FINGERPRINT DOOR LOCK USING ARDUINO

Department of Computer Science & Electronics

Microprocessor & Microcontroller Project Report

Submitted By
Team - C
Team Members-
Dipansh Sharma 21scse1120007

Submitted To
Dr. Ashish Sharma
Lecturer
Dept. of CSE
Galgotias University

Submission Date: May, 2022.

TABLE OF CONTENTS

LIST OF Figures

ABSTRACT

This concept which is of Fingerprint door locker is related to the security issues in the day today life, the physical key can be made as duplicate in very cheap cost and the key can lost somewhere or the key can steal, to overcome these issues we can use biometric security gadgets and try improvise the security much more because it can never be stolen it cannot be lost and the stealing chance of duplication are very low to break the security. From the old times the security is the big issue for the company's houses and other places and every person is worried about the security now a days. So, a solution to such problems can be by combining door lock with biometrics. Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. [2] Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures. The fingerprint sensor will take the fingerprint of the user and forward it to the microcontroller to match with its records. If the print matches with one of the fingerprints of the microcontroller's memory, the microcontroller will lock or unlock the latch, based on its current state. If the fingerprint do not match then nothing happen. The door lock is unlocked and the user have to retried. The system will be reset once a known print will be entered [15]. Here we will use fingerprint for biometric verification as it is one such thing which is unique to every individual and the use of fingerprint as the key to door locks can overcome the security problem of unauthorized people trespassing to our homes, shops, offices, etc. to a great extent as duplicate in such key is not possible. Also, this system will not lead to problems like losing keys because we do not require carrying keys if this system is used instead of traditional locks. So, using Arduino we will try to implement the system with features which will increase the security level. [18]

INTRUDUCTION

1.1 Background of Study and Motivation

These days office/corporate environment security is a major threat faced by every individual when away from home or at the home. 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. 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 system to access one's own information. Now a day, personal identification is becoming an important issue all around. Among mainstream personal identification methods, we mostly see password and identification cards techniques. But it is easy to hack password now and identification cards may get lost, thus making these methods quite unreliable. [19]

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 sometimes when a thief just breaks the lock and steals everything. 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. These are some of the hassles that people might face when using keys or smart cards. That is when our system, fingerprint door lock system comes into play. Our design is implemented to provide better securities as users don't need to remember passwords and don't need any sort of keys or cards that often get lost. If someone's fingerprint is authorized in the systems he/she would not face any sort of delays to enter a room. 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. Biometrics 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.[14]

This paper is about solving the problem regarding security of unauthorized people trespassing in our home, shops or offices. Security issues can be fixed using traditional locks but there is always possibility of someone opening the lock even without breaking it with the use of duplicate key.

Using these kinds of locks also create problem if we lose keys and also we have to carry keys along with us always. Again, using patterns in the locks can increase security but again it can be opened if somehow the passwords or patterns are known. So, leaving every system in this project we will implement a system using biometrics. Incase-of biometrics, the pattern which will be used as key will be unique. Here, to implement the project we will use fingerprint as the key This Arduino project will make use of different devices for the implementation of the security lock where there will be different features to increase the security level. [6]

In simple words, we can say that we are implementing a door access system using Arduino which make use of fingerprints to identify whom to allow and who not to allow inside our homes, offices, shops, etc. We are trying to implement it using a normal and simple door lock which is fitted in every home so as to minimize the cost of the device as a product. [1]

1.2 Project Objectives

The goal of this project is to research and analyze a suitable collection of components for developing a smart door lock using Arduino that provides excellent security and quick access. The following are the specific project goals:

- Familiarity with a smart door locking system based on a microcontroller.
- Using Arduino to create a simple and smart door locking system.

1.3 A brief outline of the report

This project is divided into ***5 chapters***. ***Chapter 1*** present the background of study and motivation of this project. Chapter one also presents objectives and a brief outline. ***Chapter 2*** provides the literature review of this project. ***Chapter 3*** introduces the project methodology and modeling like working principle, process of work, component, implementation, testing and cost analysis. ***Chapter 4*** presents the results and discussions of this project, also the simulation and experimental results. Finally, ***Chapter 5*** Conclude the project.

LITERATURE REVIEW

Meenakshi et al. has proposed “Arduino Based Smart Fingerprint Authentication System”. fingerprint locking system is a locking system that uses a fingerprint sensor module to secure the user's fingerprint. The fingerprint sensor module uses an Arduino or a Raspberry Pi to operate. In the proposed system, there is three-level security. Any two levels of security users have to face to unlock the system. This is the ideal option for avoiding the hassles of a stolen or lost key or illegal access. The authorized user must register his or her fingerprint in the system. The registered person's mobile number is then added to GSM, and a permanent image password is assigned to this user. As a first step, the unauthorized individual must choose unauthorized as the user type. The admin receives a random picture. The person must properly choose the random image. Otherwise, the system will go back to the first page. [2]

Patil et al. has proposed “Smart Door Locking System Using IoT” The internet of things, or IoT, is a wireless link that works in a door lock. With the help of IoT-enabled applications, the user may unlock the door with his smartphone. The servo library is introduced after the application is developed by creating a string variable that contains the unique device ID for the lock. The essential concept underlying the door lock's operation is the ID supplied by the Android phone via the created app. [3]

Reddy et al. has proposed “Security System Based on Knock Pattern Using Arduino and GSM Communication”. This system, which consists of Arduino, GSM Module, Servo Motor, and other components, employs a ‘Secret Knocking Pattern' that is only known by the owner of the safe, luggage, or other property or item on which the device is mounted. For the lock to open, the knocking pattern must be used only at a certain location, which is only known by the owner. The secret pattern can only be changed after the secret knock has been unlocked. Because there is no key to be copied, this approach fully eliminates the worry of duplication. [4]

Areed and Marwa F. has proposed “A Keyless Entry System Based on Arduino Board with Wi-Fi Technology.” A keyless entry system that focuses on the use of an Arduino circuit board, a Wi-Fi module, and the PHP programming language to provide access to a closed door. The suggested solution, which uses an Arduino Uno board and a Wi-Fi shield to unlock the door without a key, is described. The internet connection allows the system to unlock the door from any place, unlike traditional systems, which have a limited range. [5]

Kishwar Shafin et al. has proposed “Development of an RFID Based Access Control System in the Context of Bangladesh.” A magnetic door lock is administered through an RFID reader in the suggested system, which begins the authentication and validation of the user or regulates access in short. In addition, the systems keep track of each user's access and exit records in the form of a log report for each access. To avoid unforeseen circumstances, the administrator of the central subsystem can terminate the validity of any user at any moment. [6]

In the research paper “Fingerprint based locking system”, Ajinkya Kawale (May,2013) says that fingerprints are patterns of ridges and valleys on the surface of the finger. Like everything in the human body, these ridges form through a combination of genetic and environmental factors. The genetic code in DNA gives general orders on the way skin should form in a developing fetus, but the specific way it forms is a result of random events. With the help of interfacing, fingerprints can be used to create secure and impenetrable door locks and several lock systems. Interfacing is a method of establishing communication between Microcontroller and the Interface. Fingerprint interfaces are generic and can communicate with any microcontroller. It is a combination of hardware (i.e. the Interface) and Software (i.e. the source code to communicate, also called as the Driver). In simple words, to use LED as output device, LED should be connected to a port pin of the microcontroller and there has to be a program running inside the microcontroller to make it on or off or blink or dim. This program can be developed using any programming language like Assembly, C, Basic etc.[7]

In “An Advanced Door Lock Security System using Palmtop Recognition System”, Kawser Wazed Nafi, Lecturer of Stamford University talks about the classification of a security system

interface. According to him, the security system using fingerprint interface can be divided into the following Modules:

- Fingerprint analysis software module that accepts fingerprints images;
- Hardware interface module and the locking system module.

He (author) further added, stepwise break-up of execution plan looks like the following,

• Study of biometrics literature - especially with reference to fingerprint analysis.

• Study of basics of image processing algorithms so as to compare images with the point of view of unique-ness of fingerprints.

• Cogitation of MATLAB as a programming tool for image processing and comparing.

In major paper, "Personal authentication through biometric technologies", *Fernando L. Podio* (2002) cited that, fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. According to him, it is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical. He also added that the three basic patterns of fingerprint ridges are the arch, loop, and whorl. In his description- Arch are the ridges that enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger. Loops are the ridges that enter from one side of a finger, form a curve, and then exit on that same side. Last but not the least, he says that whorl are ridges that are formed circularly around a central point on the finger. In the whorl pattern, ridges form circularly around a finger. [11]

Published in the International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, *Tintu Pious* (B. Tech Student et al. is a prototype of a fingerprint based ignition systems in vehicles in which database of the valid users is stored in the fingerprint module. When a person tries to operate the vehicle then the CPU matches the fingerprint of the person with the stored database if the match result is successful then the vehicle is ignited and

otherwise not. External devices (hardware) can be controlled through the PC parallel port. The parallel port is a simple and inexpensive tool for building computer-controlled devices and projects. The user mode program is then made to communicate with the written device driver. The programming of this prototype was done in Visual Basic 6.0 Enterprise Edition. He describes the process saying, first of all user is asked to enroll his fingerprint. After enrollment the user's identification is done. If the person is authorized, the door automatically opens. After igniting the vehicle, the door automatically closes. When destination is reached, after a key press, the door automatically opens. After a set time delay, the door automatically closes. He adds, the system focuses on the use of fingerprints for door opening and closing. The fingerprint recognition software enables fingerprints of valid users of the vehicle to be enrolled in a database. Before any user can use the vehicle, his/her fingerprint image is matched against the fingerprints in the database while users with no match in the database are prevented from using the vehicle.

