A project report on

AUTOMATIC DOOR LOCKING SYSTEM USING IOT WITH SMS ALERT

Submitted in partial fulfilment for the award of the degree of

Bachelor of Computer Application

By

G.K.LOSHMIN	**(18BCA0112)**
P.AARTHI	**(18BCA0095)**
R.JOTHIKA	**(18BCA0123)**

Under the guidance of

Prf. J. JABANJALIN HILDA

SCHOOL OF INFORMATION TECHNOLOGY

AND ENGINEERING

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

June, 2021

DECLARATION

We hereby declare that the project entitled “Automatic door locking system using IOT with SMS alert” submitted by us, for the award of the degree of *Bachelor of Technology in Bachelor of computer application* to VIT is a record of bonafide work carried out by us under the supervision of prf. Jabanjalin Hilda.

We further declare that the work reported in this has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Place: Vellore

Date:

Signature of the Candidate

G.K.Lakshmi

R. Jothi

P. Aarthi

CERTIFICATE

This is to certify that the project entitled Automatic door locking system using IOT with SMS alert" submitted by GK.LOSHMIN–18BCA0112, R.JOTHIKA-18BCA0113, P.AARTHI – 18BCA0095. School of Information Technology, VIT, Vellore, for the award of the degree of *Bachelor of computer application* is a record of bonafide work carried out by them under my supervision, as per the VIT code of academic and research ethics.

The contents of this report have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university. We fulfill the requirements and regulations of the University and in my opinion meet the necessary standards for submission.

Place: Vellore
Date:

Signature of the guide

Internal Examiner **External Examine**

Approved by

Head of the Department Programme

ACKNOWLEDGEMENT

I would like to express my intense gratitude to our esteemed Dean Dr.Balakrushna Tripath an Academic mentor and Head of department Dr Malaserene and my University, for their patient management, enthusiastic boosterism, helpful reviews and vast resources to manage the research work. I would also covet to thank our guide prf. J. Jabanjalin Hilda, who approved our project and dedicated her time towards it and advising us in processing our development on making this digital locking system analysis. Without her guidance, the project would not have been successful.

I would like to thank my Procter Mrs. Praba devi who supported us all the time, and never forget to boost our inner self-confidence which played a very important role in handling the failures, we endured on making.

Through the journey of making this computer science project gave me a colossal learning experience and I imprinted many personal qualities during this process like responsibility, punctuality, confidence and mainly killed my procrastination.

Last but not the least I am overwhelmed to shoot my beloved gratitude to my parents who also played a very immerse role in construction of my project. I am taking this opportunity to acknowledge their support and I wish that they keep supporting me like this in every prospect.

Executive Summary

Technology advancements have made the implementation of embedded systems within home appliances. A large number of electrical appliances are used in home to help us with various works. Most of these appliances work independently on their own. But the recent trend in making these appliances smart and connected to each other has further made it easier operating them. This Project explains various security issues in the existing home automation systems and proposes the use of fingerprint based security to improve home security. Implementation of this project is done by using Arduino as a controller to which the devices are directly interfaced

In the existing system, most doors are controlled by persons with the use of keys, security cards, password or pattern to open the door. The aim of this project is to help users for improvement of the door security. With the advancement in the technology, Wireless controlling technique is proposed with a fine combination of new technologies and embedded system

In the proposed system, we are introducing finger print module to access door lock. Here we have used GSM module, which is used to send message to user through GSM if any theft happens. This signal is then sent to the microcontroller. In this project microcontroller Arduino act as a master and the remaining acts as slaves. Information from the micro controller is displayed on the LCD. The lock device is connected to the circuit; door will be opened or closed depending on the command given. If any unauthorized people try to open the door it will display on LCD. GSM is used for the purpose of communication with the user by sending SMS

CONTENTS

LIST OF FIGURES:

LIST OF TABLES

LIST OF ABBRIVATIONS

Arduino IDE	Integrated Development Environment
Arduino UNO	One in Italian
USB	Universal serial Bus
STK	Sim Application Toolkit
FTDI	Future Technology Devices International
GSM	Global for Mobile Communication
ETSI	European Telecommunication Standard Institute
GPRS	General Packet Radio Service
EDGE	Enhanced Data Rates For Evolution
SMS	Short Message service
UMTS	Universal Mobile Telecommunication System
LTE	Long Term Evolution
FLASH	Free Electron Laser in Homburg
TTL	Technology Time To Live
UART	Universal Asynchronous Receiver Transmitter
LCD	Liquid Crystal Display
VDC	Volts of Direct Current
VCC	Voltage Common Collector
CCTV	Closed Circuit Television

Symbols and Notations

Common NC	Normally Closed
Common NO	Normally open
V	Voltage
DC	Direct Current
TX	Transmit
RX	Receive
GND	Short for Ground
SCL	Two lines to send and receive data(Serial Clock Pin)

1. INTRODUCTION

Every living being wishes to be safe whether it is a safety related to his belongings or safety of his own precious life. We have been taking several measures in order to attain it to live a worry-free life. In this project we propose a smart locking system which is designed to work based on the Internet of Things to prevent unauthorized access and trespassing. Normally the common targets where unauthorized access takes place are Banks, Financial organization, Government offices and organization, and shops. Such activities are performed with an intention of stealing money, or any important documents for personal gain. The main aim of our project is to provide a useful and a feasible solution to many of such issues. Fingerprint acknowledgment is one of the most secure systems in light of the fact that a fingerprint of one individual never coordinates with the others. Hence, unapproved access can be restricted by arranging a lock that stores the fingerprints of at least one approved individual and opens the lock when a match is found. Bio-measurements approval ends up being perhaps the best attribute considering the fact that the skin on our palms and soles shows a stream like case of edges on each fingerprint which is uncommon and invariable. This makes fingerprint a novel ID for every individual. With this idea, a plan and a model of fingerprint based entryway lock framework has been presented in this paper.

1.1 Objective

In this project we propose a smart locking system which is designed to work based on the Internet of Things to prevent unauthorized access and trespassing. Normally the common targets where unauthorized access takes place are Banks, Financial organization, Government offices and organization, and shops. Such activities are performed with an intention of stealing money, or any important documents for personal gain. The main aim of our project is to provide a useful and a feasible solution to many of such issues. Fingerprint acknowledgment is one of the most secure systems in light of the fact that a fingerprint of one individual never coordinates with the others. So, the main objective of this project is to implement a fingerprint based door locking system by using the GSM Module and to integrate the hardware and software in order to simulate the functions of the above system. The microcontroller based Door locking system is an access control system that allows only authorized persons to access a restricted area. The fingerprint is stored in the cloud so that we can change it any time. The system a sensor which is used to enter the fingerprint. A 16×2 LCD is also used to display the command like "welcome to home" if the fingerprint does not match it will display has unauthorized access. If the entered fingerprint is correct then the system opens the door by using solenoid lock. If the fingerprint is wrong then the door will remain closed and an SMS will be generated to detect an unauthorized entry of a person and sends alert message to the owner of the house.

1.2 Motivation

Nowadays, people are very afraid about the safety of their premises. For an example, a house without its owner is not safe enough to store valuable things or leave kids behind, because no safety procedures taken and the intruder take opportunity to break the simple locking system. To improve the standard of the locking system, this project was built upon various hardware and software. The main motivation of the project is to provide highly secured system with the help of finger print sensor. Fingerprint sensors provide almost 100% of accuracy during authentication. Once fingerprint captured, this digital data is analyzed to look for distinctive and unique fingerprint attributes. Fingerprint allow companies to replace passwords and security. Fingerprint sensors increase device and application-level security without overburdening the user with numerous credentials. Once fingerprint captured, this digital data is analyzed to look for distinctive and unique fingerprint attributes. Although password management comes free with devices and software systems, fingerprint authentication is an affordable solution that delivers greater security for any kind of secure access control.

1.2Background

Technological advancement has been on the rise since the past 2 centuries. Due to the rise of the rate of technological advancements, measures have to be taken to protect tangible assets that can be looted resulting in high expenses to the owner(s). 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/her confidential belongings manually. Instead, he/she finds an alternative solution which provides better, reliable and atomized security.

Many security systems including passwords, pins and even as simple as keys may be efficient means in a way but have their deficiencies. A power surge of the right current can damage the circuits thus causing it to malfunction and any computer professional can hack into passwords or pins and gain access. Keys are not configured to just a single person therefore once anybody else gets the keys, such a person automatically gets access to the door being locked. Hence the use of biometrics is seen as the next most proficient means of security.

Fingerprint recognition is one of the most secure systems because a fingerprint of one person never matches with others. Therefore, unauthorized access can be restricted by designing a lock that stores the fingerprints of one or more authorized users and unlock the system when a match is found. Bio-metrics authorization proves to be one of the best traits because the skin on our palms and soles exhibits a flow like pattern of ridges on each fingertip which is unique and immutable. This makes fingerprint a unique identification for everyone. The popularity and reliability on fingerprint scanner can be easily guessed from its use in recent hand-held devices like mobile phones and laptops

The following includes the background of this project using Arduino software

SOFTWARE DESCRIPTION

Arduino IDE 1.8.13

The open-source Arduino Software (IDE) makes it easy to write code and upload it to the board. This software can be used with any Arduino board.

Arduino IDE 2.0 beta (2.0.0-beta3) The new major release of the Arduino IDE is faster and even more powerful! In addition to a more modern editor and a more responsive interface it features auto completion, code navigation, and even a live debugger.

This software is still in beta status, which means that it’s almost complete but there might be minor issues. Help us test it and report your feedback in the forum!

2. PROJECT DESCRIPTION AND GOALS

The fingerprint sensor is mainly used for computer safety. Human fingerprints are extremely detailed and nearly unique. When the technology which can recognize and differentiate between fingerprints is deployed in securing access to a door way, you get a “Fingerprint Door Lock System”. The features of fingerprint sensor systems include faster speed, lower costs, as well as consistency. Using a fingerprint key, you gain the advantage of enhanced security while working from home, the office, or any other location. With the help of the software ARUDINO IDE with the implementation of code check whether it works or not.The digital and analog input/output pins equipped in this board can be interfaced to various expansion boards and other circuits. Serial communication interface is a feature in this board, including USB which will be used to load the programs from computer. We use LCD to display the limited set of output statements. At present we use mostly 16*2 and 16*4 which means 16 letter spaces with 2 lines and 16 letter spaces with 4 lines. The security door lock automation system promises a bold step to the future where mechanical door locks will be substituted by electronic door locks. The fingerprint sensor applications include mobile, lock, unlock, in the display, on screen, security systems, time attendance systems, door locks. A fingerprint sensor system is highly secure and comfortable.

GOALS:

- It provides more security compared to the currently used systems.
- It is easy to implement and easy to access by the user.
- It ensures the owner by the range of security provides
- Only authorized person can able to unlock the door
- The owner can be altered by sending SMS message to his sim card.
- It is easier to reach the place at the time of robbery attempt.

3. LITERATURE SURVEY

No	TITLE AND YEAR	ALGORITHIM	ADVANTAGES	DISADVANTAGES
1	**IOT ENHANCED SMART DOOR LOCKING SYSTEM (2020) [1]**	LDR sensor, Ultrasonic sensor, servo motor, and laser module, Bluetooth application.	This Bluetooth controls the door and Arduino UNO processes data at a particular place and the distance from all these sensors continuously.	The relay usually requires a high voltage to operate and current which cannot be given from the micro controller.
2	**DESIGN, CONSTRUCTION AND PERFORMANCE EVALUTAION OF AN AUTOMATED DOOR LOCK USNG BIOMETRIC SECURITY WITH PHONE TEXT ALERT NOTIFICATION (2020)[2]**	A fingerprint sensor, SIM, LCD screen	We can connect the system with an Integrated Power System (IPS) or add rechargeable batteries to the seestem.	When we use pattern password some times, unauthorized person can access and unlocking the door.
3	**DESIGN IMPLEMENTATION OF INTRUDER DETECTOR SYSTEM WITH SMS AERT (2020)[3]**	ATmega8 micro controller, GSM module, SIM Light dependent resistor, Micro controller unit.	Mmicro controller is used for this research. The flexibility of the algorithm of the system can be increased by introducing more sensors.	The system enables to differentiate between a human intruder and a household pet by computer vision technology to minimize false positives and negatives to the system.
4	**Smart Anti-Theft Door locking System (2019) [4]**	Viola Jones, Local Binary Pattern, Grey scale image, Principal Component Analysis	System captured face using a motion detector. Motion Detection means keeping a security and the detection appliance	This system would be expensive security systems being used in the present days.

			at homes, buildings and also for surveillance.	
5	**Design and Implementation of Automated Door Accessing System with Face Recognition (2018)[5]**	PCA approach, Fast based principal component analysis (FBPCA) approach, Web camera	The system which makes the cost effective. SMS operated home security system has been designed and tested with the GSM network.	Reliability and robustness in both the recognition and detection process.
6	**Fingerprint for Automatic Door Integrated with Absence and User Accesss (2016) [6]**	Fingerprint sensor, button, keypad 4x4, LCD, Relay Channel 1, and Electric Door Arduino Mega 2560, C # language	The integrated fingerprint database controls the use of the room and attendance, so that the process becomes easier and faster.	It does not have intrusion detection.
7	**Enhanced Security Methods of Door Locking Based Fingerprint (January 2020)[7]**	Fingerprint scanner R305 interfaced Arduino microcontroller-ATMEGA328P	The proposed door lock security system is can be used at homes, offices, banks, hospitals, and in other governmental and private sectors.	When homeowners lose the key and have no alternative key, they should wait for long hours for a technician to come, otherwise they should break the door.
8	**Automatic Door Opening System (March 2019)[8]**	Raspberry Pi Model B board, SMS Gateway	This system plays a major role in helping reduce the work by using Raspberry pi 3, especially for children, old aged people and physically challenged.	Multiple micro controllers are used. Usage of ZigBee based network to communicate with the base station is limited to 100-150 meters long distance only.
9	**Automatic Door Access System Using Face Recognition (6 June 2015)[9]**	PCA, Viola-Jones Face Detection Method	Face recognition does not require to be touched with any hardware.	The system has limitations in head orientation. Because, this detection method can detect only face images for frontal view correctly.

10	**An IoT based Automated Door Accessing System for Visually Impaired People (2019)[10]**	Audio alert, Automated door control through voice command	It supports automatic door lock and unlock from a remote location via internet and sending the user an email.	The existing systems lack audio alert feature. These systems also missed to detect potential threats (such as visitor carrying unsafe objects) or force entry into the room.
11	**Design of Smart Lock System for Doors with Special Features using Bluetooth Technology (2018)[11]**	Bluetooth Signal Area, Pairing and Link Key Generation	SLS design provides fingerprint feature for smartphone users or other application with fingerprint detector.	If the user of access is not located on the validation area, the door will be locked automatically.
12	**IoT Open-Source and AI based Automatic Door Lock Access Control Solution (2017)[12]**	Camera based VLC System, Radio frequency identification (RFID)	The access control systems (ACS) designed to provide safe and secure access in the building facilities for authorized individuals like homes, offices, factories, facility server rooms, airports, defense zone, banks.	The cost of the access control system installation is high. The network interface has the weakness with access distance, security and network access efficiency issue.
13	**IOT Enabled Door Lock System (2019)[13]**	GPS based smart door lock, GPIO-B PORT CONFIGURATION IN STM32L100 MICROCONTROLLER	Objects within IoT network can also communicate using various communication technologies such as WIFI, Bluetooth, near field communication, and many more.	Enhancing home security using smart home can be done in a number of ways, including but not limited to installation of smart, customized door lock.

