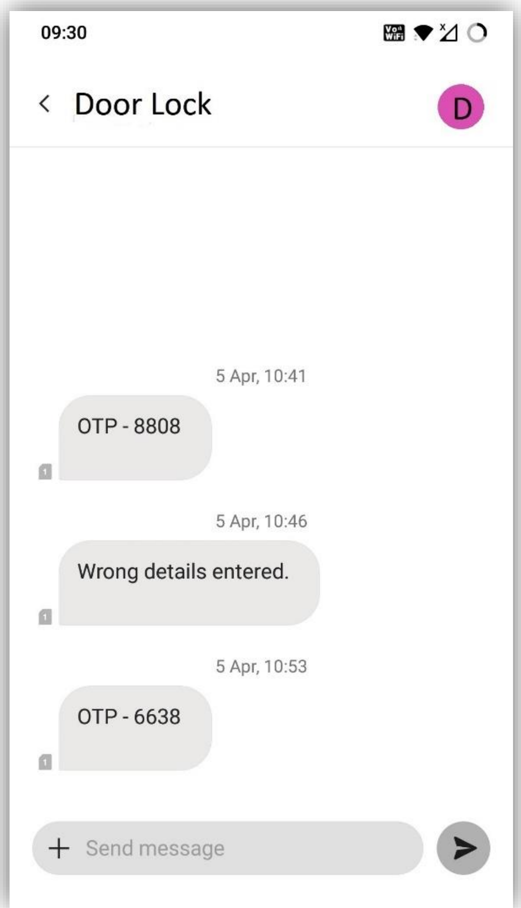


Figure 5.2 Back view of the system



5 Apr, 10:41

OTP - 8808

5 Apr, 10:46

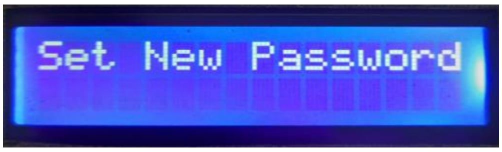
Wrong details entered.

5 Apr, 10:53

OTP - 6638

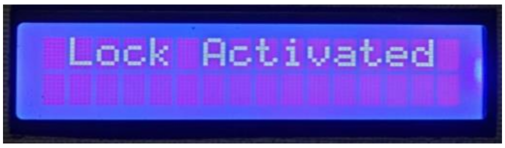
Screen 5.1 System sending OTP and notification to mobile

- Various displays in process of unlocking and resetting password



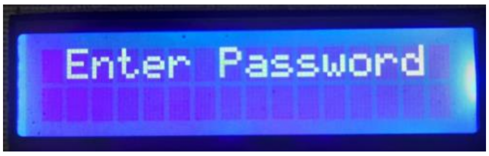
```
Set New Password
```

Figure 5.3 Set password on LCD



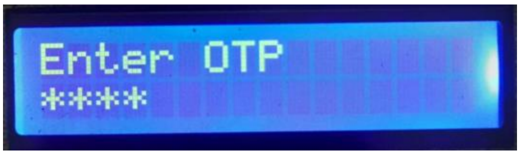
```
Lock Activated
```

Figure 5.4 LCD showing lock activated



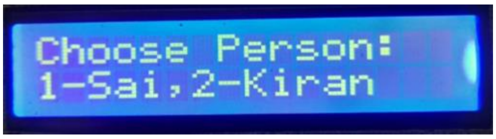
```
Enter Password
```

Figure 5.5 System waiting for password



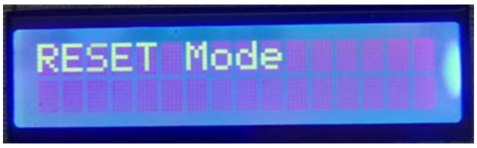
```
Enter OTP
****
```

Figure 5.6 System reading OTP



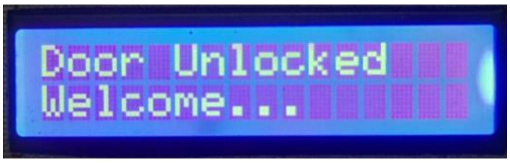
```
Choose Person:
1-Sai,2-Kiran
```

Figure 5.7 Model asking to choose person



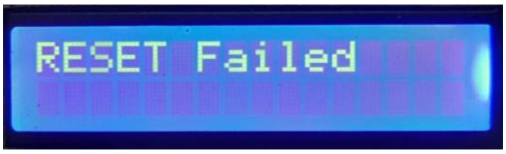
```
RESET Mode
```

Figure 5.8 Lock in Reset mode



```
Door Unlocked
Welcome...
```

Figure 5.9 Display when door unlocked



```
RESET Failed
```

Figure 5.10 LCD when reset failed

CHAPTER 6 - APPLICATIONS & ADVANTAGES

6.1 APPLICATIONS

- To improving security, this system can be employed in:
  - ✓ House locking system
  - ✓ Bank locking system
  - ✓ Jewelry shops
- It can be used at organizations to ensure authorized access to enter into a building or office even for restricted areas in military.
- Armament room or document rooms can be safe guarded with this technology.
- This system can be implemented as an alternate key in vehicles.