In the final term paper, "Design and Implementation of a Fingerprint Based Lock System for Shared Access", Jayasree Baidya et al. of North South University talks about 'smartphone based fingerprint security system'. They prompted that smartphones with latest features use fingerprint ID system to allow access to the phone. According to them, the very system can be made to connect with those phones and use their print ID and their sensor on the phone to open doors. The system can be connected to the phone via Bluetooth or Wi-Fi, and an application can be made for the phone allowing them to interact. In conclusion, they added, fingerprint ID is being used in most new phones now-a-days and soon the fingerprint ID based phone will be everywhere, almost everyone will have them and then this security system will be very helpful.[15]

Anu and Bhatia, D. (2014) in his paper 'A smart door access system using finger print biometric system', quotes that previously, for high security areas or in locker rooms for banks, traditional lock systems, passwords, etc., were employed. However, these systems were found to be not perfectly secure. After advancements in technology RFID cards were used. These cards however were not much useful for the user due to chances of getting lost, stolen and forgotten. The purpose of this study is to provide high security for such high-end security applications. The aim of this study is to design a smart door access system using finger print module. The use of this device is to provide access to only authorised persons. Both hardware and software technology are used to

design it. An emergency beep sound is provided to protect the system by giving alarm if any unauthorised person intrudes into the system. An indicator indicates for any emergency condition. Motors are used for locking and unlocking the door. [9]

Security of valuables is as paramount as their acquisition. Valuables ranging from human lives to expensive resources and sensitive data need to be tightly secured. In this present day when armed robbery has gotten more sophisticated particularly in developing countries, there is the need for tighter security means, and one of the most secured technologies that can be employed is biometrics, finger print door lock to be precise. Biometrics is the science and technology of measuring and analysing biological data, biometrics measures and analyses human body characteristics such as DNA, fingerprint, eye retina and iris, voice pattern, facial pattern and hand measurement [1]. The software that drives the microcontroller was done using the C language on MPLAB compiler, the coding was segmented into various modules; first, the module that drives the LCD screen, next is the module that drives the finger print scanner, this instructs the scanner to first register users and allow the inputted finger print to be compared with the pre-registered finger prints. The pre-registered finger prints are saved on the IC registers of the Micro controller. An alert is sounded whenever a fingerprint that is not found in the Microcontroller memory is placed on the scanner as an intruder. The construction of this project was done in three different stages, the writing of the code (driver) which controls the Microcontroller using C language, the implementation of the whole project on a solder-less experiment board, the soldering of the circuits on Vero-boards and the coupling of the entire project to the casing. The implementation of this project was done on the breadboard as a prototype, the power supply was first derived from a bench power supply in the electronics laboratory, in all the development guaranteed security for illegal intrusion of illegal entity to room, the mechanism can be implemented in a broader sense on a door where a there is restriction of access.

Source: International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013

In forensic medicine, identification of a deceased person is very important. Reliance was too often placed on visual inspection in establishing the identity of the deceased. Card acceptance devices are often limited to live subjects. Several studies proposed the usage of scanners as electronic fingerprinting of cadavers. However, to the best of our knowledge, no study had been conducted on cadavers for verification with the identity card alongside the body. We wish to propose a

standard procedure on the verification of a deceased person by using card acceptance device to match his/her fingerprint with the print embedded in the identity card. The equipment tested was Sagem Morpho smart MSO350. Methodology of the study was according to the manufacturer's instruction. This study was carried out on patients who had died from natural diseases in Hospital Sultanah Aminah. A total sample of 153 deceased persons, which comprised of 88 Malay (57.5%), 51 Chinese (33.3%) and 14 Indian (9.2%) individuals between 16 to 95 years old were included in the study. We found that the percentage of matching of fingerprint is 94.8%. It is concluded that card acceptance device is useful for the purpose of identification of a deceased person and his/her Malaysian identity card.

A latent print was developed on an aluminium window frame more than two years after it had been deposited. The ability to develop a fingerprint after such a long time is probably due to a "fixation" phenomenon to the metal frame. To understand this unusual case, we simulated the event in the laboratory.

Source: International Journal of Computer Applications (0975 – 8887) Volume 56– No.17, October 2002

These are the summaries of some of the renowned research papers, experiments, projects and case studies that we went through to shape our project- 'Smart door lock using fingerprint'.

METHODOLOGY AND MODELING

3.1 Introduction

This chapter will cover the details explanation of methodology that is being used to make this project complete and working well. Many methodologies or findings from this field mainly generated into journal for others to take advantages and improve as upcoming research on projects. The methodology refers to the overall approach that our project requires. We need to explain our project briefly, demonstrating that we comprehend the meaning of our approaches. The methods are the tools of data collection, the procedure of our project. The procedures or strategies used to find, select, process, and analyze information about a topic are referred to as methodology. [12]

In this project, we implemented a Fingerprint-Based Security System Using Arduino & Fingerprint Sensor. As thefts are increasing day by day security is becoming a major concern nowadays. So a digital fingerprint lock can secure our home or locker easily. It will open your door only when the right fingerprint is entered. Only authorized people are allowed access to the restricted sections due to a fingerprint-based door lock mechanism. The Arduino is responsible for the entire project's operation.

A particular procedure or set of procedures demonstrating the issue is massive revision of teaching methodology. In a report or article, the methodology section allows the reader to critically evaluate a study's overall validity and reliability. So, this methodology chapter explains what we did and how we did it. [17]

3.2 Circuit and Working Principle

The circuit shown in Fig. 1 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.

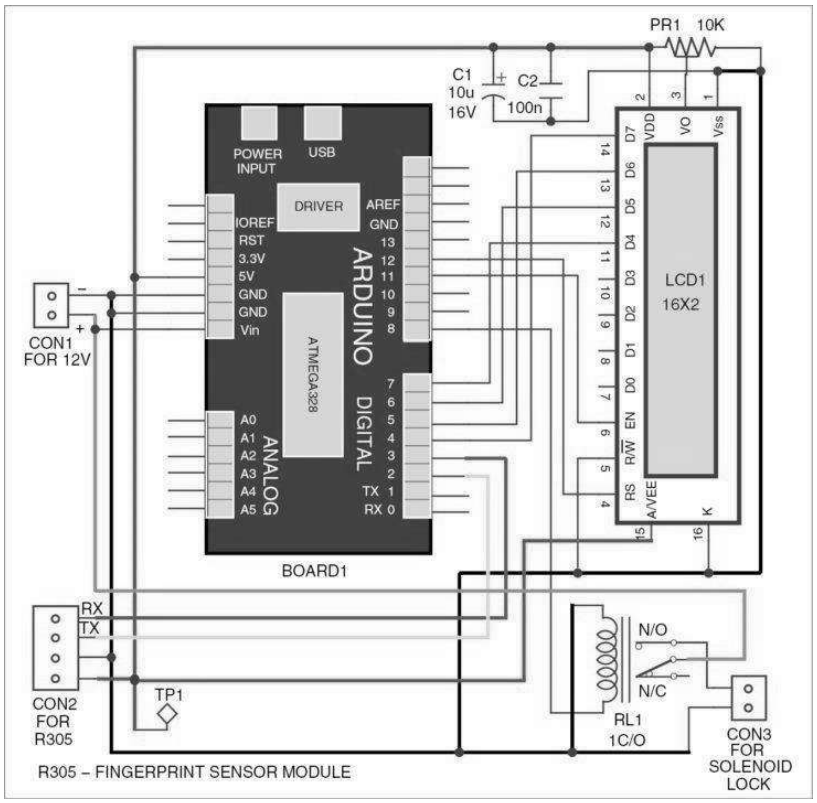


Figure-1: circuit diagram of the fingerprint door unlock system

The brain of the circuit is Arduino Uno MCU board (BOARD1). It is based on Arduino UNO R3 V1.0 and has 14 digital input/output (I/O) pins, six analogue inputs, Fingerprint sensor , a USB connection, power jack, Battery, Charger 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 max232/USB serial adaptor. The user can store fingerprint data in the module and con 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 preset (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. Preset PR1 is used to adjust the contrast of the LCD display.

3.2.1 Process of Work:

The purpose of this experiment is to implement a door-locking mechanism that opens or closes the lock on the door automatically with a key code. There are two work processes for this experiment which are:

***Case 1*: The lock will open:**

In this system, user will enter fingerprint in the fingerprint scanner which is connected to the door latch through the microcontroller. After scanning the print, the system runs its database and looks for a match. If any match is found, the latch opens and thus the door gets unlocked. Same thing happens when user wants to lock the door. Correct fingerprint makes the latch to close, locking the door behind the user.