14	**SHORT MESSAGE SERVICE (SMS) ALERT INTELLIGENT SECURITY DOOR SYSTEM (2017)[14]**	Start. Establish link with GSM modem and EEPROM. Enter access code. Is password correct? If Yes. Grant access. 10sec delay. Close door. .	The SMS alert intelligent security door system has been satisfactorily proved to be a reasonable advancement in access control and door security system technology. This gave the opportunity for code debugging to be fast and at no cost.	Control unit consists of a read only memory (ROM) in which the control program is burnt into the Response Unit and is the GSM module and an electric motor interfaced to the microcontroller unit through a DB9 connector and transistor.
15	**Security System U sing Biometric Technology: design and Implementation of Voice Recognition System (VRS) (2008)[15]**	MATLAB (SIMULINK) function blocks, microcontroller, transistor, capacitor, resistor, voice recognition system (VRS) oscillator, Light Emitting Diode (LED)	The system is proven to provide medium security access control and also has an adjustable security. The technology helps business and governments to fight identity theft and fraud, secure transactions, protect confidential information, reduce costs and enhance levels of service.	One reason is not as accurate as other biometric technologies due to the tendency to have a high false reject rate because of background noise and other variables.
16	**Smart Lock Controlled using Voice Call (2018) [16]**	Begin. Call the lock. Lock receives the call ID. Is Caller ID a registered number if yes Check current status of lock or else if No Alert the user. In state of YES Check current status of lock in LOCKED: request PIN via SMS UNLOCKED: lock the door	The proposed system offers a longer geographical range when compared to earlier Smart Lock Systems controlled through Bluetooth, Mobile Apps, etc. It offers an easy-to-use interface and eliminates the requirement of Smartphone.	Smartphones only can be used so that it will track with http. Though the idea serves the purpose of security, but it would be quite annoying to hear a buzzer go on for every 30 seconds.
17	**Smart Door Locking System using IoT [1] (2020)[17]**	Create a string variable. Servo library is added. Call the function and set the default band width	Security, Usability and Inaccessible. Fingerprint of each	Without the use of smartphones, this device can't able to work because it may loss it's

		of 9600. Create loop function. Store the Results in read string. Use if condition the string is right opens the door else it is locked.	person is unique with the usage of a biometric lock. .	connectivity and takes time to debug the error.
18	**Iopt based facial recognition door access control home security system using Raspberry pi (2020)[18]**	Face recognition using Raspberry Pi, it helps to resolve the limitation of PC such as its weight, size high power consumption Raspberry Pi is a device that can divide the software part into three parts which are recording images, training and face recognition.	Best security device using IoT shows the tested image with positive and negative results for authorized and unknown. Real-time face recognition is performed using web camera. .	Due to the module used which is Raspberry Pi 3, the processing time of the coding took a long time so process the image taken and take action. By using another better module, this project can be improved greatly.
19	**A Prototype Model of an IoT-based Door System using Double-access Fingerprint Technique (2020) [19]**	Start. Include serial input from library. Add input whatever we use. Get data from finger print. Give some delays for printing information about security process. Output of finger print get using loop whenever get input then realize the process. Use templates for displaying details. Stop.	This paper presents a double authentication IoT security door technique access to both the users and the administrators. Storage, comparison, memory check, image (prints) retrieval and prints deletion The very fast process of converting the finger image (print) scanned to the 562 bytes data is done each time a finger is placed on it for access.	High cost of real-life implementation. One of the major challenges faced during the development process was memory management, as an Arduino has a very low memory level connection to the internet is bad, it was unable to find match on the webserver.
20	**Development of a Lock Biometric Authentication System for a Battery Powered Locking Device (2021)[20]**	Start. Button activation. Single click if yes. Authenticate user and checks fingerprint. Authorization then lock actuation else result the user again finger print. Authorization again reset user and confirm with finger print registration.	The system can be placed in an enclosure and implemented for the use of housing, vehicles or any commercial building security. The system will sustain to work longer hours in an inactive state, where the state of the	Highly cost. It was found that the device is able to match a fingerprint in less than 1s for up to 50 registered fingerprints

		End.	microprocessor is idle	

4. Technical Specification

4.1Hardware Requirements

ARDUINO UNO The Arduino Uno is an open-source microcontroller board based on the Microchip ATmega328P microcontroller and developed by Arduino.cc. The board is equipped with sets of digital and analogue input/output (I/O) pins that may be interfaced to various expansion boards(shields) and other circuits. The board has 14 Digital pins, 6 Analog pins, and programmable with the Arduino IDE (Integrated Development Environment) via a type B USB cable. 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 also similar to the Arduino Nano and Leonardo. The hardware reference design is distributed under a Creative Commons Attribution Share-Alike 2.5 license and is available on the Arduino website. Layout and production files for some versions of the hardware are also available.

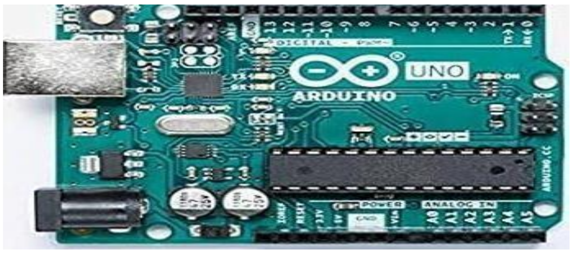


Figure 4.1 Arduino UNO

Figure 4.1. Arduino Uno The word "uno" means "one" in Italian and was chosen to mark the initial release of the Arduino Software. The Uno board is the first in a series of USB-based Arduino boards, and it and version 1.0 of the Arduino IDE were the reference versions of Arduino, now evolved to newer releases. The ATmega328 on the board comes pre-programmed with a bootloader that allows uploading new code to it without the use of an external hardware programmer. While the Fig.1 communicates using the original STK500 protocol, it differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it uses the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to- serial converter.

4.2 GSM MODULE

The Global System for Mobile Communications (GSM) is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second- 8 | P a g e generation (2G)digital cellular networks used by mobile devices such as mobile phones and tablets. It was first deployed in Finland in December 1991.By the mid-2010s, it became a global standard for mobile communications achieving over 90% market share, and operating in over 193 countries and territories.

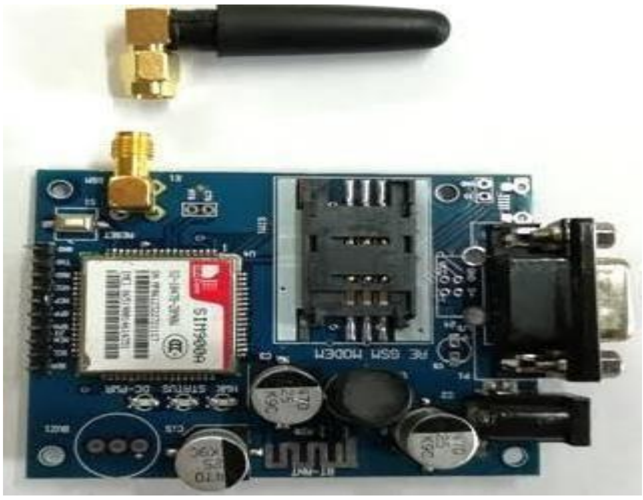


Figure 4.2 GSM Module

2G networks developed as a replacement for first generation (1G) analogue cellular networks. The GSM standard originally described a digital, circuit-switched network optimized for full duplex voice telephony. This expanded over time to include data communications, first by circuit-switched transport, then by packet data transport via General Packet Radio Service (GPRS), and Enhanced Data Rates for GSM Evolution (EDGE). Subsequently, the 3GPP developed third-generation (3G) UMTS standards, followed by fourth-generation (4G) LTE Advanced standards, which do not form part of the ETSI GSM standard. "GSM" is a trade mark owned by the GSM Association. It may also refer to the (initially) most common voice codec used, Full Rate.

4.3 FINGER PRINT SENSOR

Fingerprint sensor modules, like the one in the following figure, made fingerprint recognition more accessible and easier to add to your projects. This means that is is super easy to make fingerprint collection, registration, comparison and search. These modules come with FLASH memory to store the fingerprints and work with any microcontroller or system with TTL serial. These modules can be added to security systems, door locks, time attendance systems, and much more

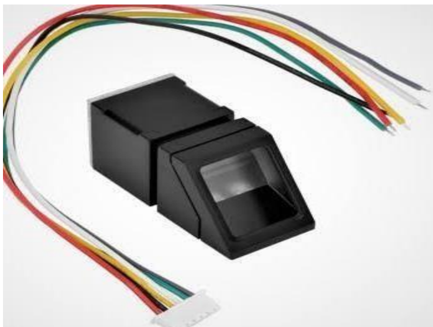


Figure 4.3 Finger print sensor

SPECIFICTIONS:

Here’s the specifications of the fingerprint sensor module we’re using (you should check your sensor datasheet or the specifications provided by your supplier – they shouldn’t be much different than these):

- Voltage supply: DC 3.6 to 6.0V
- Current supply: <120mA
- Backlight color: green
- Interface: UART
- Bad rate: 9600

Safety level: five (from low to high: 1,2,3,4,5) False
Accept Rate (FAR): <0.001% (security level3) False
Reject Rate (FRR): <0.1% (security level) Able to store
127 different fingerprints

The fingerprint sensor module used in this project came with really thin wires, so soldering breadboard-friendly wires was needed. We recommend using different colors according to the pin function.

4.4LCD 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. These displays are mainly preferred for multi-segment light emitting diodes and seven segments. The main benefits of using this module are inexpensive; simply programmable, animations, and there are no limitations for displaying custom characters, special and even animations, etc.

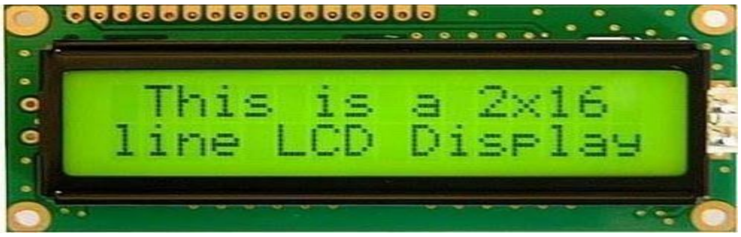


Figure 4.4 LCD Display

FEATURES OF LCD DISPLAY

- 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

4.5 12v SOLENOID LOCK 12V

Solenoid lock has a slug with a slanted cut and a good mounting bracket. It's basically an electronic lock, designed for a basic cabinet, safe or door. When 9-12VDC is applied, the slug pulls in so it doesn't stick out and the door can be opened. It does not use any power in this state. It is very easy to install for automatic door lock systems like electric door lock with the mounting board. This solenoid in particular is nice and strong.

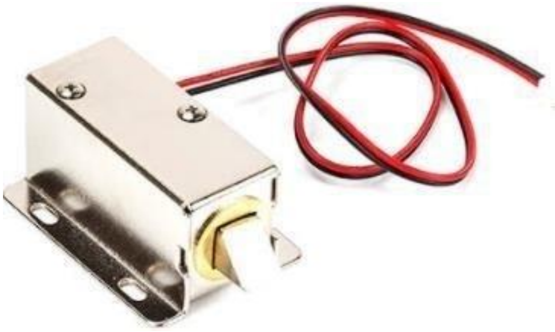


Figure 4.5 Solenoid lock

4.6-volt RELAY

Relays are most commonly used switching device in electronics. Let us learn how to use one in our circuits based on the requirement of our project. Before we proceed with the circuit to drive the relay, we have to consider two important parameters of the relay. Once is the Trigger Voltage; this is the voltage required to turn on the relay that is to change the contact from Common->NC to Common->NO. Our relay here has 5Vtrigger voltage, but you can also find relays of values 3V, 6V and even 12V so select one based on the available voltage in your project. The other parameter is your Load Voltage & Current, this is the amount of voltage or current that the NC, NO or Common terminal of the relay could withstand, in our case for DC it is maximum of 30V and 10A. Make sure the load you are using falls into this range.

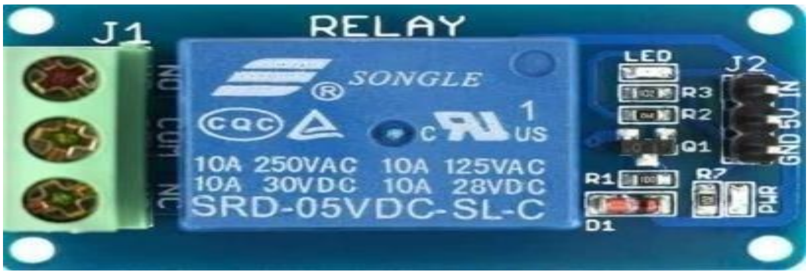


Figure 4.6 5 volt Relay

Features of 5-Pin 5V Relay:

- Trigger Voltage (Voltage across coil): 5V DC
- Trigger Current (Nominal current): 70mA
- Maximum AC load current: 10A @ 250/125V AC
- Maximum DC load current: 10A @ 30/28V DC
- Compact 5-pin configuration with plastic molding
- Operating time: 10msec Release time: 5msec
- Maximum switching: 300 operating/minute (mechanically)

4.7 PLUG SOCKET

The female connector is generally a receptacle that receives and holds the male connector. Sometimes the terms plug and socket or jack are used, particularly in reference to electrical connectors.

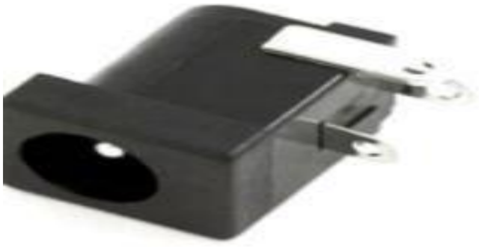


Figure 4.7 Plug socket

4.8 JUMPER WIRES:

Jumper wires are used for making connections between items on your breadboard and your Arduino’s header pins. Use them to wire up all your circuits

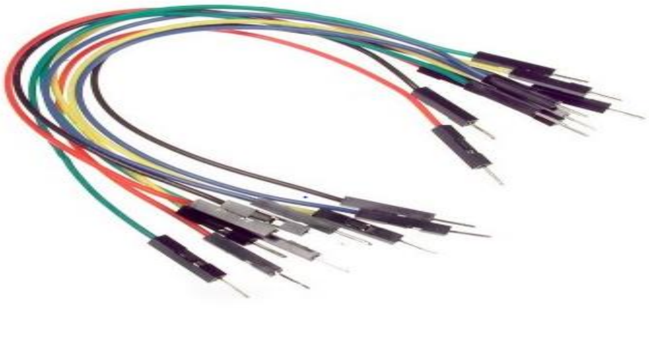


Figure 4.8 jumper wires

4.8 SOFTWARE REQUIREMENTS:

The **Arduino Integrated Development Environment (IDE)** is a -crosslink application (for Windows, macho’s, Linux) that is written in functions from C and C++ It is used to write and upload programs to Arduino compatible boards, but also, with the help of third-party cores, other vendor development boards.