6.2 ADVANTAGES

- ✓ Increase Accessibility without Compromising Security.
- ✓ Physical key is not required.
- ✓ Alert message is sent to user when wrong details are entered.
- ✓ Security code is hidden.
- ✓ Easily available components are used.
- ✓ Power consumption is low.
- ✓ Very easy to use.
- ✓ Simplified Home Security.

6.3 DISADVANTAGES

- ○ The main disadvantage here is the GSM, since it needs to have network to send SMS. Also, sim needs to be recharged. But now-a-days multiple networks are introduced with good signal strength. So, signal strength can be checked and installed.

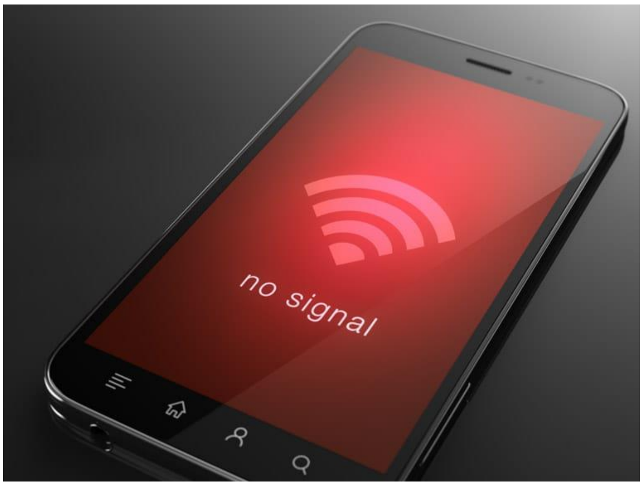


Figure 6.1 No signals in mobiles

CHAPTER 7 - CONCLUSION

The design and implementation of GSM based lock system is customizable and flexible. This door locking mechanism is comparatively cost-effective than the available lock systems in the traditional market. Our lock system has high accuracy rate and provides tighter security. In our country, private and government organizations are very much concerned about security. Many companies are interested in using this type of locking mechanism but the system which is available have very high installation cost. Due to this excessive cost, many small firms cannot afford such systems. Keeping the installation cost in mind a system that is affordable to both large and small firms is developed.

In present situation, there are possibilities to hack and unlock the smart locks. The proposed system can overcome the security issues faced in the present situation. The high-level security in the system can help the user for accurate security. The main reason for the proposed system is to secure the user living place, working place or to keep their valuable things, documents in a protected way. Hence this project can be understood by people and future work can be done.

Many times, we forgot to carry the key of our home. Sometimes we come out of our home and door latch closes by mistake. In these cases, it is really difficult to get inside the house. This project will help in keyless entry and at the same time will be more secure.

The “GSM Based Smart Door Locking System” is a modern successor of the conventional door locking system. This system is very cost effective and easy to install and is designed under different modes which makes it useful. This system is considerably easy to manage, more secure from hacking and easy circuitry which concludes the purpose of this project.

CHAPTER 8 - FUTURE SCOPE

- This system can be implemented in college premises. Now security manually checks for permission and leave the students. With this implemented faculty can directly give access to the right student.

- Use of camera can also be done for surveillance. By including camera we can see the live feed through mobile. We can use remote unlocking method to unlock the door from any place if anyone known comes to doorstep

- A rechargeable battery can be provided which can give power backup in case of power failure. Whenever power comes back the battery can be recharged again. This can be helpful if power cuts are more in installed area. Also battery size can be different based on the users interest

- To make it easy door can be opened with a DC motor but with that door can’t be kept unlocked as long as we need unless we use a button to close it.

- For further security, Biometric sensors can be used in place of password which can increase security level. But only some biometrics are efficient like retinal scanner or fingerprint.

REFERENCES:

[1]. A. Hemalatha, G. Gandhimathi "*RFID, Password and OTP based Door Lock System using 8051 Microcontroller*" CONFCALL – 2019 (Volume 7 – Issue 11), Publisher Name : IJERT

[2]. M Shanthini, G Vidya, R Arun "*IoT Enhanced Smart Door Locking System",* 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT).

[3]. D Aswini, R Rohindh, K S Manoj Ragavendhara, C S Mridula, *"Smart Door Locking System",* Advancements in Electrical Electronics Communication Computing and Automation (ICAECA) 2021 International Conference.

[4]. https://www.slideshare.net/aswin5432/smart-door-lock

[5]. https://create.arduino.cc/projecthub/muhammad-aqib/rfid-and-keypad-based-door-lock-using-arduino-89e1d5?ref=tag&ref_id=lock&offset=2