***Case 2*: The lock will not open:**

If fingerprint is wrong, the lock will not open allowing the door to remain locked and user have to retried until the door is opened. Scanning the wrong fingerprint will automatically instruct the user to start again from the beginning.

3.3 Description of the important component:

First of all, we use Proteus software to complete the simulation. in this simulation, we've used some important components to build the whole door locked system, which are Arduino UNO R3 V1.0, LEDGREEN, LM044L 16x2 Alphanumeric Display, Fingerprint, Door Lock, 12volt Adapter, Speaker, Transistor IRFZ44N and TIP122.

3.3.1 Arduino UNO R3 V1.0

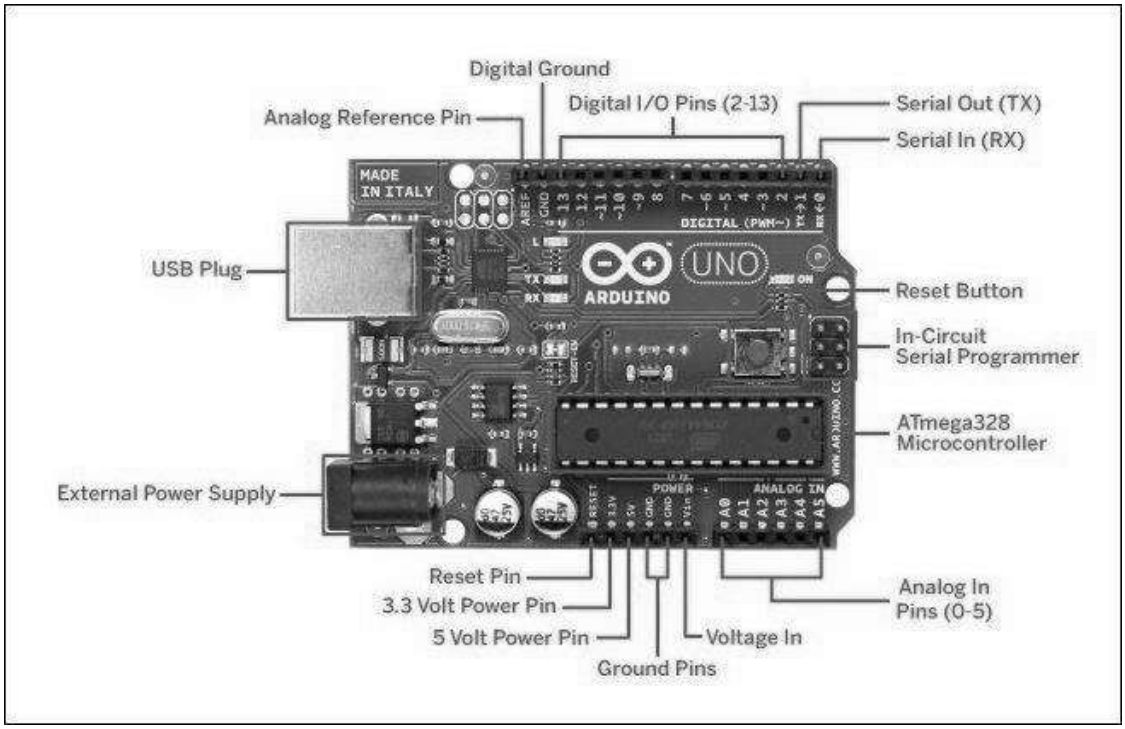


Figure-2: Arduino Uno

The Arduino UNO is the best board to get started with electronics and coding. If this is your first experience tinkering with the platform, the UNO is the most robust board you can start playing with. The UNO is the most used and documented board of the whole Arduino family.

Main Features

Arduino UNO is a microcontroller board based on the **ATmega328P**. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. You can tinker with your UNO without worrying too much about doing something wrong, worst case scenario you can replace the chip for a few dollars and start over again.

Tech Specs

Here you will find the technical specifications for the Arduino UNO R3.

Board	**Name**	**Arduino UNO R3**
	SKU	A000066
Microcontroller	**ATmega328P**	
USB connector	**USB-B**	
Pins	**Built-in LED Pin**	13
	Digital I/O Pins	14
	Analog input pins	6
	PWM pins	6
Communication	**UART**	Yes
	I2C	Yes
	SPI	Yes
Power	**I/O Voltage**	5V
	Input voltage (nominal)	7-12V
	DC Current per I/O Pin	20 mA
	Power Supply Connector	Barrel Plug
Clock speed	**Main Processor**	ATmega328P 16 MHz
	USB-Serial Processor	ATmega16U2 16 MHz

Memory	**ATmega328P**	2KB SRAM, 32KB FLASH, 1KB EEPROM
Dimensions	**Weight**	25 g
	Width	53.4 mm
	Length	68.6 mm

[23]

3.3.2 Fingerprint

Figure-3: Fingerprint

Nothing is completely secure. Locks can be picked, safes can be broken into, and online passwords can be guessed sooner or later. How, then, can we protect the things that we value? One way is to use biometrics—fingerprints, iris scans, retinal scans, face scans, and other personal information that is more difficult to forge. Not so long ago, if you'd had your fingerprints taken, chances are you were being accused of a crime; now, it's innocent people who are turning to fingerprints to protect themselves. And you can find fingerprint scanners on everything from high-security buildings to ATM machines and even laptop computers. Let's take a closer look at how they work!

What can you use fingerprint scanning for?

Fingerprint scanning is the most popular biometric technology (used in over half of all biometric security systems)—and it's easy to see why. We store more and more information on our computers and share it, online, in ever much risky ways. Much of the time, our bank information and personal details are protected by just the few hastily thought-out numbers in our passwords. Anyone can use your credit or debit card to get money from an ATM (automated teller machine or "cashpoint") if they know just four numbers!

In future, it will be much more common to have to confirm your identity with biometric information: either your fingerprint, a scan of the iris or retina in your eye, or a scan of your face. Some laptop computers and most smartphones now use fingerprint scanning to make them more secure. Large banks, such as Bank of America and JPMorgan Chase, have introduced fingerprint authentication as part of the sign in process for their smartphone apps. Soon we could be seeing fingerprint scanners on ATMs, in airport security scanners, on checkouts in grocery stores, in electronic voting systems, and perhaps even replacing the keys in our (self-driving) automobiles!

Some people don't like the sound of a "Big Brother" society where you have to do everything with your fingerprints—and it's true that there are important issues of privacy. But humans have always used biometrics for personal identification: we tell one another apart chiefly by recognizing one another's faces and voices. Worry about the drawbacks, by all means, but don't forget the advantages too: your information should be much more secure from criminals—and you'll never again have the problem of losing your keys or forgetting your password![24]

3.3.3 Solenoid Electric Door Lock

Figure-4: Solenoid Electric Door Lock

12V Solenoid lock are basically electromagnets: they are made of a big coil of copper wire with an armature (a slug of metal) in the middle. When the coil is energized, the slug is pulled into the center of the coil. This makes the solenoid able to pull from one end.

This solenoid lock in particular is nice and strong, and has a slug with a slanted cut and a good mounting bracket. It's basically an electronic lock, designed for a basic cabinet or safe or door. Normally the lock is active so you can't open the door because the solenoid slug is in the way. It does not use any power in this state. When 9-12VDC is applied, the slug pulls in so it doesn't stick out anymore and the door can be opened.

The solenoid lock come with the slanted slug as shown above, but you can open it with the two Phillips-head screws and turn it around so its rotated 90, 180 or 270 degrees so that it matches the door you want to use it with.

To drive a solenoid lock with an Arduino you will need a relay module fairly good power supply, as a lot of current will rush into the solenoid to charge up the electro-magnet, about 500mA, so don't try to power it with a 9V battery![25]

3.3.4 16x2 LCD Display

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

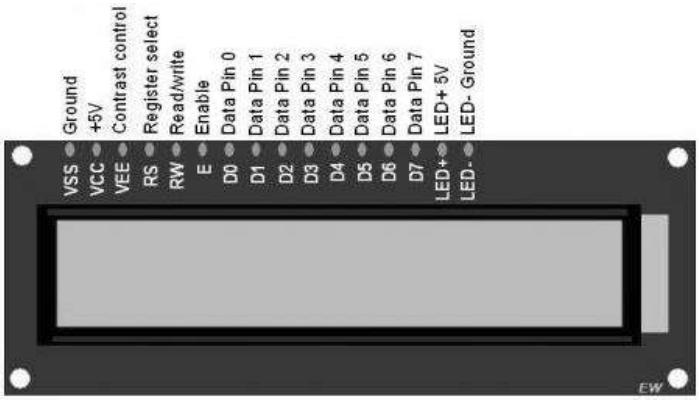


Figure-5 :16X2 LCD Display

LCD 16×2 Pin Diagram

The 16×2 LCD pinout is shown below.