The source code for the IDE is released under the GNU General Public License, version 2. The Arduino IDE supports the languages C and C++ using special rules of code structuring The Arduino IDE supplies a software library from the Wiring project, which provides many common input and output procedures. User-written code only requires two basic functions, for starting the sketch and the main program loop, that are compiled and linked with a program stub *main()* into an executable cyclic executive program with the GNU toolchain, also included with the IDE distribution. The Arduino IDE employs the program *argued* to convert the executable code into a text file in hexadecimal encoding that is loaded into the Arduino board by a loader program in the board's firmware. By default, avrdude is used as the uploading tool to flash the user code onto official Arduino boards.

Arduino IDE is a derivative of the Processing IDE, however as of version 2.0, the Processing IDE will be replaced with the Visual Studio Code-based Eclipse Theia IDE framework.

With the rising popularity of Arduino as a software platform, other vendors started to implement custom open source compilers and tools (cores) that can build and upload sketches to other microcontrollers that are not supported by Arduino's official line of microcontrollers.

Cloud storage:

Node MCU connects the data with Cloud and stored in drive. In the data, user admin can able to see data of the Person who’s open the door with time and date. This is the major advantages of the project.

5. TECHNICAL SPECIFICATION

5.1 PIN CONFIGURATION:

The following table shows how to wire the Fingerprint sensor to the Arduino

Fingerprint Sensor	Arduino
VCC	5V(IT also works with 3.3 v)
TX	RX (digital pin 2, software serial)
RX	TX (digital pin 3, software serial)
GND	GND

Table 5.1 Connecting wires for Fingerprint to Arduino

The following table shows how to wire the GSM Module to the Arduino.

GSM MODULE	ARDUINO
VCC	5V
TX	RX(digitally pin 4, software serial)
RX	TX(digital pin 5, software serial)
GND	GND

Table 5.2 Connecting for Wire GSM Module to Arduino

The following table shows how to wire the Arduino UNO to the 16X2 LCD Display

ARDUINO UNO	16X2 LCD DISPLAY
3.3V	VCC
GND	GND
Analog A5	SCL

Table 5.3 Connecting for Wire Arduino UNO to LCD Display

5. DESIGN APPROACH AND DETAILS

5.1System architecture

The design of the software and architecture diagram as shown in Figure. 2. In this design shows the complete diagram and connection for the project. All hardware requirements connected with the Arduino UNO micro-controller. The enrolled finger prints are stored in Arduino Board. Then check the validation through the finger print and stored in cloud of drive storage

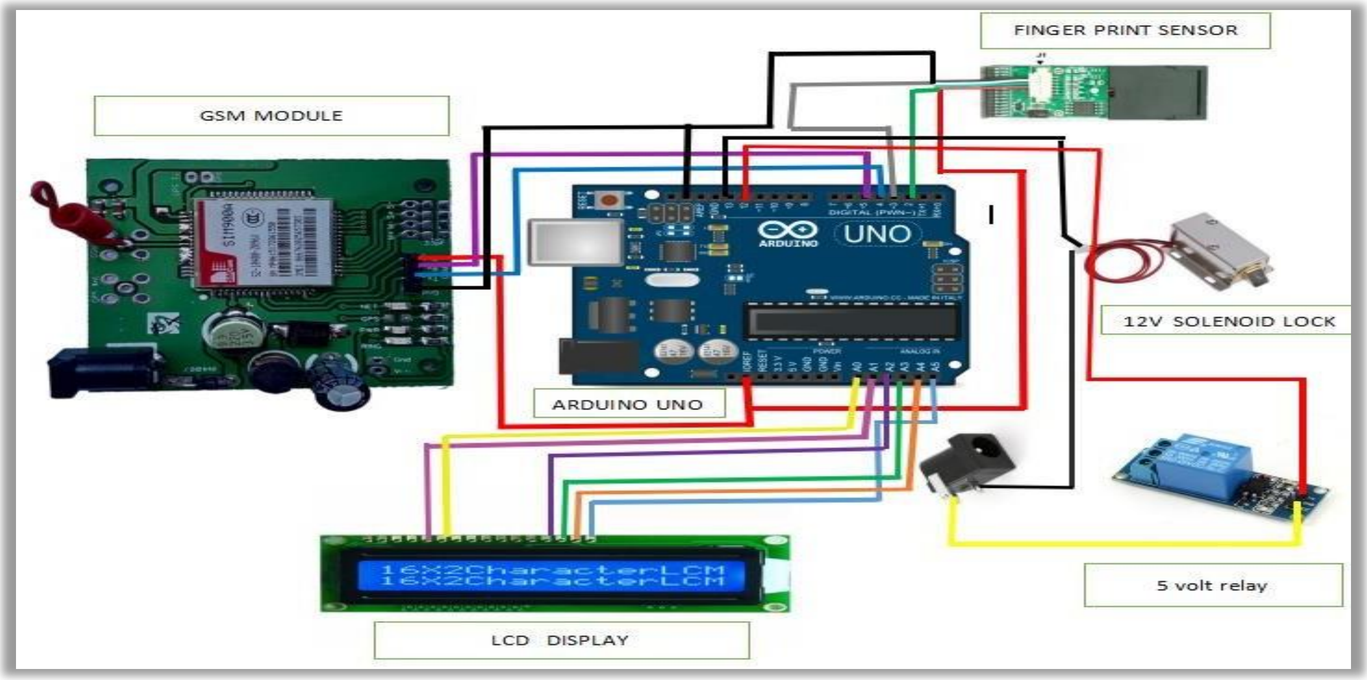


Figure 5.1 System Architecture

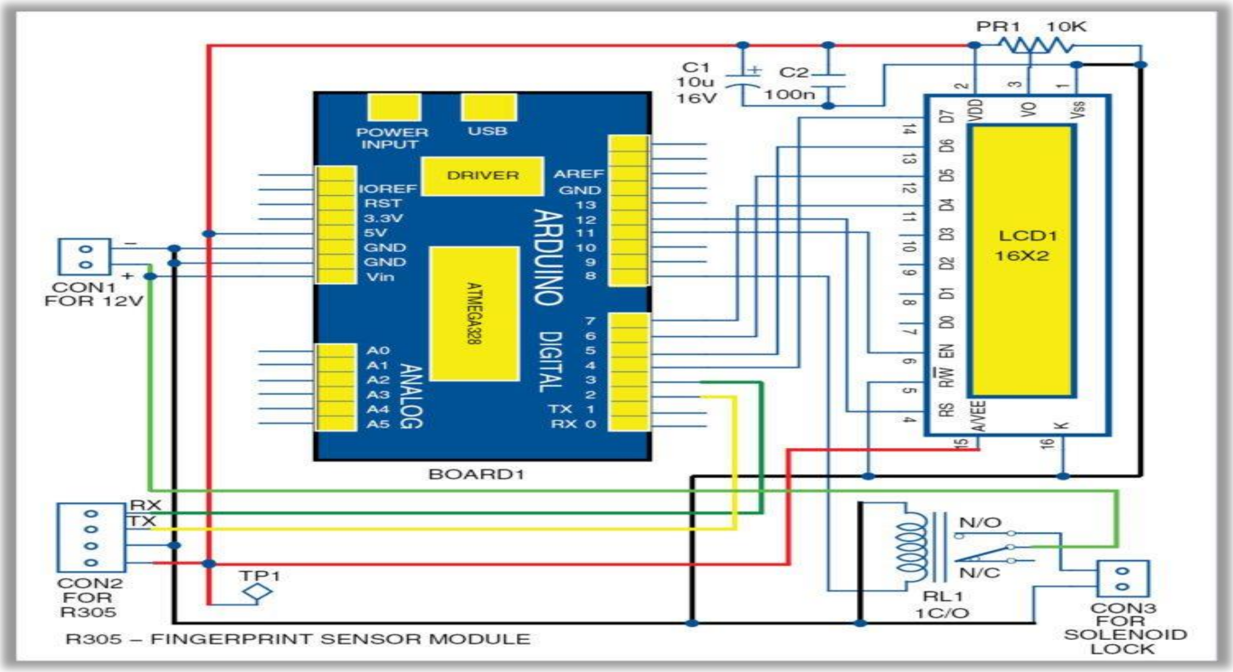


Figure 5.1.1 Circuit diagram for fingerprint door locking system

5.1.1 Circuit and working

The circuit shown in Fig 5.2 operates using a 12V power supply. An Arduino microcontroller (MCU) requires only 5V but the solenoid electric lock requires 12V. As Arduino Uno has an inbuilt 5V voltage regulator, a common 12V supply can be used for the whole system.

The brain of the circuit is Arduino Uno MCU board (BOARD1). It is based on ATmega328/ATmega328P and has 14 digital input/output (I/O) pins, six analogue inputs, 32k flash memory, 16MHz crystal oscillator, a USB connection, power jack, ICSP header and reset button, among others. It can be programmed using Arduino IDE software.

Fingerprint sensor module R305 (connected across CON2) has UART interface with direct connections to the MCU or to the PC through USB serial adaptor. The user can store fingerprint data in the module and configure it in 1:1 or 1:N mode for identification. Pins TX and RX of R305 sensor are connected to Arduino digital pins 2 and 3, which are used for serial communication.

The LCD display (LCD1) is used to display messages during action. Here, a 16×2 display is used; each character is made of 5×7 dot-matrix. Pins 3, 4, 5 and 6 of the LCD are the control lines connected to pre-set (PR1) output, pin 12 (Arduino),

GND and pin 11 (Arduino). Pins 11, 12, 13 and 14 are data pins of the LCD that are connected to pins 7, 6, 5 and 4 of Arduino, respectively. Pre-set PR1 is used to adjust the contrast of the LCD display.

An electronic door-lock solenoid (connected across connector CON3) is basically an electromagnet made of a big coil of copper wire with an armature (slug of metal) in the middle. When the coil is energised, the slug is pulled into the centre of the coil. This allows the solenoid to move to one end

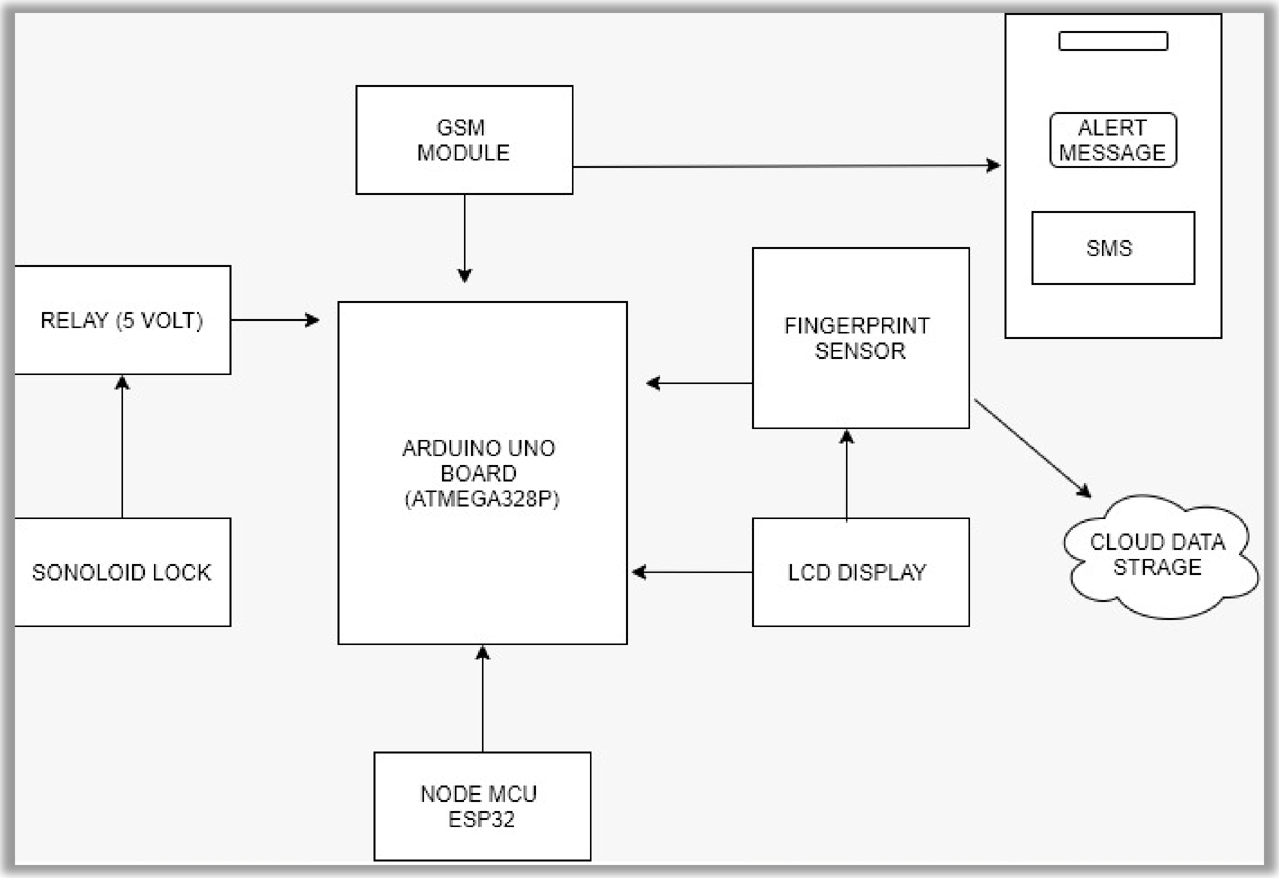


Figure 5.1.2 Overall block diagram for automatic door locking system

Fig 5.1.2 Show the Diagram of the implementation work are included in all hardware requirements that are used to complete the security task .Arduino UNO is a main part of the project. It act as a main role for the security. All other hardware requirements are depends on the Arduino UNO Board. Remaining requirements are all connected with Arduino Board. The finger print data are stored in cloud computing. Each and every requirements are made a major role in a different way to provide a enough security protections and all these tools are work together under the micro-controller.