- Pin1 (Ground/Source Pin): This is a GND pin of display, used to connect the GND terminal of the microcontroller unit or power source.
- Pin2 (VCC/Source Pin): This is the voltage supply pin of the display, used to connect the supply pin of the power source.
- Pin3 (V0/VEE/Control Pin): This pin regulates the difference of the display, used to connect a changeable POT that can supply 0 to 5V.
- Pin4 (Register Select/Control Pin): This pin toggles among command or data register, used to connect a microcontroller unit pin and obtains either 0 or 1(0 = data mode, and 1 = command mode).
- Pin5 (Read/Write/Control Pin): This pin toggles the display among the read or writes operation, and it is connected to a microcontroller unit pin to get either 0 or 1 (0 = Write Operation, and 1 = Read Operation).
- Pin 6 (Enable/Control Pin): This pin should be held high to execute Read/Write process, and it is connected to the microcontroller unit & constantly held high.
- Pins 7-14 (Data Pins): These pins are used to send data to the display. These pins are connected in two-wire modes like 4-wire mode and 8-wire mode. In 4-wire mode, only four pins are connected to the microcontroller unit like 0 to 3, whereas in 8-wire mode, 8-pins are connected to microcontroller unit like 0 to 7.
- Pin15 (+ve pin of the LED): This pin is connected to +5V
- Pin 16 (-ve pin of the LED): This pin is connected to GND.

Features of LCD16x2

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 [26]

3.3.5 Transistor IRFZ44N

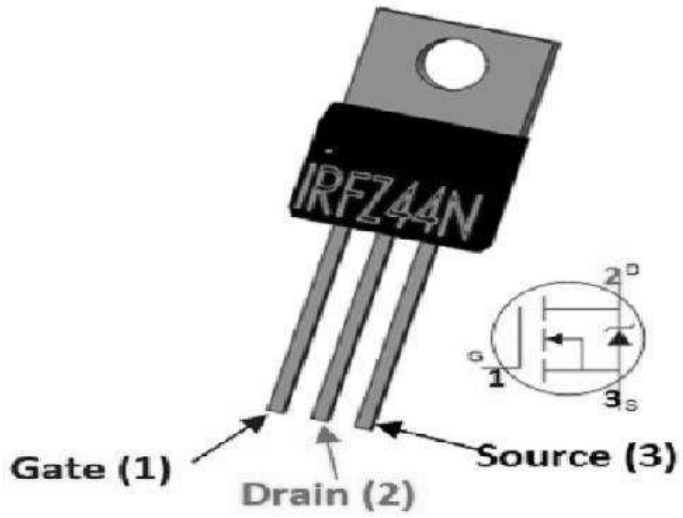


Figure -6: Transistor IRFZ44N

The **IRFZ44N** is a **N-channel MOSFET** with a high drain current of 49A and low Rd value of 17.5 mΩ. It also has a low threshold voltage of 4V at which the MOSFET will start conducting. Hence it is commonly used with microcontrollers to drive with 5V. However, a driver circuit is needed if the MOSFET has to be switched in completely.

Pin Number	Pin Name	Description
1	Gate	Controls the biasing of the MOSFET
2	Drain	Current flows in through Drain

3	Source	Current flows out through Source

Features and Specifications

- Small signal N-Channel MOSFET
- Continuous Drain Current (ID) is 49A at 25°C
- Pulsed Drain Current (ID-peak) is 160A
- Minimum Gate threshold voltage (VGS) is 2V
- Maximum Gate threshold voltage (VGS) is 4V
- Gate-Source Voltage is (VGS) is ±20V (max)
- Maximum Drain-Source Voltage (VDS) is 55V
- Rise time and fall time is about 60ns and 45ns respectively.
- It is commonly used with Arduino, due to its low threshold current.
- Available in To-220 package [270. [29]

3.3.6 Transistor TIP122

Figure-7: Transistor TIP122

The **TIP122** is a Darlington pair NPN transistor. It functions like a normal NPN transistor, but since it has a Darlington pair inside it has a good collector current rating of about 5A and a gain of about 1000. It can also withstand about 100V across its collector- Emitter hence can be used to drive heavy loads.

Pin Number	Pin Name	Description
1	Base	Controls the biasing of transistor, Used to turn ON or OFF the transistor
2	Collector	Current flows in through collector, normally connected to load
3	Emitter	Current Drains out through emitter, normally connected to ground

Features

- Darlington Medium-power NPN Transistor
- High DC Current Gain (hFE), typically 1000
- Continuous Collector current (IC) is 5A
- Collector-Emitter voltage (VCE) is 100 V
- Collector-Base voltage (VCB) is 100V
- Emitter Base Voltage (VBE) is 5V
- Base Current(IB) is 120mA
- Available in To-220 Package.[27]

3.3.7 Speaker

Figure-8: Speaker

Information

- Speakers - Sturdy steel construction with easy-to-solder lugs and 3.3 mm mounting holes. These speakers are often used in commercial flat screen monitors.
- PAM8403 - This top of the line class D amplifier mounted on a breakout board pairs perfectly with the speakers to provide great sound.
- Speaker specs:
  -4 ohm, 3 watt power
  -Wires already attached
  -31 mm wide, 70 mm high, 18 mm deep.
  -4 mounting holes, 3 mm diameter.
- PAM8403 specs:
  -Operation Voltage: 5V. Get power from USB supply, 3 AA batteries, or cell phone battery bank (power supply not included)
  -Output power: 3w + 3w (3 watts to each speaker)
  -Efficiency: up to 90%
  -Knob: smooth turning knob to adjust volume and turn unit on / off
  -Mounting: drill a hole and mount using the volume knob with the included nut and washer
  -Includes breakaway headers for connection, soldering required

Connections:

- Refer to diagram picture for wiring
- Note: do not connect (-) or (+) speaker connections together, this will damage the amplifier
- Note: do not apply power without speakers connected, this will damage the amplifier.[30]

3.3.8 12 Volt Adapter

Figure-9: 12 Volt Adapter

Professional 12 Volt DC 1 Amp power supply is suitable for powering a wide range of applications including CCTV cameras and wireless routers. Features: 100% Brand New Excellent Quality Short Circuit, Over Voltage & Over Current Protection. Meet CEC Energy Efficiency Level IV. Incredibly Low Fault Rates No Minimum Load. This power supply is a regulated Center Positive power supply and has a 2.1mm x 5.5mm Jack It's plug design is for Indian power socket. So, no plug converter is required. Compact size & light weight. High Reliability. Regulated Stable Voltage. Good quality SMPS Based Adapter Power LED Monitor (LED Glow when in Use)

Stabilized Output, low ripple & low interference Single Output Voltage High Efficiency & low energy consumption Input - 100-240 VAC 50/60hZ Category - Switch Mode Power Adaptor (SMPS) Output Type - DC Output - 12Volts 1Amp **PLEASE NOTE THAT DESIGN AND COLOR MAY CHANGE FROM THE PICTURE SHOWN ABOVE** Applications: Powerful 12v 12w 1A max Current Draw. Replaces lower amped adapters 12v 0.5A 1A. 1.5A etc. Smart Replacement Gadget Power Supply for LED, SMD, LED Strip, RGB LED Strip Ideal for Routers / Modems / Mobile Phones / Mp3 players / POS Machines etc. Best for Routers, Wi-Fi Routers security/spy camera receiver and some advanced cameras CCTV, Gadgets, Portable Players, Set Top Boxes, best for Toys etc., Charging or any gadgets as per the rating of the device, please study and then buy as this a very technical item only works as per its precise current outputs This power supply is an ideal replacement for a wireless network router such as the Net-gear DG834, DG834GT, DG934 etc. plus a range of many other wireless routers. You will need to check the DC socket size & power rating with the supplier of the router you are using as we can't confirm it will work.

Features:

- Excellent Quality
- Short Circuit, Over Voltage & Over Current Protection
- Meet CEC Energy Efficiency Level IV
- Incredibly Low Fault Rates
- Smart Replacement Gadget
- Power Supply for LED, SMD, LED Strip, RGB LED Strip
- Ideal for Routers / Modems / Mobile Phones / Mp3 players / POS Machines etc
- No Minimum Load
- This power supply is a regulated Center Positive power supply and has a 2.1mm x 5.5mm Jack
- It's plug design is for Indian power socket so, no plug converter is required
- Compact size & light weight
- High Reliability
- Regulated Stable Voltage

- Good quality SMPS Based Adapter
- Power LED Monitor (LED Glow when in Use)
- Stabilized Output, low ripple & low interference
- Single Output Voltage
- High Efficiency & low energy consumption. [27]

3.3.9 LEDGREEN

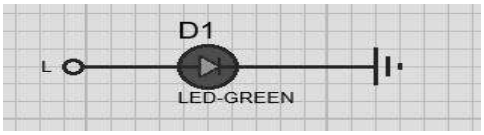
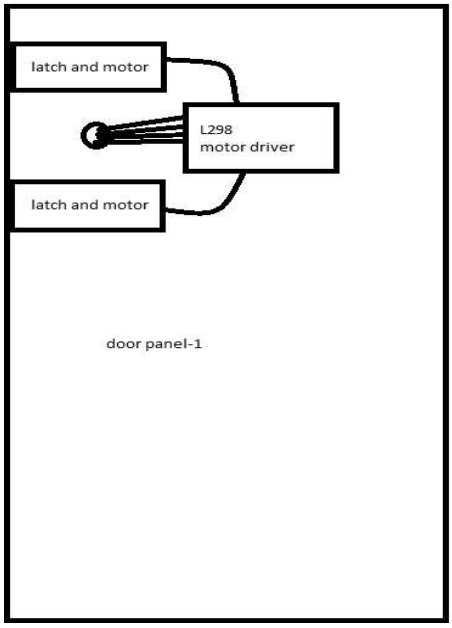


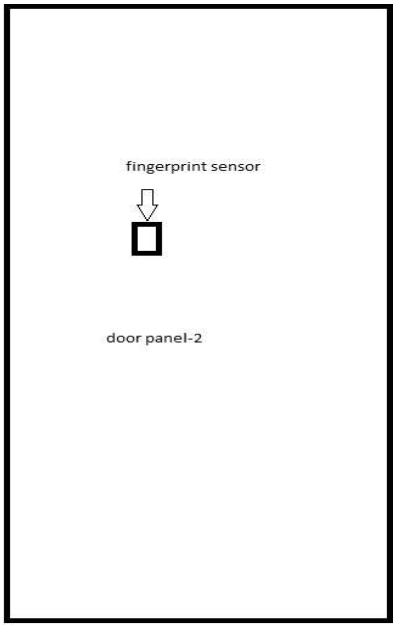
Figure-10: LEDGREEN

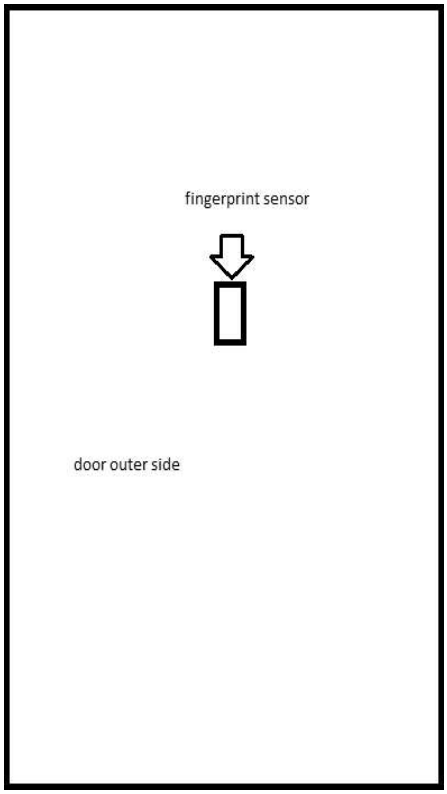
At LED **Green** Light International, we understand that LED lighting is the foundation of energy efficient, environmentally responsible and sustainable lighting technology.

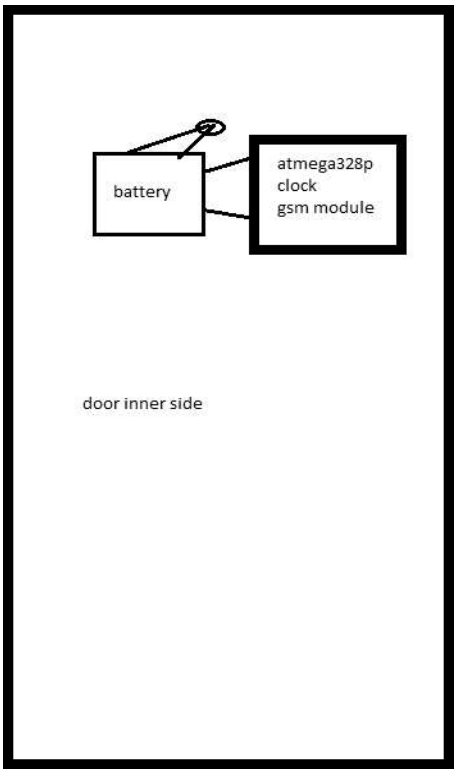
That's why we design and market the most innovative and advanced LED lighting solutions for our customers – encouraging them to "**go green**" using advanced LED and Controls Products for every possible lighting application. [30]

3.4 Architectural Design:









3.5 Implementation

To implement the Smart Parking System, we have used Proteus professional 8.12 simulating software and Arduino IDE. 9 shows the simulation implementation of the project.

Firstly, A new project created without any firmware in proteus. After creating the blank new project, there will be a schematic diagram window. In this schematic window, the simulation circuit is constructed. All of the devices used here, were found under pick device option. Arduino UNO R3 V1.0 was chosen as microcontroller board for Fingerprint door lock system. This system works on the basis of some major components such as Arduino UNO R3 V1.0, LEDGREEN, LM044L 16x2 Alphanumeric Display, Fingerprint, Door Lock, 12volt Adapter, Speaker, Transistor IRFZ44N and TIP122 had used in this project.

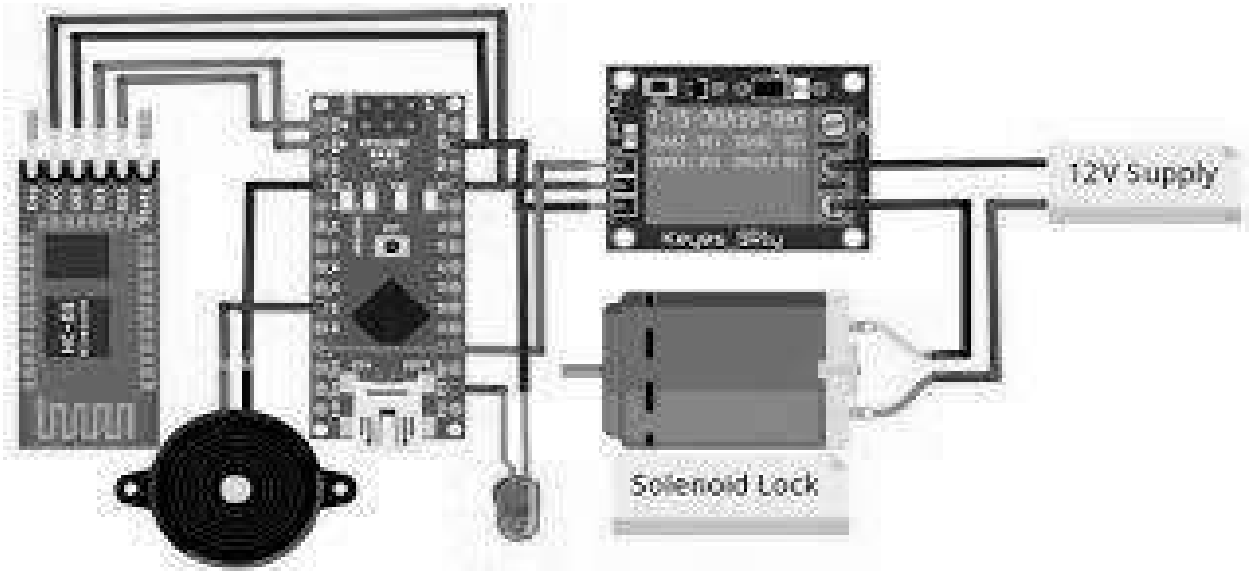


Figure-11: Complete Circuit Diagram in Proteus

Figure-12: The code window on Arduino IDE

Figure-13: The code window on Arduino IDE

After setting up the components as 10, we went to Arduino IDE and installed all the necessary libraries to run the project successfully. Then the codes/commands were written and uploaded to the Arduino Board. After upload finely, the code worked without any errors.

3.6 Test/Experimental setup:

While doing the setup, the project was evaluated that every functionality is accomplished or not. The code was edited as proposed requirements.

Figure-14: Hex File in Arduino IDE

After running the instruction code finely, there will be a .HEX file found under IDE's compiler console and this file location should be copied. In proteus, double click in the Arduino board and in the program file section, paste the link without any change. Click ok and run the simulation. The system will run expectedly. All the output was observed while running the simulation as like following.