5.1.3 UML Diagram

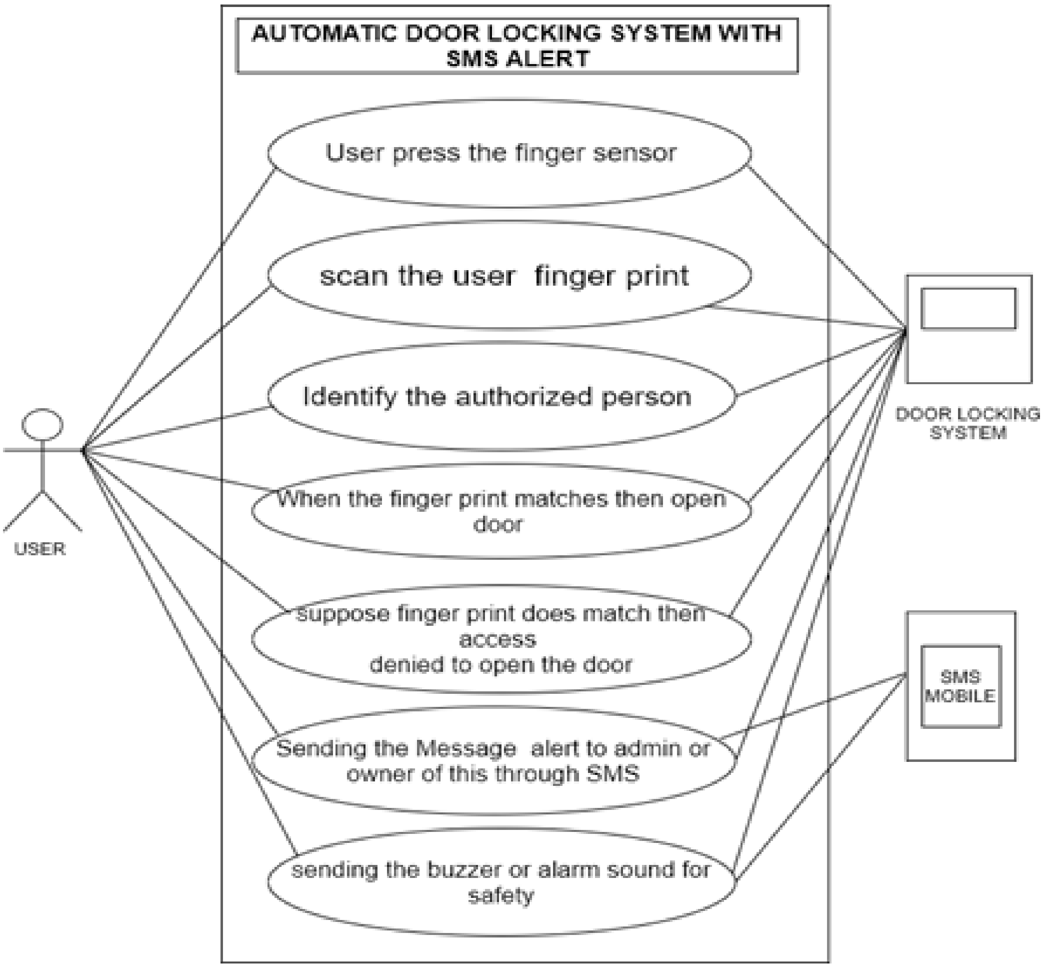

AUTOMATIC DOOR LOCKING SYSTEM WITH SMS ALERT
User press the finger sensor
scan the user finger print
Identify the authorized person
When the finger print matches then open door
suppose finger print does match then access denied to open the door
Sending the Message alert to admin or owner of this through SMS
sending the buzzer or alarm sound for safety
USER
DOOR LOCKING SYSTEM
SMS MOBILE

Figure 5.1.3 USE CASE Diagram for automatic door locking system

Figure:5.1.3 give us a detailed outlook on the entire project . To shows a complete Process of the security system. In the Use-case diagram. Step by step process to explained validation of fingerprint sensor. When the system is powered on, the sensor and Arduino board activated. Once, the user place the finger for the validate. When its matches to stored finger then it will display message on LCD as “Door open welcome home”. It does not matches with enrol finger then it shows the message as “Not valid finger print” then, It will send a SMS message to particular register mobile through the GSM module.

5.2 CODES AND STANDARDS

5.2.1 ACCURACY [FOR EXAMPLE][4]

Accuracy test Accuracy test is performed to observe the security level of the fingerprint scanner. Figure 5.2.1 shows the result of the accuracy test based on the confidence level. The test was done on five individual with four thumbprints from each and one of them. The fingers scanned were, left and right thumbprint and also left and right index finger. From the result below, it shows that finger with the most accurate result is left thumbprint with the percentage of 70%, followed by right thumbprint, right index finger and left index finger with the accuracy of 67.2%, 41.4% and 30% respectively

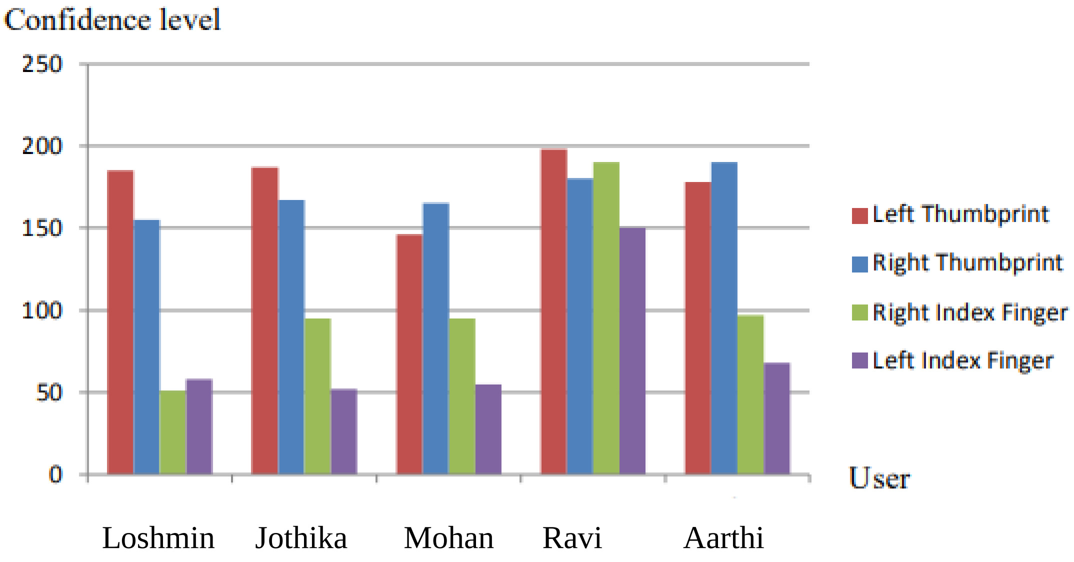


Figure 5.2.1 Accuracy level of fingerprint[4]

1. Comparison Differing from Automatic door locking system with SMS alert.

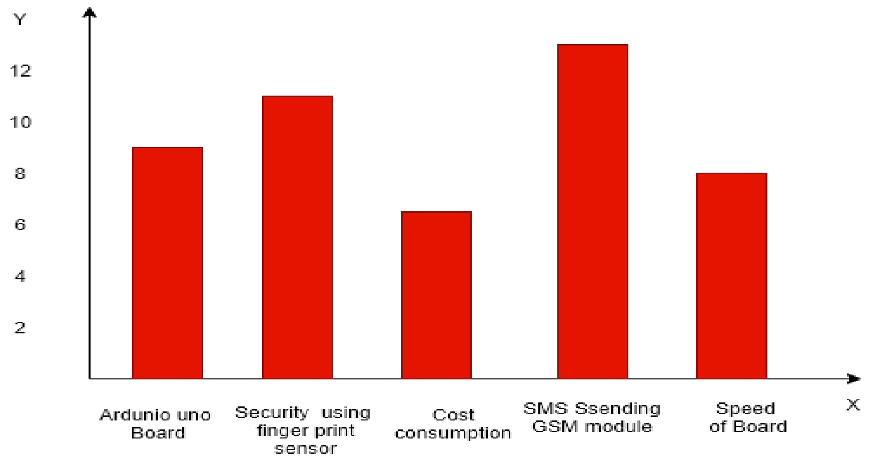


Figure Graph 5.2.2 AUTOMATION DOOR LOCKING SYSTEM USING SMS ALERT

With Arduino Board

Comparison graph represents different modes of security system for door locking

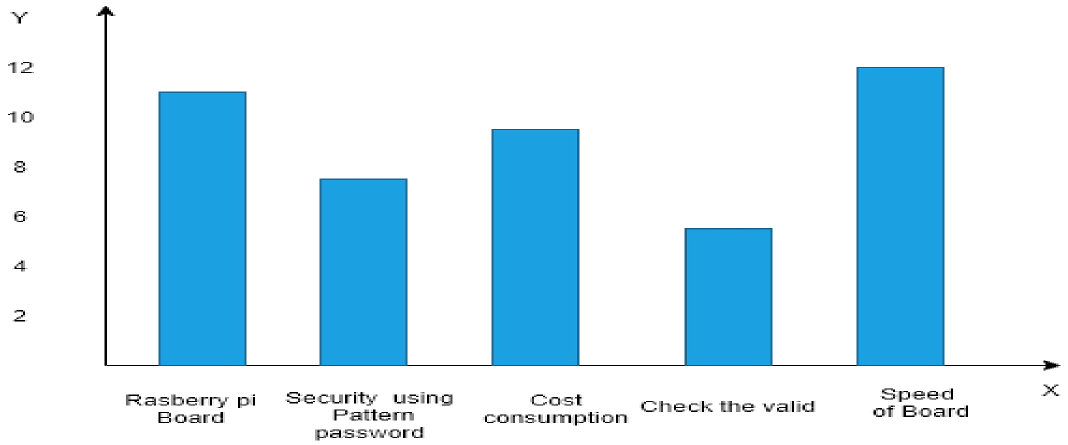


Figure Graph 5.2.3 Compared report Security method of door locking system

In the door locking system we use the two different codes for the project. One is used to store and enrol the finger print and saved in the Arduino board. Another code is used to deduct and check the validity of the fingerprint and also modification code is there to delete any finger print. They validity data are stored in cloud. Arduino board have a 127 fingerprint stored data to save the enrol fingers. In figure.4.1 For this project , The micro-controller of Arduino UNO used a C programme.

5.2.4 CODE

```
#include
<Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
SoftwareSerial mySerial(2, 3);
Adafruit_Fingerprint finger =
Adafruit_Fingerprint(&mySerial); uint8_t id;
void setup()
{
Serial.begin(9600);
if (finger.verifyPassword())
{ Serial.println("Found fingerprint sensor!");
} else {
Serial.println("Did not find fingerprint sensor
:("); while (1) { delay(1); }
}
```

```
while (!Serial);
delay(100);
  Serial.println("\n\nFingerprint sensor enrollment");

  // set the data rate for the sensor serial port
  finger.begin(57600);

  if (finger.verifyPassword())
  { Serial.println("Found fingerprint sensor!");
  } else {
  Serial.println("Did not find fingerprint sensor
  :("); while (1) { delay(1); }
  }
  }

  uint8_t readnumber(void)
  {uint8_t num = 0;

  while (num == 0) {
  while (! Serial.available());
  num = Serial.parseInt();
  }
  return num;
  }

  void loop() // program wil repeat this part (loop here)
```

```
{
Serial.println("Ready to enroll a fingerprint!");
Serial.println("Please type in the ID # (from 1 to 127) you want to save this finger
as…"); id = readnumber();
if (id == 0) {// ID #0 not allowed, try
again! return;
}
Serial.print("Enrolling ID
#"); Serial.println(id);

while (! getFingerprintEnroll() );
}

uint8_t getFingerprintEnroll() {

int p = -1;
Serial.print("Waiting for valid finger to enroll as #");
Serial.println(id); while (p != FINGERPRINT_OK) {
p = finger.getImage();
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image taken");
break;
case FINGERPRINT_NOFINGER:
Serial.println(".")
; break;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
break;
case FINGERPRINT_IMAGEFAIL:
Serial.println("Imaging
error"); break;
default:
Serial.println("Unknown error");
break;
}
}

// OK success!

P=finger.image2Tz(1);
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image converted");
break;
case FINGERPRINT_IMAGEMESS:
Serial.println("Image too messy");
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
return p;
case FINGERPRINT_FEATUREFAIL:
```

```
Serial.println("Could not find fingerprint features");
return p;
case FINGERPRINT_INVALIDIMAGE:
Serial.println("Could not find fingerprint features");
return p;
default:
Serial.println("Unknown error");
return p;
}

Serial.println("Remove
finger"); delay(2000);
p = 0;
while (p != FINGERPRINT_NOFINGER) {
p = finger.getImage();
}
Serial.print("ID");
Serial.println(id); p = -1;
Serial.println("Place same finger
again"); while (p !=
FINGERPRINT_OK) {
p = finger.getImage();
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image taken");
break;
case FINGERPRINT_NOFINGER:
```

```
Serial.print(".");
break;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
break;
case FINGERPRINT_IMAGEFAIL:
Serial.println("Imaging
error"); break;
default:
Serial.println("Unknown error");
break;
}
}

// OK success!

p =
finger.image2Tz(2);
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image converted");
break;
case FINGERPRINT_IMAGEMESS:
Serial.println("Image too messy");
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
```

```
return p;
case FINGERPRINT_FEATUREFAIL:
Serial.println("Could not find fingerprint features");
return p;
case FINGERPRINT_INVALIDIMAGE:
Serial.println("Could not find fingerprint features");
return p;
default:
Serial.println("Unknown error");
return p;
}

// OK converted!
Serial.print("Creating model for #"); Serial.println(id);

p = finger.createModel();
if (p == FINGERPRINT_OK) {
Serial.println("Prints matched!");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
Serial.println("Communication error");
return p;
} else if (p == FINGERPRINT_ENROLLMISMATCH) {
Serial.println("Fingerprints did not match");
return p;
} else {
Serial.println("Unknown error");
```

```
return p;

}


Serial.print("ID ");

Serial.println(id); p =

finger.storeModel(id);

if (p == FINGERPRINT_OK) {

Serial.println("Stored!");

} else if (p == FINGERPRINT_PACKETRECIEVEERR) {

Serial.println("Communication error");

return p;

} else if (p == FINGERPRINT_BADLOCATION) {

Serial.println("Could not store in that location");

return p;

} else if (p == FINGERPRINT_FLASHERR) {

Serial.println("Error writing to

flash"); return p;

} else {

Serial.println("Unknown error");

return p;

}

}
```

CHECK THE VALID FINGER:

```
  #include
<Adafruit_Fingerprint.h> #include
<SoftwareSerial.h> #include
<LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x27, 16, 2)



void setup()
{
  lcd.begin();
    lcd.setCursor(0, 0);
 lcd.print("Fingerprint
 Door"); lcd.setCursor(0, 1);
 lcd.print("DOOR locked");
 delay(3000);
 lcd.clear();


Serial.begin(9600);
while (!Serial); // For
Yun/Leo/Micro/Zero/… delay(100);
Serial.println("fingertest");
pinMode(12, OUTPUT);
pinMode(11, OUTPUT);

// set the data rate for the sensor serial port
```

```
finger.begin(57600);
```

```
SoftwareSerial mySerial(2, 3);


  Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);


  void setup()

  {

    lcd.begin();

      lcd.setCursor(0, 0);

   lcd.print("Fingerprint

   Door"); lcd.setCursor(0, 1);

   lcd.print("DOOR locked");

   delay(3000);

   lcd.clear();



  Serial.begin(9600);

  while (!Serial); // For

  Yun/Leo/Micro/Zero/… delay(100);

  Serial.println("fingertest");

  pinMode(12, OUTPUT);

  pinMode(11, OUTPUT);


  // set the data rate for the sensor serial port

  finger.begin(57600);


  if (finger.verifyPassword()) {
```

```
Serial.println("Found fingerprint sensor!");
} else {
Serial.println("Did not find fingerprint sensor :(");

while (1) {
delay(1);
}
}

finger.getTemplateCount();
Serial.print("Sensor contains ");
Serial.print(finger.templateCount);
Serial.println("templates");
Serial.println("Waiting for valid finger…");
}
void loop() // run over and over again
  {
  getFingerprintIDez();
delay(50); //don’t ned to run this at full speed.
digitalWrite(12, LOW);
digitalWrite(11, LOW);
}

uint8_t getFingerprintID()
{ uint8_t p =
finger.getImage();switch (p)
{
```

```
case FINGERPRINT_OK:
Serial.println("Image taken");
break;
case FINGERPRINT_NOFINGER:
Serial.println("No finger detected");
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
return p;
case FINGERPRINT_IMAGEFAIL:
Serial.println("Imaging
error"); return p;
default:
Serial.println("Unknown error");
return p;
}

// OK success!

p =
finger.image2Tz();
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image converted");
break;
case FINGERPRINT_IMAGEMESS:
Serial.println("Image too messy");
```

```
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
return p;
case FINGERPRINT_FEATUREFAIL:
Serial.println("Could not find fingerprint features");
return p;
case FINGERPRINT_INVALIDIMAGE:
Serial.println("Could not find fingerprint features");
return p;
default:
Serial.println("Unknown error");
return p;
}

// OK converted!
p =
finger.fingerFastSearch(); if
(p == FINGERPRINT_OK)
{
Serial.println("Found a print match!");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
Serial.println("Communication error");
return p;
} else if (p == FINGERPRINT_NOTFOUND) {
Serial.println("Did not find a
match"); return p;
} else {
```

```
Serial.println("Unknown error");
return p;
}
{digitalWrite(11, HIGH);
delay(3000);
digitalWrite(11, LOW);
Serial.print("Not
Found");
Serial.print("Error");
return finger.fingerID;
}

// found a match!
Serial.print("Found ID #"); Serial.print(finger.fingerID);
Serial.print(" with confidence of "); Serial.println(finger.confidence);

return finger.fingerID;
}

// returns -1 if failed, otherwise returns ID #
int getFingerprintIDez() {
uint8_t p = finger.getImage();
if (p != FINGERPRINT_OK)
{
lcd.clear(); lcd.setCursor(0, 0);
lcd.print(" Waiting For"); lcd.setCursor(0, 1);
lcd.print("ValiFinger"); delay(3000);
return -1;
}
p = finger.image2Tz();
if (p != FINGERPRINT_OK) {
lcd.clear(); lcd.setCursor(0, 0);
lcd.print(" Messy Image"); lcd.setCursor(0, 1); lcd.print(" Try Again"); delay(3000);
clear(); return -1;}
P=finger.fingerFastSearch(); if (p != FINGERPRINT_OK) {
lcd.clear(); lcd.setCursor(0, 0);
lcd.print("Not Valid Finger"); delay(3000);
lcd.clear(); return -1;
}
// found a match!
```