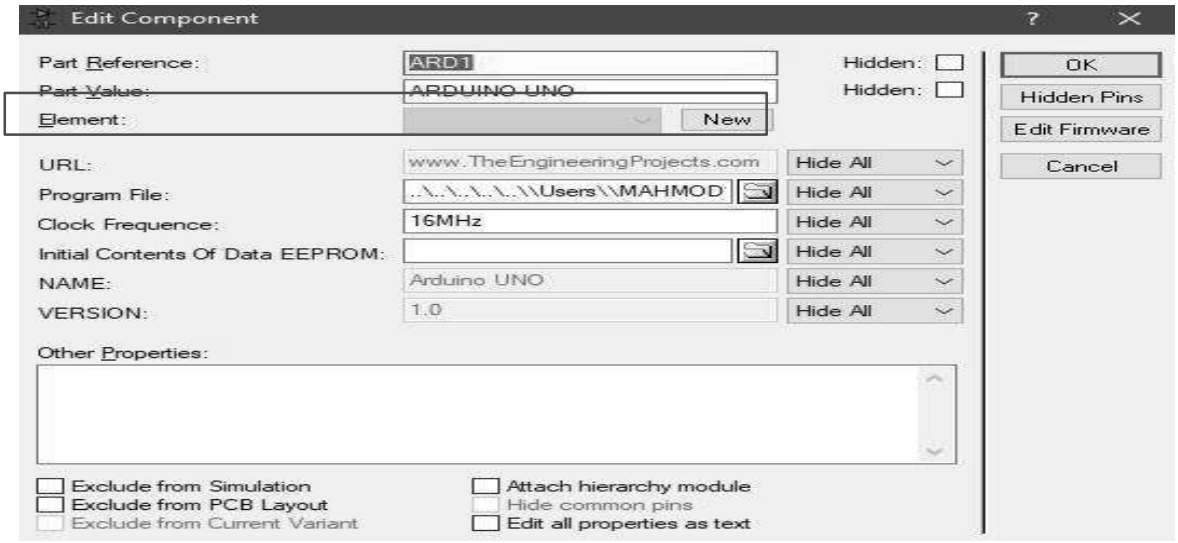


Figure-15: The program file location for Arduino

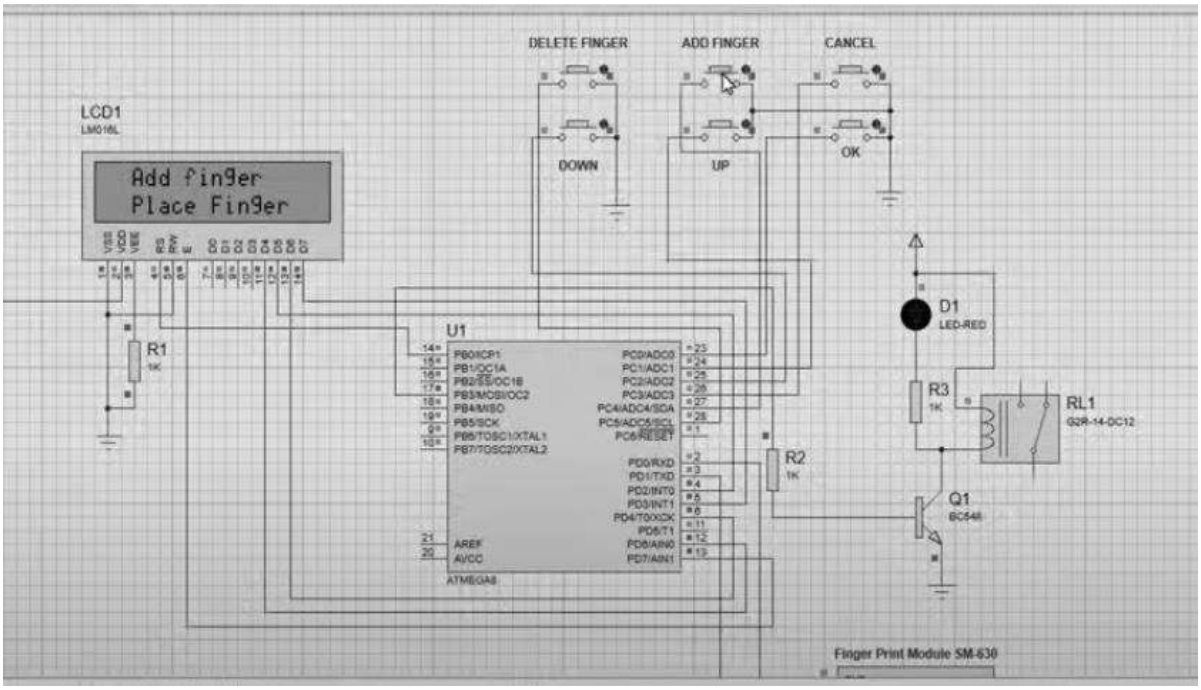


Figure-16: After simulation run successfully

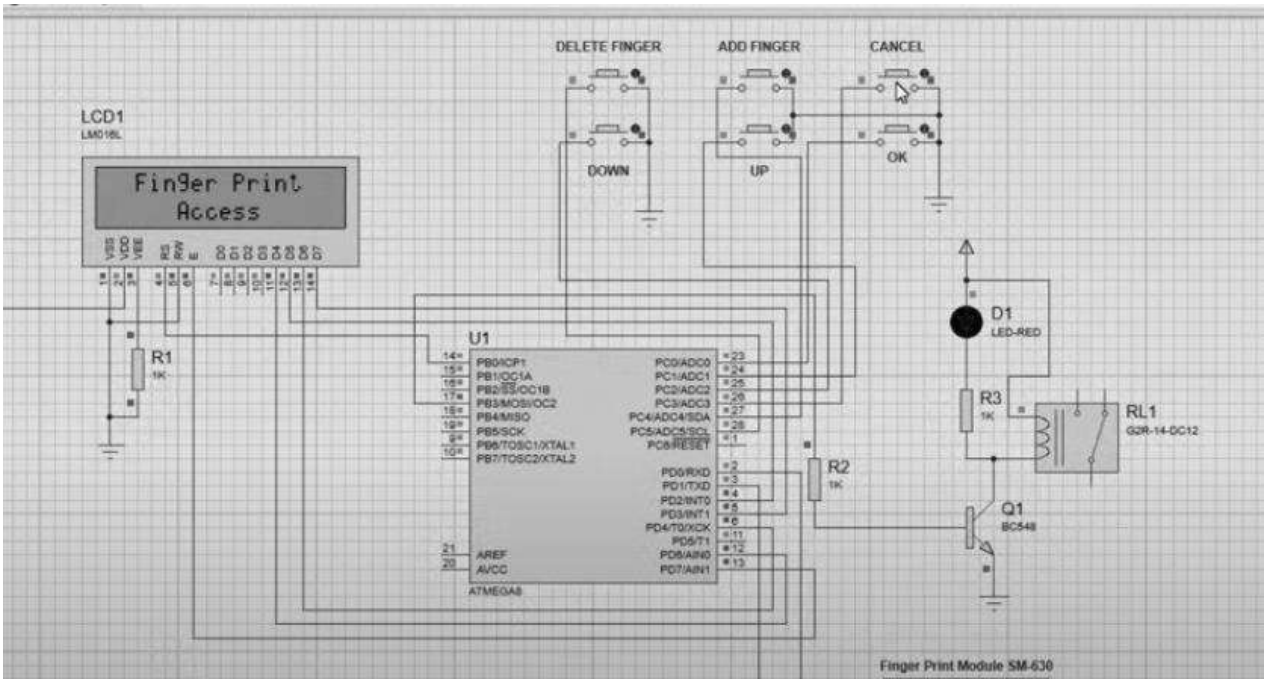


Figure-17: On giving the correct fingerprint

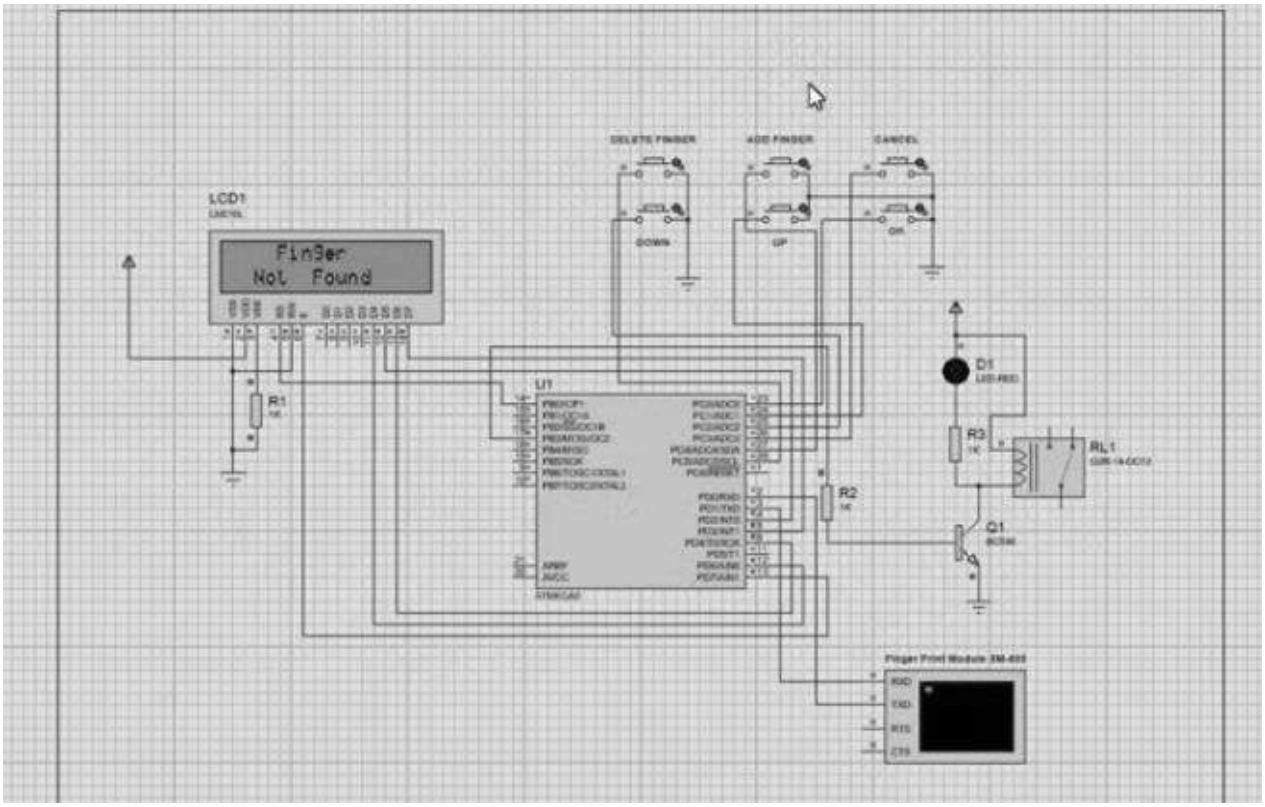


Figure-18: On giving the wrong fingerprint

3.7 Cost analysis:

The costs of each individual component are listed here:

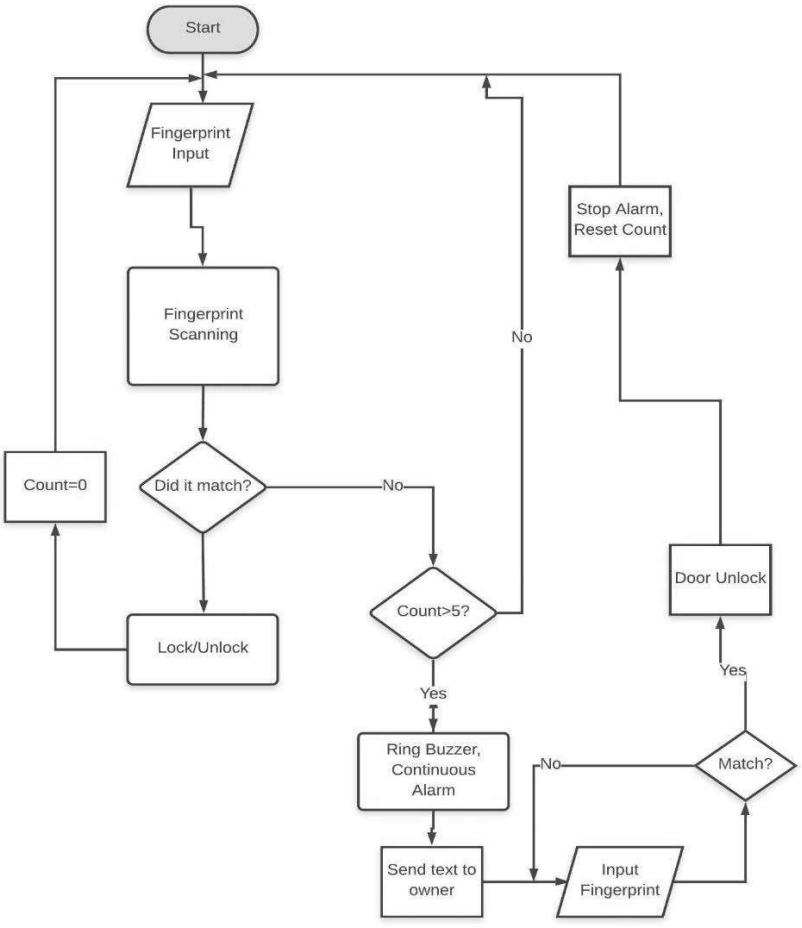
Item	Quantity	Price (Taka)
Arduino UNO Board	1	700/=
16x2 LCD	1	300/=
Fingerprint Sensor	1	1300/=
Electrical Door Lock	1	1100/=
Battery	1	200/=
Charger	1	150/=
Wire	1	50/=
Sound System	1	200/=
Total		4000/=

Here, the total cost is BDT 4000/=. Here we tried to keep the cost minimal and used better components to implement the circuit. This budget will not so over for such a sustainable system with good components. We used less wire and other unnecessary components to complete the project.

RESULTS AND DISCUSSION

The Fingerprint door lock using Arduino, we are showing the components and connected them to the power supply. This system is based for improving the security which will register the owner's fingerprint into the Arduino using the fingerprint sensor, and this system we have given 5v power supply to Arduino through the code uploading wire. When you put your thumb on fingerprint sensor after registering yourself the lock will be unlocked and you repeat this process again then the solenoid lock will be got locked. The process of locking and unlocking requires less than 1 second so this is why the Solenoid lock is used inside this project. [13]

4.1 Flow-chart of system:



4.2 Performance Evaluation

Compared to a traditional secured system, our fingerprint door lock system is advanced, efficient and more secured. A normal security system is comprised of locks, which in contact with the appropriate keys, get unlocked. In our system, an authorized and correct fingerprint is the only key to unlocking the secured lock system.

Lock systems are very necessary in our day to day life. In order to secure important and personal belongings as well as one's privacy, there is no alternative to lock and key. But the type of the system implemented, tells a lot about the extent to which something can be and will be secured. Fingerprint door lock system is a biometric lock in which fingerprint interface is used as the key to unlock. It is safer and more secured as fingerprints are unique and cannot be copied. There are some basic differences between locking systems of many kinds. Traditional lock and key system, fingerprint lock system, password/pin code system, biometric lock system are some of the security system one can simply implement for security purpose. The pros and cons of each system makes them efficient, secured, differentiable and hard to break. Some basic differences in performance and system structure between these security systems are as follows:

Table 1. Differences between different types of lock systems

Types of differences	**Lock & key**	**Biometric Lock**	**Fingerprint Lock**
Composition	Composed of simply lock and its key	Composed of LCD display, number pad, fingerprint scanner and/or retina scanner.	Composed of LCD display, fingerprint scanner and GSM module.
Interfaces	Key	Fingerprint and/or retina	Fingerprint
Function	Unlocks by key only	Unlocks by fingerprint and/or retina scan	Unlocks by fingerprint
Performance	Low	Very high	High
Strength	Moderate	Very high	High
Efficiency & vulnerability	Less effective and highly vulnerable	Very effective and less vulnerable	Highly effective and less vulnerable

From the chart above, it is quite clear that security systems should have unique interface entities like fingerprint, retina, palm-print, voice-recognition etc. to make the system more complicated, secured and effective.

Compared to traditional and other similar security systems like biometric, palm-print, voice-recognition systems, our proposed system i.e. fingerprint lock system with GSM functionality is highly useful and secured. It not only stops unauthorized access but also informs the owner of any intrusion and burglary and at the same time alerts the intruder.[16]