5.3 CONSTRAINTS, ALTERNATIVES AND TRADEOFFS

5.3.1 CONSTRAINTS:

Though the finger print sensor is highly secure it may also cause some limitations they are:

- Different biometric technologies need the use of different devices that have a range of cost.
- Entry and delete fingerprints need to operate multiple steps, the program is too much trouble,
- convenience is not enough.
- Performance can be fluctuating to dry, wet, dirty fingers.
- Population coverage may be a problem with old age people or people with skin disease.
- Sometimes it take few minutes to scan the finger print
- At a time pressing finger more than two to three times the sensor cant able to detect the right finger print which has already stored.

- Apartment from the family member a new person who is well known to the owner .Trying to open the door first he have to store his fingerprint to the owner of the house
- At a time pressing finger more than two to three times the sensor can’t able to detect the right finger print which has already stored.
- Apartment from the family member a new person who is well known to the owner .Trying to open the door first he have to store his fingerprint to the owner of the house

5.3.2 ALTERNATIVES:

In the terms of automatic door locking system there are many alternatives like raspberry pi, pattern/password, face recognition, RFID, Bluetooth module, pic microcontroller.

Bluetooth module:

The mechanism of device is give a digital keypad as input on the software on android smartphone first, if there is a command which is controlled by the user, the data will be instantly sent via a Bluetooth network then the input received by the Hc-05 Bluetooth module that connected to Arduino microcontroller.

Face recognition:

Face Recognition based on PCA is generally referred to as the use of Eigen faces. If a face is recognized, it is known, else it is unknown. The door will open automatically for the known person due to the command of the microcontroller. On the other hand, alarm will ring for the unknown person.

Password based using 8051 microcontroller:

This system demonstrates a Password based Door Lock System using 8051 Microcontroller, wherein once the correct code or password is entered, the door is opened and the concerned person is allowed access to the secured area. Again, if another person arrives, it will ask to enter the password whether it is wrong the door remained to be closed.

RFID:

An RFID based Door Lock is based on some simple concepts. We store a set of RFID card data in our system, say 3 or 10 RFID card data. When the person with the right RFID card (compatible to data preloaded in our program/**system**) come and swipes his RFID tag, access will be granted.

Raspberry pi:

The system works by taking snaps for the guest through a code and camera pi positioned in the doors then, such snaps will be sent to the owner. The proposed system can be extended to be used for different properties and facilities such as banks and office.

Using Bluetooth:

The mechanism of device is give a digital keypad as input on the software on android smartphone first, if there is a command which is controlled by the user, the data will be instantly sent via a Bluetooth network then the input received by the Hc-05 Bluetooth module that connected to Arduino microcontroller.

Pic microcontroller:

Electronic lock takes inputs from the user with the help of 4X4 keypad. PIC16F877A microcontroller reads these inputs and compared it with a already stored password. Default password 1234 is stored in EEPROM of PIC microcontroller. After taking inputs from a user, these inputs are stored in array.

5.3.3 Trade- offs:

1. The Schlagle Encode: It is a Wi-Fi-enabled smart lock can be controlled via phone and voice and integrates with Amazon Key and Ring cameras.

Trade-offs:

- Easy to install.
- Works with Amazon Alexa, Amazon Key, and Google Assistant.

2. Godrej Locks has been securing every home in India ever since 1897.

Trade-offs:

- It has a designer style and superior security

3.The Ultralow U-Bolt Pro is a multifaceted smart lock that lets you unlock your door with a fingerprint scan, a mobile app, a keypad, a voice command, or even a traditional key.

Trade-offs:

- Fingerprint, keypad, and automatic unlocking.
- Works with Amazon Alexa and Google Assistant voice control.
- Supports IFTTT.
- Includes Wi-Fi Bridge.

4.The Remote Lock Open Edge RG Deadbolt is a Wi-Fi smart lock that you can control from anywhere and integrates with several vacation rental platforms.

Trade-offs:

- Mobile app and web browser control.
- Responsive keypad.
- Integrates with multiple vacation rental platforms.

5. The Nest X Yale Lock with Nest Connect is a sharp-looking smart door lock that combines Yale reliability with Nest IOT home connectivity.

Trade-offs:

- Stylish design.
- Easy to install.

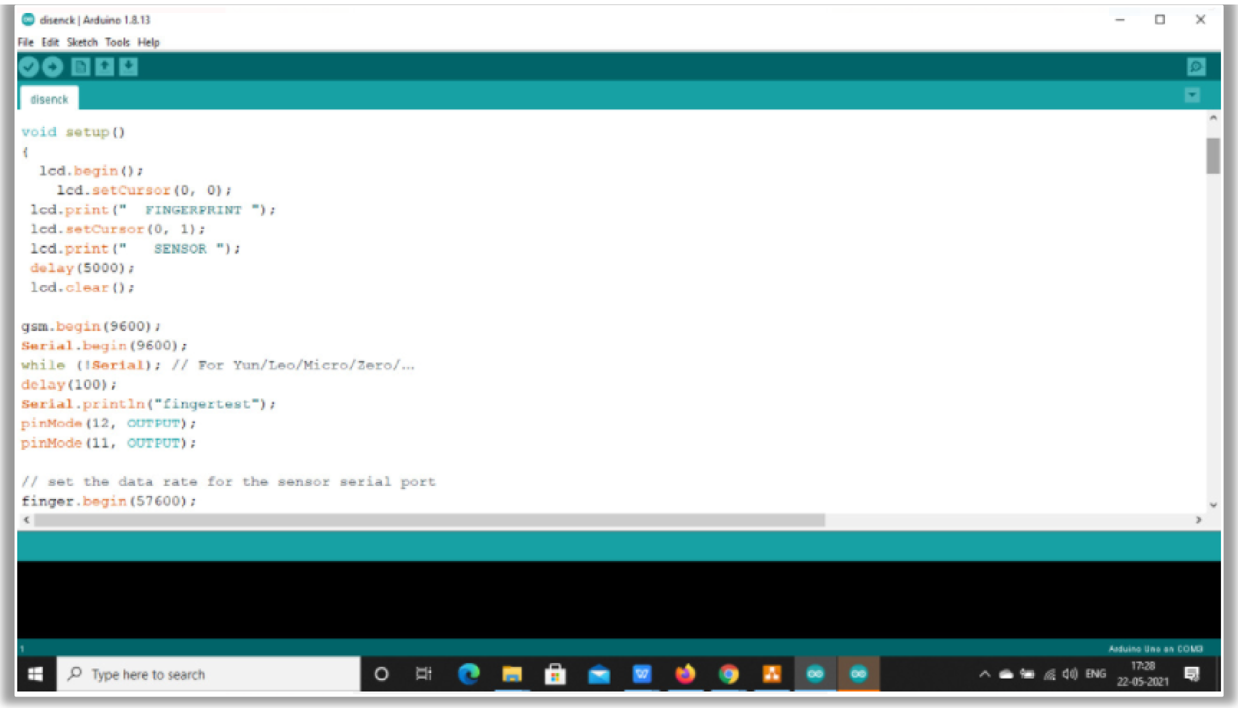
TABLE 6.1 SCHEDULES, TASK AND MILESTONE

ACTIVITIES	DECEMBER				JANUARY				FEBRUARY				MARCH				APRIL				MAY/JUNE			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Project title selection	🟦																							
Literature survey		🟨	🟨																					
Zeroth review		🟩																						
Hardware and software requirements				🟥	🟥																			
30% of code implementation						🟪	🟪																	
First review								🟥																
Storing of finger print								🟥																
Verification of valid finger print									🟥	🟥														
Connection of Arduino UNO and fingerprint sensor										🟩	🟩													
Combining all the inputs and verification of all finger print												🟦	🟦		🟦									
Second review														🟩										
Connection of GSM Module														🟩		🟩								
Cloud storage with spread sheet																	🟦	🟦	🟦	🟦				
Final review																								

7. PROJECT DEMONSTRATION:

ARDUNINO IDE

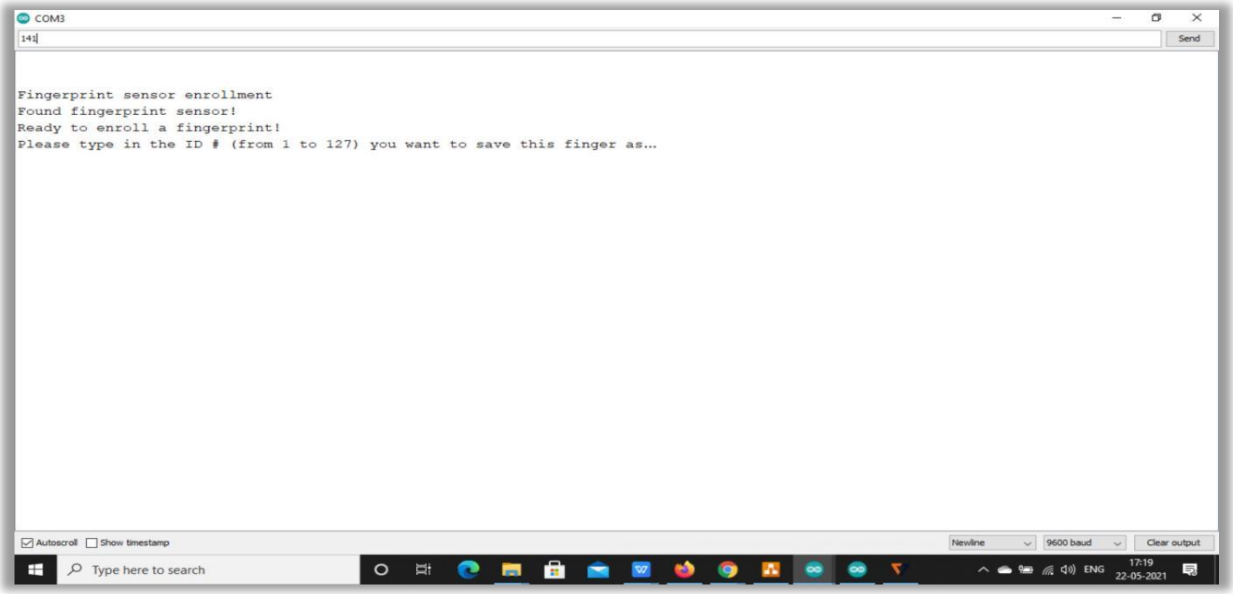
Implementation of code for storage of finger print



```
void setup()
{
  lcd.begin();
    lcd.setCursor(0, 0);
 lcd.print("  FINGERPRINT ");
 lcd.setCursor(0, 1);
 lcd.print("   SENSOR ");
 delay(5000);
 lcd.clear();

gsm.begin(9600);
Serial.begin(9600);
while (!Serial); // For Yun/Leo/Micro/Zero/...
delay(100);
Serial.println("fingertest");
pinMode(12, OUTPUT);
pinMode(11, OUTPUT);

// set the data rate for the sensor serial port
finger.begin(57600);
```

Figure 7.1 Code for storing finger print

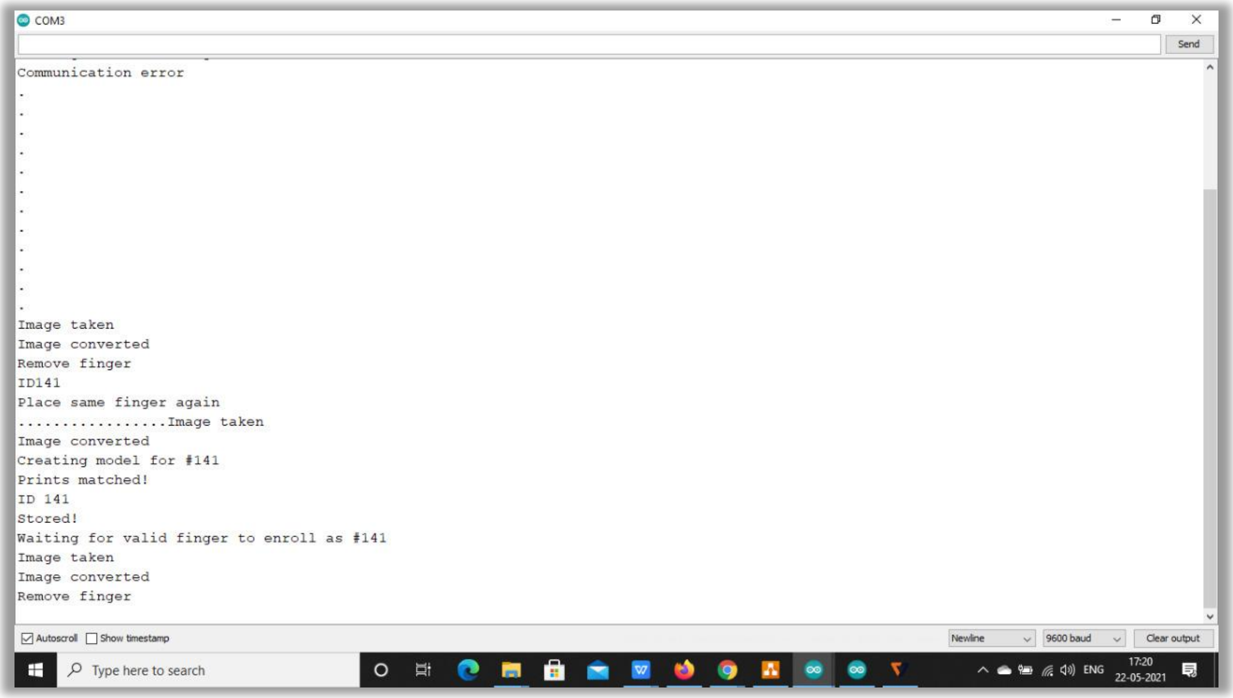
Output:



```
141
```

```
Fingerprint sensor enrollment
Found fingerprint sensor!
Ready to enroll a fingerprint!
Please type in the ID # (from 1 to 127) you want to save this finger as...
```

Enrolling The function of fingerprint scanner is to scan the users fingerprint. During scanning the fingerprint scanner will capture and store the users finger print. To have a database of users fingerprint minutiae, the user needs to enrol their fingerprint. Figure 7.2 shows the result of an enrolled fingerprint. Once Arduino detected fingerprint scanner, the users will insert the ID that will be saved together with their fingerprint minutiae. According to figure above, the users fingerprint minutiae is enrolled with the ID: 141 It is then stored in the fingerprint scanner and in spread sheet

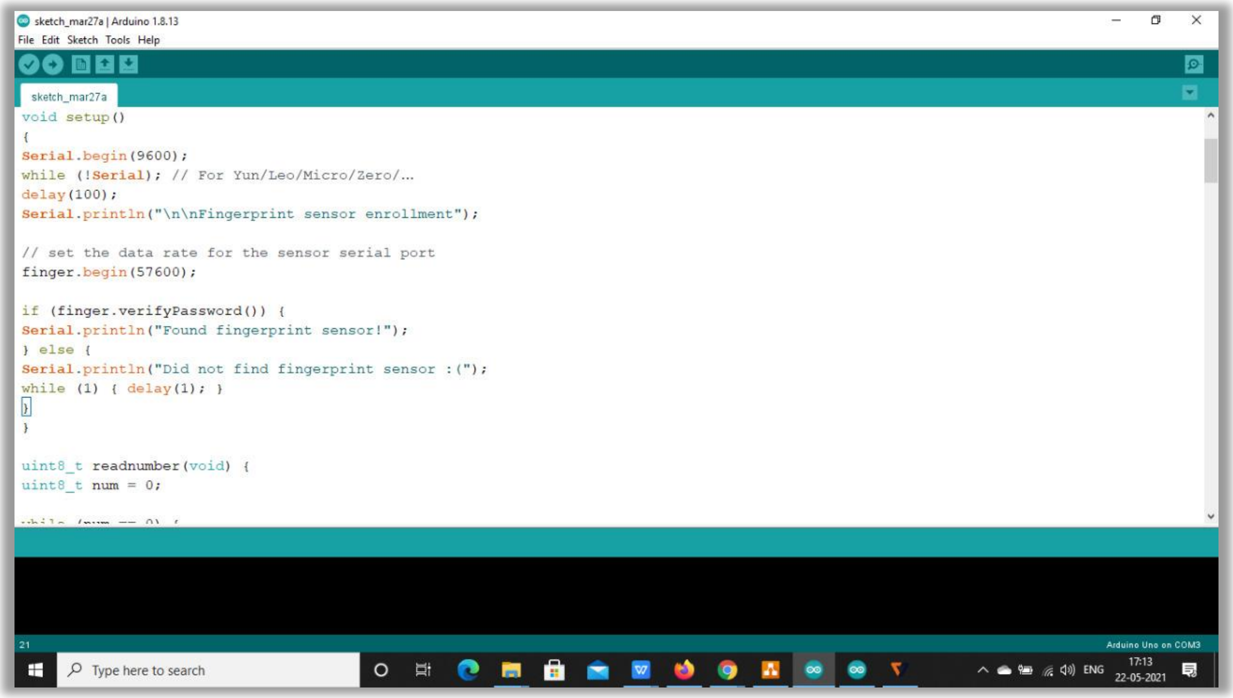


```
Communication error
.
.
.
.
.
.
.
.
.
.
.
.
Image taken
Image converted
Remove finger
ID141
Place same finger again
................Image taken
Image converted
Creating model for #141
Prints matched!
ID 141
Stored!
Waiting for valid finger to enroll as #141
Image taken
Image converted
Remove finger
```

Figure 7.2 Finger print enrolling output at serial monitor

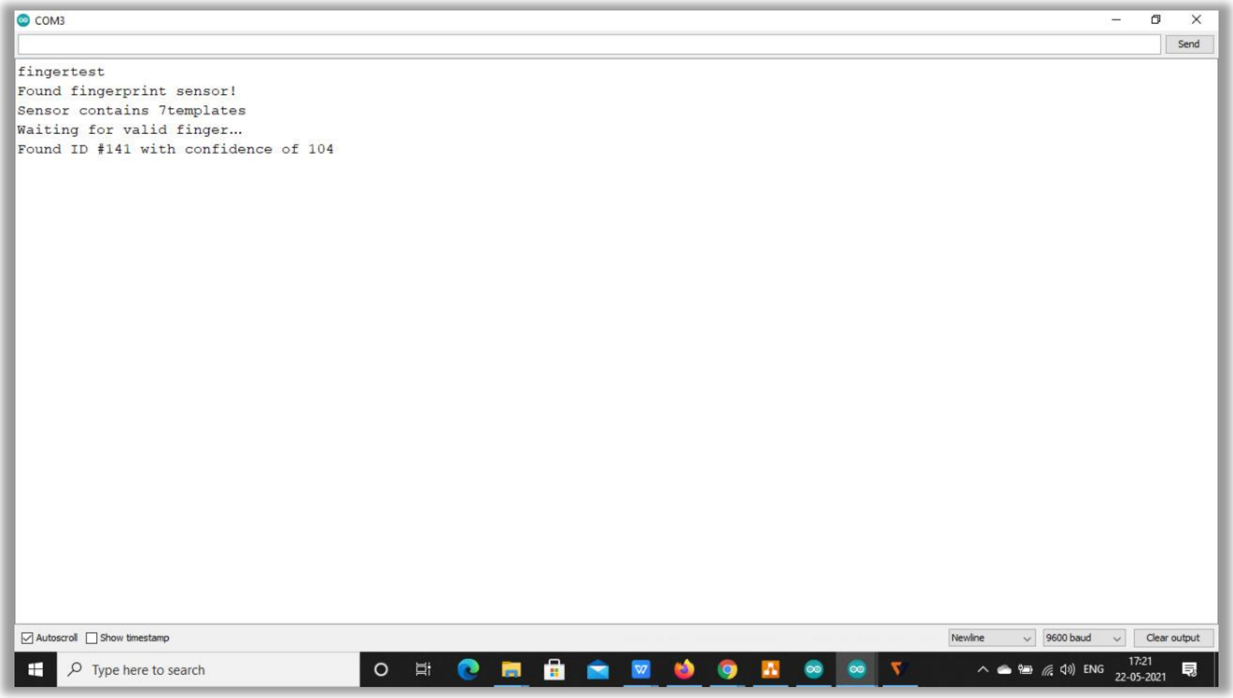
Finger test and matching

After enrolling the fingerprint, the stored minutiae need to be tested to test the accuracy of the fingerprint scanner. Figure 43 shows the finger test output at serial monitor. The user ID is found to be ID: 141. It states the confidence which actually measures the accuracy of the current scanned fingerprint and the ones stored in memory. The finger print scanner has a level of confidence from 0 to 255 which indicates from less accurate to very accurate. place the fingerprint using finger print sensor. After scanned finger, then it will shows the output being displayed at LCD display. The output indicates the current scanned fingerprint is matched with the stored minutiae with ID: 141(Fig 7.5)



```
void setup()
{
Serial.begin(9600);
while (!Serial); // For Yun/Leo/Micro/Zero/...
delay(100);
Serial.println("\n\nFingerprint sensor enrollment");

// set the data rate for the sensor serial port
finger.begin(57600);

if (finger.verifyPassword()) {
Serial.println("Found fingerprint sensor!");
} else {
Serial.println("Did not find fingerprint sensor :(");
while (1) { delay(1); }
}
}

uint8_t readnumber(void) {
uint8_t num = 0;

while (num == 0) {
```

Figure 7.4 Code for verification of finger print

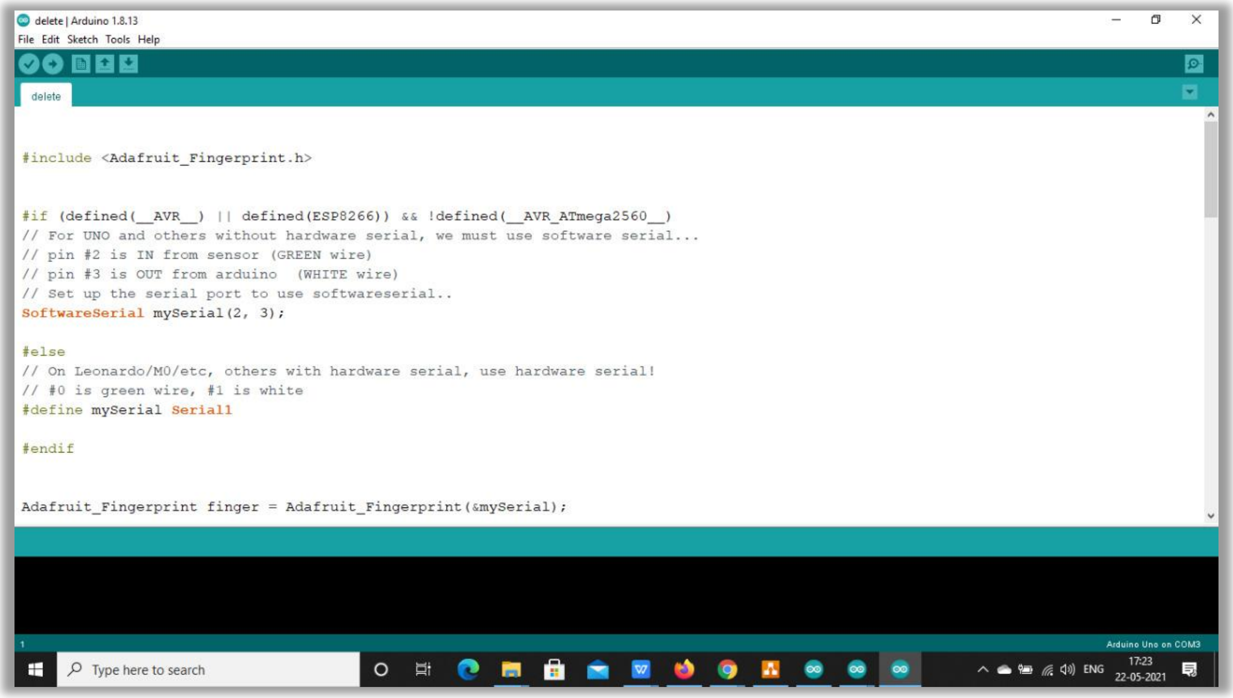


```
fingertest
Found fingerprint sensor!
Sensor contains 7templates
Waiting for valid finger...
Found ID #141 with confidence of 104
```

Figure 7.5 Finger print test at serial monitor

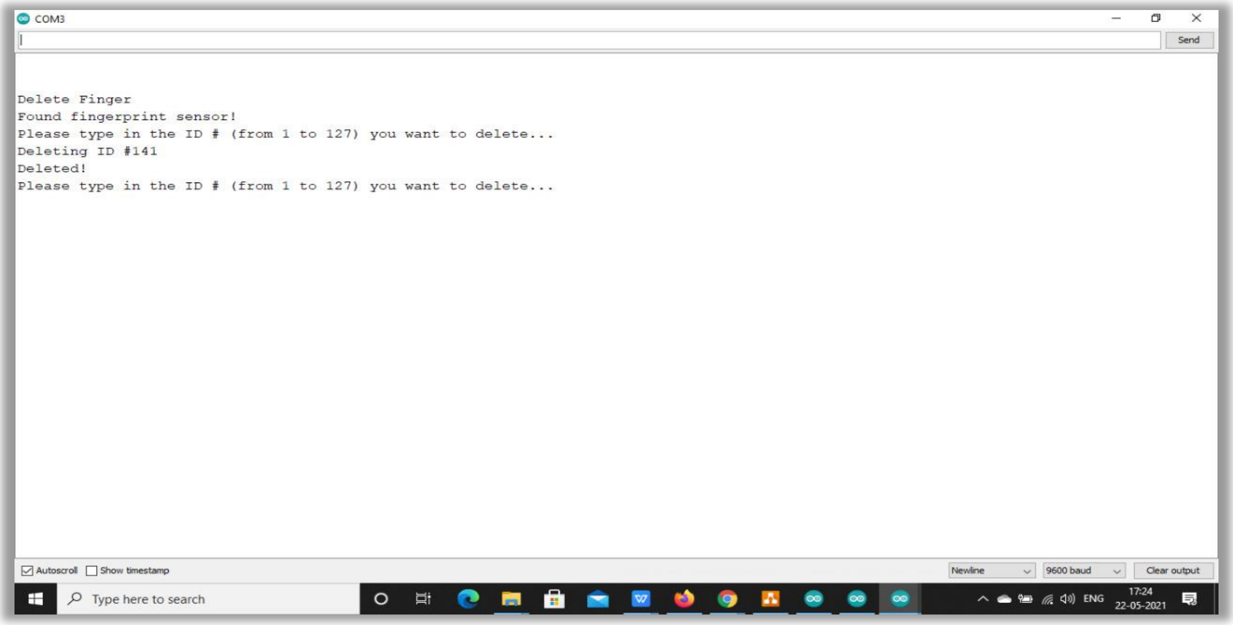
7.6 Deletion of finger print:

Unnecessarily we stored a fingerprint or want to eliminate unwanted finger print from the cloud we should implement code for deletion of finger print. For example from figure 7.7 already stored finger print ID: 141 wants to be deleted just select the ID:141 it will display as Deleted.



```
#include <Adafruit_Fingerprint.h>


#if (defined(__AVR__) || defined(ESP8266)) && !defined(__AVR_ATmega2560__)
// For UNO and others without hardware serial, we must use software serial...
// pin #2 is IN from sensor (GREEN wire)
// pin #3 is OUT from arduino  (WHITE wire)
// Set up the serial port to use softwareserial..
SoftwareSerial mySerial(2, 3);

#else
// On Leonardo/M0/etc, others with hardware serial, use hardware serial!
// #0 is green wire, #1 is white
#define mySerial Serial1

#endif


Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
```

Figure 7.6 Code for deletion of finger print

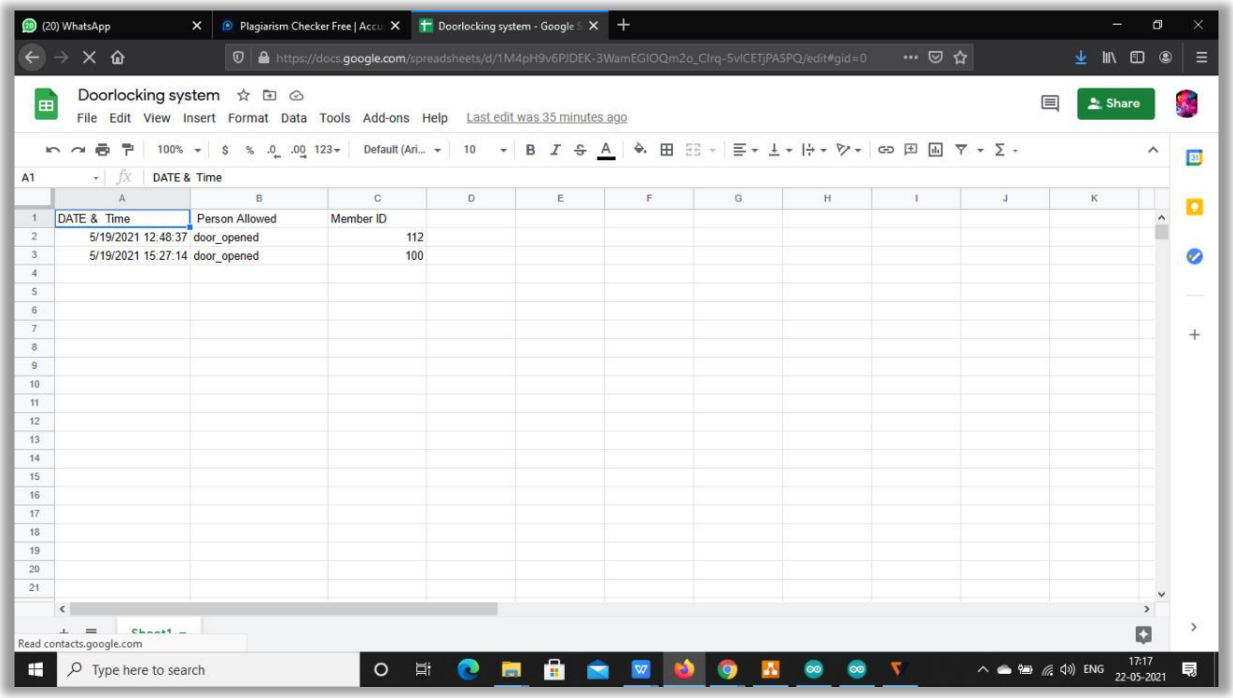


```
Delete Finger
Found fingerprint sensor!
Please type in the ID # (from 1 to 127) you want to delete...
Deleting ID #141
Deleted!
Please type in the ID # (from 1 to 127) you want to delete...
```

Figure 7.7 Output for deletion of finger print

7.8 CLOUD STORAGE:

In the figure.10 shows the cloud data storage. Node MCU connect the data with Cloud and stored in drive. In the data, user admin can able to see data of the Person who's open the door with time and date. This is the major advantages of the project.



(20) WhatsApp
Plagiarism Checker Free | Accu
Doorlocking system - Google S
https://docs.google.com/spreadsheets/d/1M4pH9v6PJDEK-3WamEGIOQm2o_Clrq-5vlCETjPASPQ/edit#gid=0
Doorlocking system
File Edit View Insert Format Data Tools Add-ons Help
Last edit was 35 minutes ago
Share
A1
DATE & Time
Sheet1
Read contacts.google.com
Type here to search
ENG
17:17
22-05-2021

DATE & Time	Person Allowed	Member ID
5/19/2021 12:48:37	door_opened	112
5/19/2021 15:27:14	door_opened	100

Figure 7.8 Storage of finger print in spread sheet

8. RESULT AND DISCUSSION

After constructing the circuit, testing was done. Figures 7.1 to 7.6 shows the results obtained from each feature and the interfacing all feature with Arduino. During testing, the outputs obtained were displayed to the LCD display .

8.1 Finger print sensor:

The first stage to access the door is to enter finger print . Figure 8.1.2 shows a display for the user as finger print sensor. In this program the finger print can able to store from 1 to 127 . If the users entered the same finger print as the ones stored as , it will resulted as " DOOR UNLOCKED WELCOME HOME", Now scan finger' as in Figure 8.1.1. Next the users may scan their fingerprint immediately for the next stage of door access system. Otherwise, if the wrong finger print is scanned as in Figure 39, the LCD display will display as "INVALID FINGERPRINT' as in Figure 40. While Figure 41 shows the output of

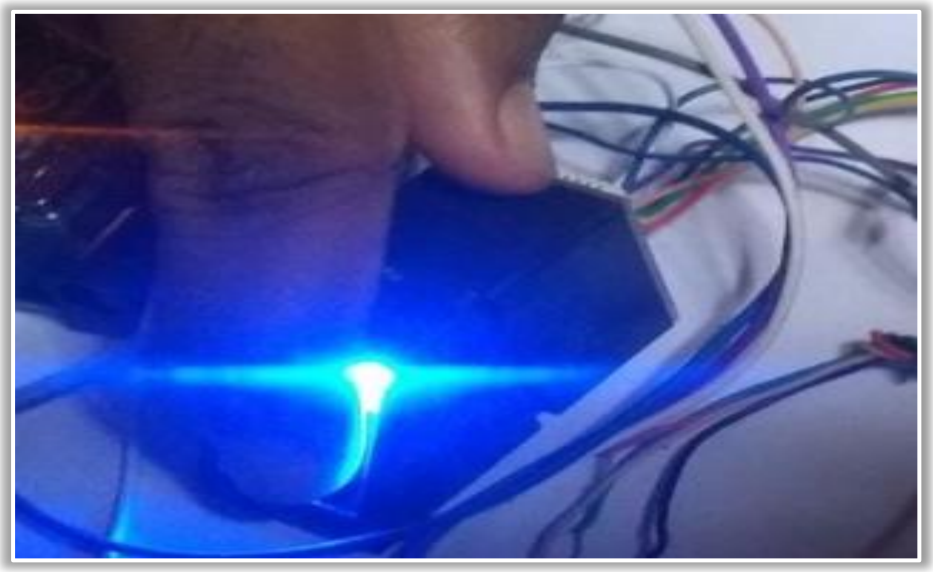


Figure 8.1 Scanning the finger print using finger print sensor

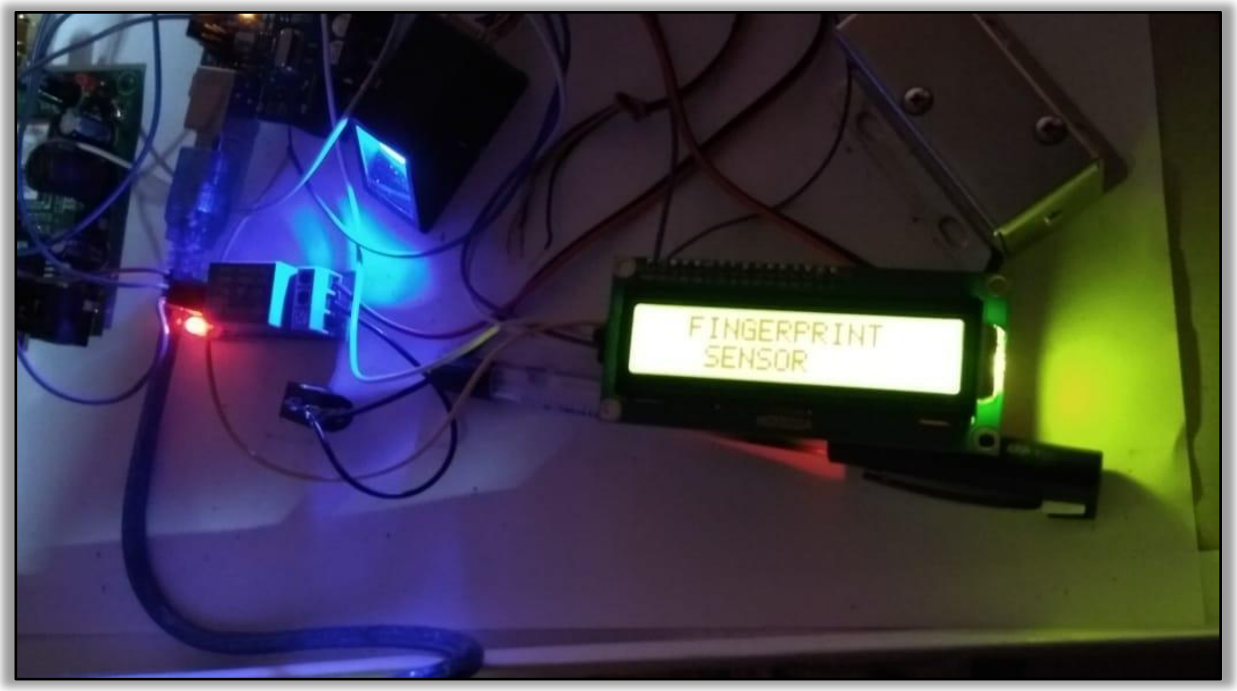


Figure 8.2 LCD Display is showing as Finger print sensor

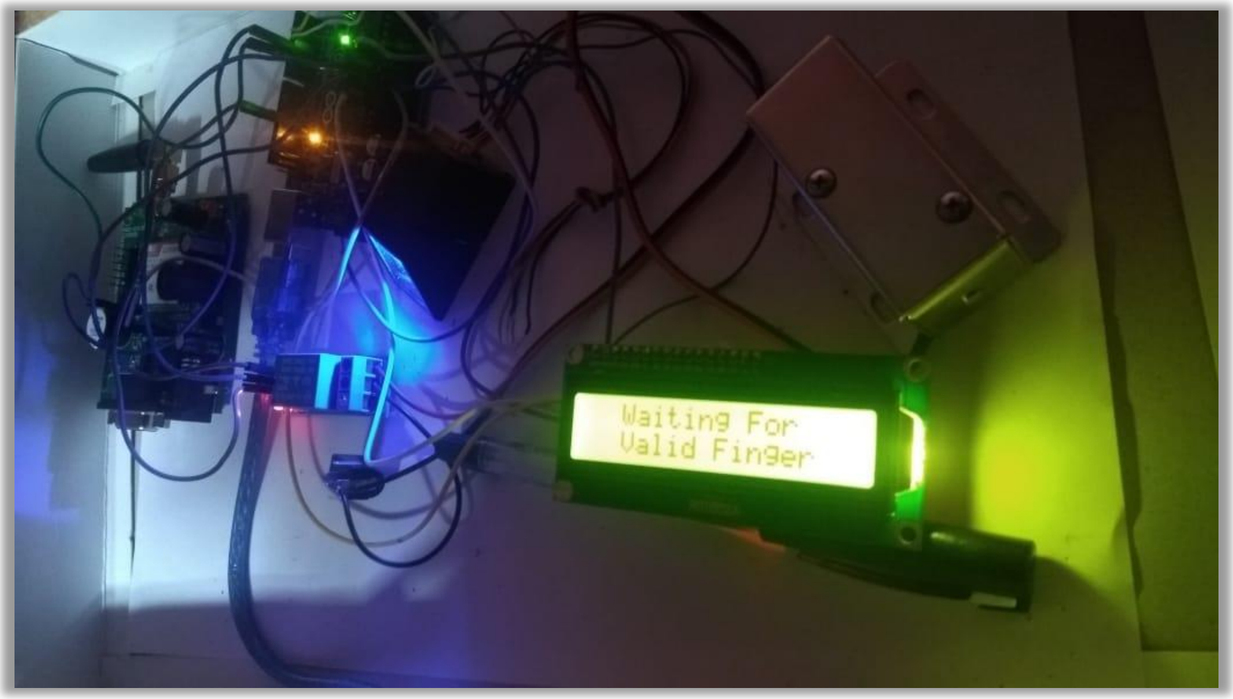


Figure 8.3 Waiting for valid finger print

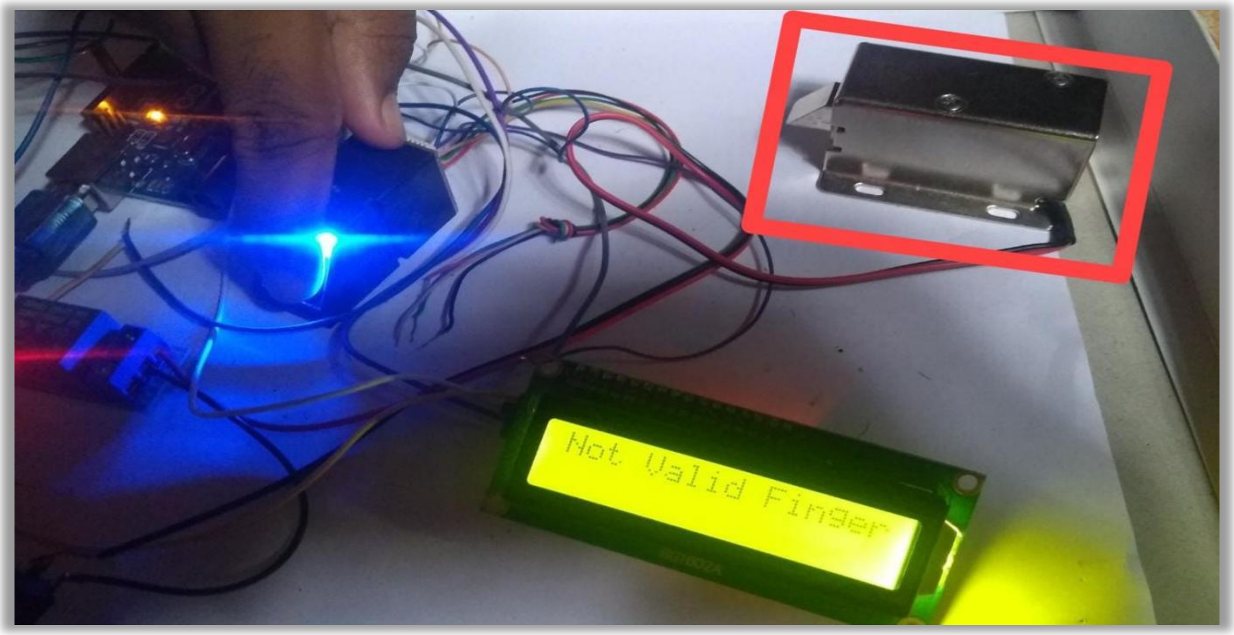
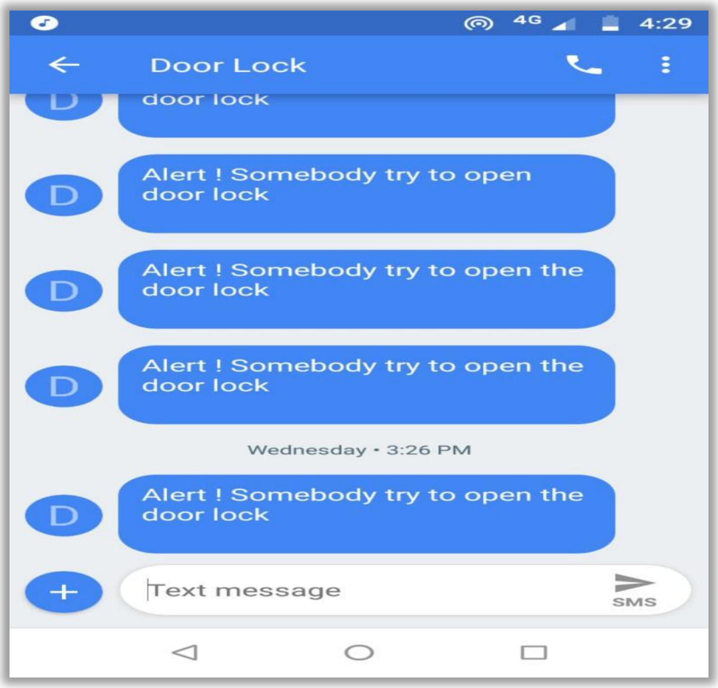


Figure 8.4 Not valid finger print

Figure. 8.5 shows the Alert text message, When Unauthorized try to access the door locking system then, The GSM module (ESP32) have one SIM is inserted on it board. This GSM module send SMS Alert text message to register owner number. In this Figure.9 can we see the message Send to the authorized person.



door lock

Alert ! Somebody try to open door lock

Alert ! Somebody try to open the door lock

Alert ! Somebody try to open the door lock

Wednesday • 3:26 PM

Alert ! Somebody try to open the door lock

Figure 8.5 alert message will be send to owner Through GSM Module.

In the figure.8.6 and 8.7, Show as the Micro-controller the after the validity ,If the finger print matches with the stored finger then, Unlocked the solenoid lock with power of 12V Supply and Display the LCD Screen as “ Door unlocked welcome home” Message.

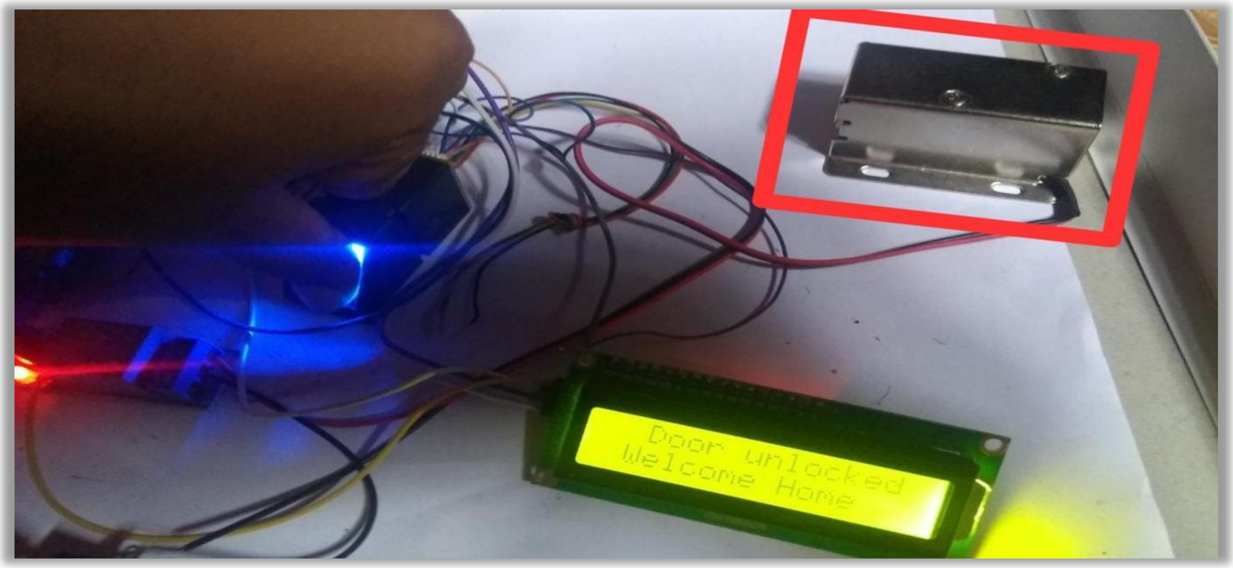


Figure 8.6 For valid finger print door will be unlocked and displayed on LCD

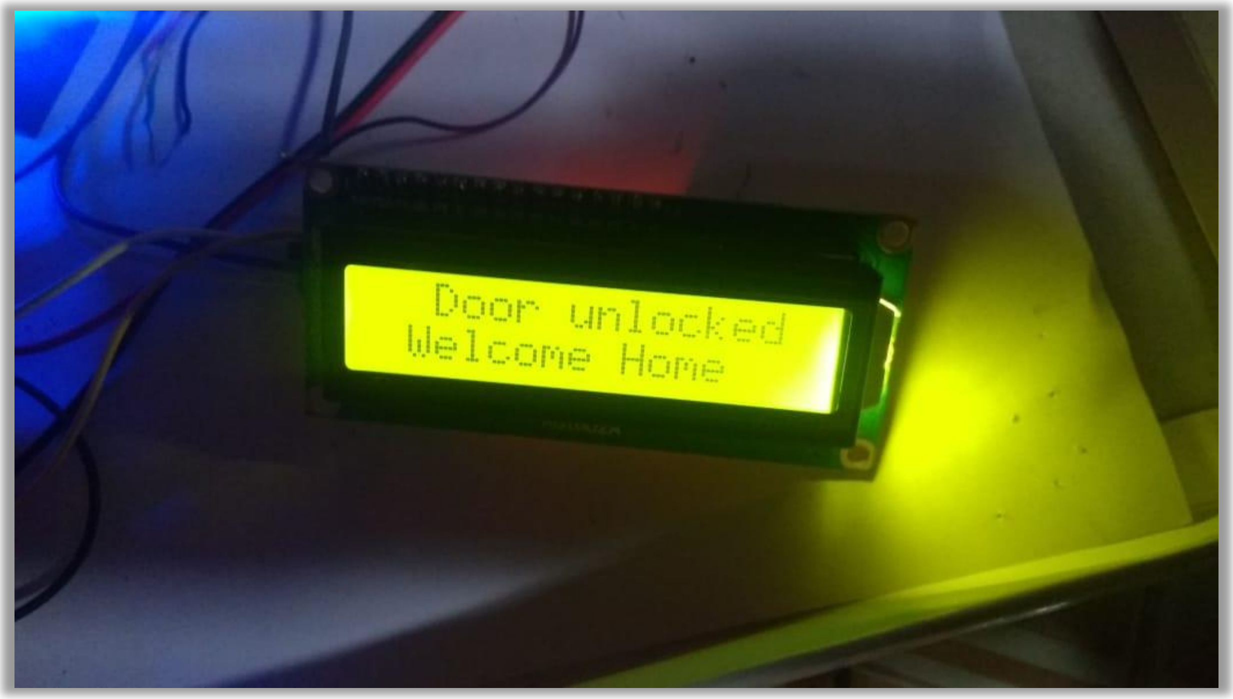


Figure 8.7 Output display on LCD

This is our overall set up of our project and all the hardware requirements are connected by using jumper wires and an adapter is connected with Arduino UNO with power supply.

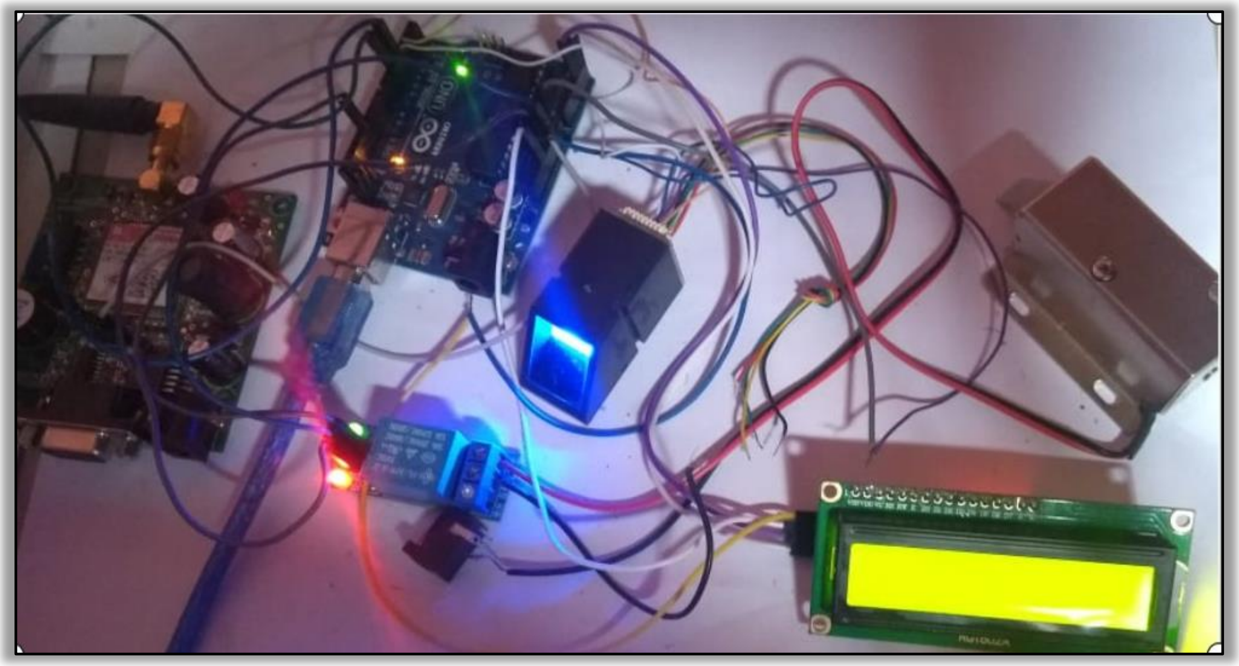


Figure 8.9 Over all implementation and design of the project

9. SUMMERY

The implementation of Automatic door locking system is considered to be a need for a building especially companies to have a security system in order to keep the people inside and assets to be safe from unwanted cases such as burglaries and kidnapping.

Many has been reported that the house existing door access system have problems in maintaining due to its obsolete components that could not be replaced. The Automatic Door locking System – Arduino Based is developed to overcome this issue as Arduino does not use a lot of components with the existence of the Arduino platform board and Atmel AVR microcontroller. The Arduino approach also overcome the issue of upgrading as it comes with an Atmel AVR microcontroller which can be edited and reprogrammed many times . Arduino is also known to its open source and cross-platform that could ease the task of a programmer

The software used in this project is Arduino programming language which is similar to C++. Based on the research done it shows that Arduino is much simpler compared to other and suitable to be used in this project. Besides software and approach, this project also differs in terms of its features which is fingerprint scanner. It clearly shows that the features used in this project are more efficient compared to the existing system.

There input used in this project is fingerprint scanner. While the outputs are LCD display and solenoid door lock. The fingerprint scanner has also high accuracy with the percentage of 70% for the highest fingerprint. The fingerprint scanner used is in this project also have high efficiency due to its time in obtaining results identifying minutiae which is less than 6 second in identifying minutiae.

CONCLUSION:

In conclusion the implementation of a Automatic door locking system with SMS alert using IOT. Arduino is a less time-consuming programming because it is an open-source microcontroller. It has high quality system compared to the existing door access system. The features used in this system helps to overcome the security issues. The proposed system overcomes the issues of maintaining the device in future as Arduino comes with ATMEGA2560 microcontroller that can be edited to comply with any changing system. Adopting the fingerprint scanner features, creating a Automatic door locking system-Arduino Based brings a whole new high security access system with a simple new approach.

FUTURE IMPROVEMENTS

Advancements in biometric identification management technology are moving so fast, In future we will make advancement and multi functions like image recognizing process system and password system based. Also eyes retina for password which helps authorized persons for authentication for entrance so biometric technology makes individual convenient in real life

It is recommended to add another feature such as smart card to increase the security level. Smart card stores data such as name and ID of the owner and in future it can be used to match the entered ID using keypad.

10. REFERENCE

[1] Shanthini, M., Vidya, G., & Arun, R. (2020, August). IoT Enhanced Smart Door Locking System. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 92-96). IEEE.

[2] Raju, N. G., Vikas, J., Appaji, S. V., & Hanuman, A. S. (2018, December). Smart Lock Controlled using Voice Call. In 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 97-103). IEEE.

[3] Bangali, J., & Shaligram, A. (2013). Design and Implementation of Security Systems for Smart Home based on GSM technology. International Journal of Smart Home, 7(6), 201-208.

[4] Jahnavi, S., & Nandini, C. (2019, March). Smart Anti-Theft Door locking System. In 2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE) (pp. 205-208). IEEE.

[5] Yugashini, I., Vidhyasri, S., & Devi, K. G. (2013). Design and implementation of automated door accessing system with face recognition. International Journal of Science and Modern Engineering (IJISME), 1(12).

[6] Cahyaningtiyas, R., Arianto, R., & Yosrita, E. (2016, November). Fingerprint for automatic Door integrated with Absence and User Access. In 2016 International Symposium on Electronics and Smart Devices (ISESD) (pp. 26-29). IEEE.

[7] Alnabhi, H., Al-naamani, Y., Al-madhehagi, M., & Alhamzi, M. (2020). Enhanced Security Methods of Door Locking Based Fingerprint. International Journal of Innovative Technology and Exploring Engineering, 9(03), 1173-1178.

[8] Nishida, D., Tsuzura, K., Kudoh, S., Takai, K., Momodori, T., Asada, N., ... & Tomizawa, T. (2014, May). Development of intelligent automatic door system. In 2014 IEEE International Conference on Robotics and Automation (ICRA) (pp. 6368-6374). IEEE.

[9] Lwin, H. H., Khaing, A. S., & Tun, H. M. (2015). Automatic door access system using face recognition. international Journal of scientific & technology research, 4(06), 294-99.

[10]Barsha, F. L., Tasneem, Z., Mojib, S., Afrin, M., Jahan, N., Tasnim, M., ... & Islam, M. N. (2019, November). An IoT based Automated Door Accessing System for Visually Impaired People. In 2019 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE) (pp. 1-4). IEEE.

[11] Hadis, M. S., Palantei, E., Ilham, A. A., & Hendra, A. (2018, March). Design of smart lock system for doors with special features using bluetooth technology. In 2018 International Conference on Information and Communications Technology(ICOIACT) (pp. 396-400). IEEE.

[12] Yoon, S. H., Lee, K. S., Cha, J. S., Mariappan, V., Young, K. E., Woo, D. G., & Kim, J. U. (2020). IoT Open-Source and AI based Automatic Door Lock Access Control Solution. International Journal of Internet, Broadcasting and Communication, 12(2), 8- 14.

[13] Adiono, T., Fuada, S., Anindya, S. F., Purwanda, I. G., & Fathany, M. Y. (2019). IoT-enabled door lock system. Int. J. Adv. Comput. Sci. Appl, 10(5), 445-449.

[14] Nnenna, N. H. SHORT MESSAGE SERVICE (SMS) ALERT INTELLIGENT SECURITY DOOR SYSTEM.

[15] Rashid, R. A., Mahalin, N. H., Sarijari, M. A., & Aziz, A. A. A. (2008, May). Security system using biometric technology: Design and implementation of Voice Recognition System (VRS). In 2008 International Conference on Computer and Communication Engineering (pp. 898-902). IEEE.

[16] Raju, N. G., Vikas, J., Appaji, S. V., & Hanuman, A. S. (2018, December). Smart LockControlled using Voice Call. In 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 97-103). IEEE.

[17] Patil, K. A., Vittalkar, N., Hiremath, P., & Murthy, M. A. (2020). Smart Door Locking System using IoT.

[18] Radzi, S. A., Alif, M. M. F., Athirah, Y. N., Jaafar, A. S., Norihan, A. H., & Saleha, M. S. (2020). IoT based facial recognition door access control home security system using raspberry pi. International Journal of Power Electronics and Drive Systems, 11(1), 417.

[19] Akanbi, C. O., Ogundoyin, I. K., Akintola, J. O., & Ameenah, K. (2020). A prototype model of an iot-based door system using double-access fingerprint technique. Nigerian Journal of Technological Development, 17(2).

[20] Ismail, I. F., Fawzi, M., Jamaludin, W. A. W., Madon, R. H., Abdullah, A. F., & Abdullah, M. A. (2021). Development of a Lock Biometric Authentication System for a Battery Powered Locking Device. International Journal of Integrated Engineering, 13(2),