4.3 Graphical Representation

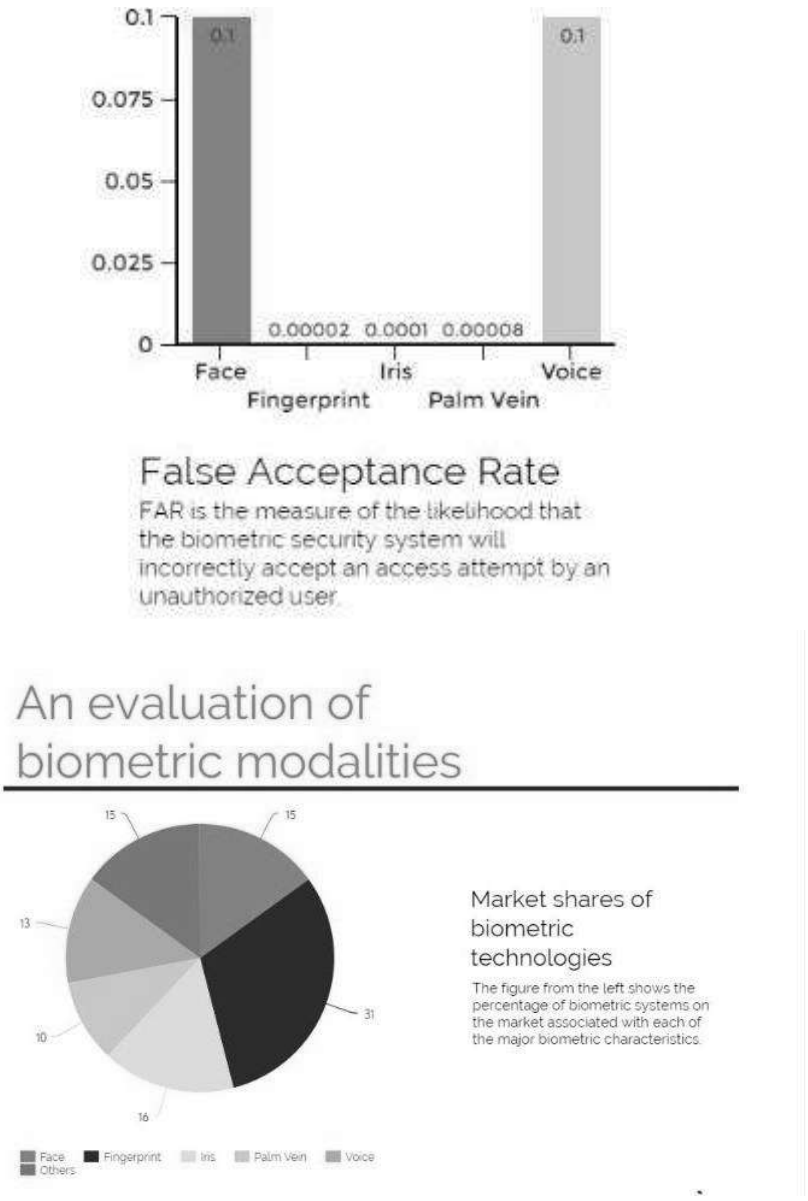


Figure 19: Graphical comparison of different biometric lock systems

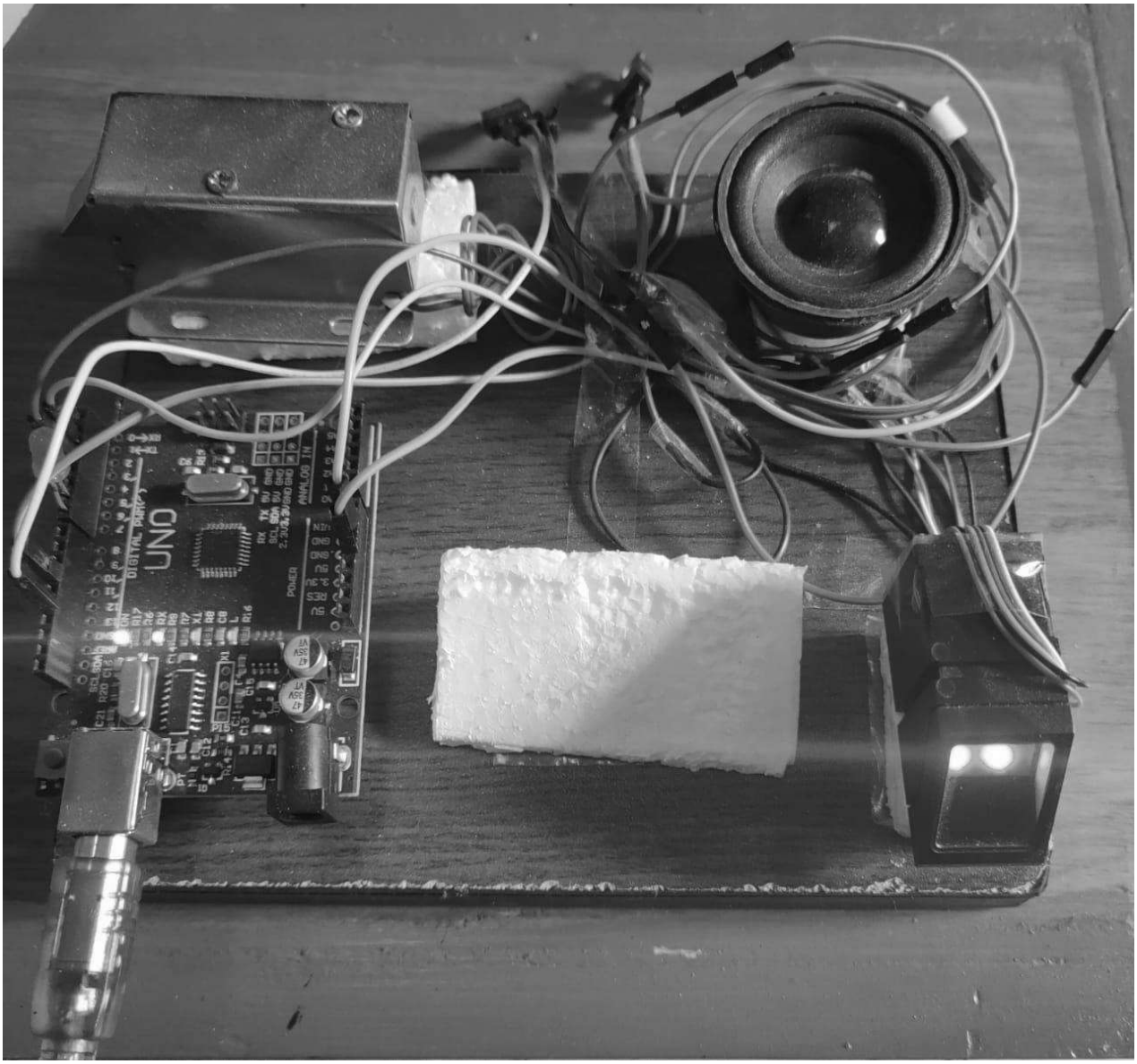


Figure 20: Connected Circuit.

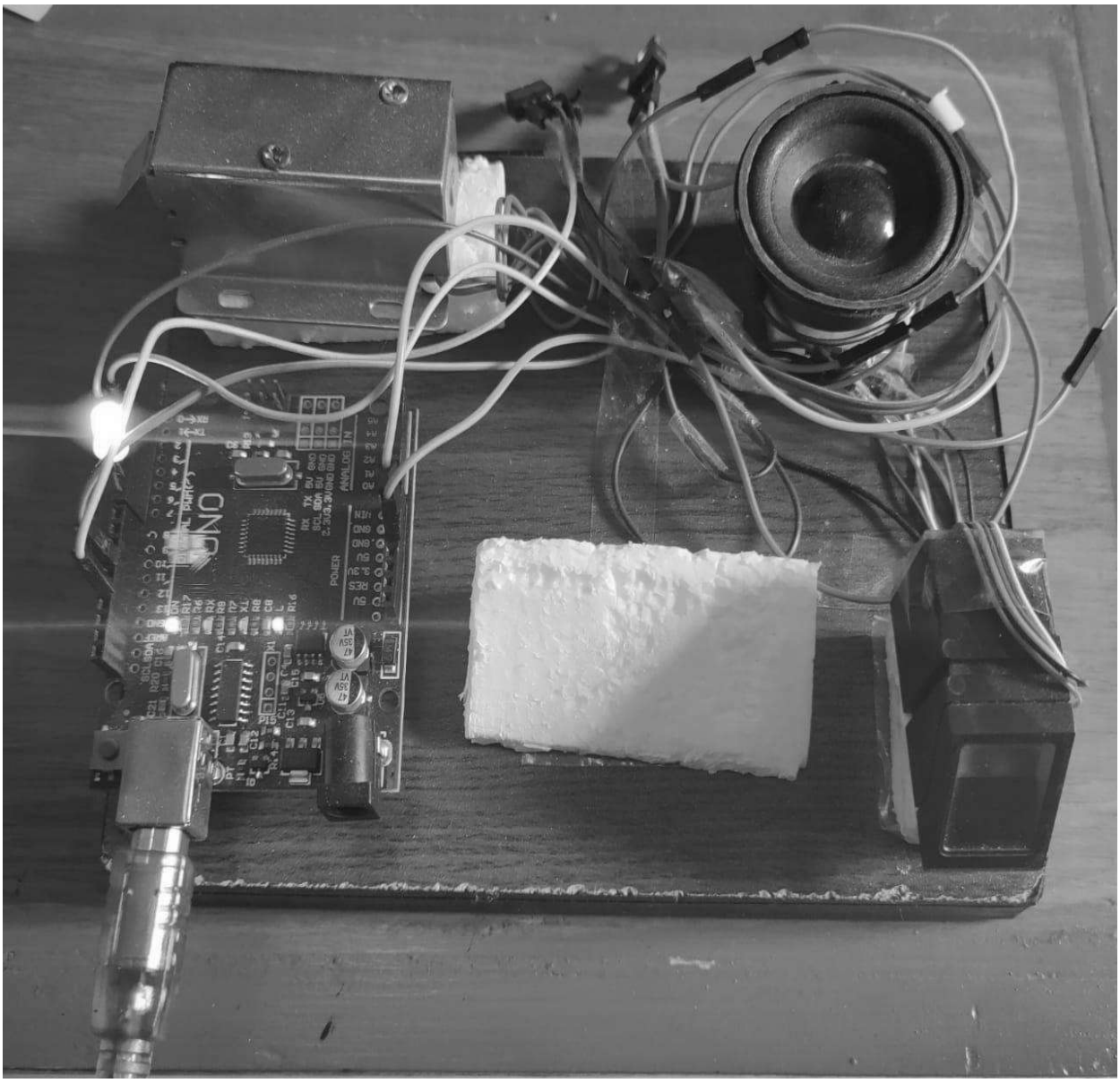


Figure 21: Actual Working Model

CONCLUSIONS AND FUTURE WORK

5.1 Conclusion

The design and implementation of fingerprint-based door lock system is customizable and flexible. This door locking mechanism is comparatively cost-effective than the available lock systems in the traditional market. Our fingerprint-based lock system has high accuracy rate and is also quick to recognize fingerprints which enable seamless integration with the users 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 we planned to develop a system that should be affordable to both large and small firms. This design can be improved by more intensive development and additional features such as more locks can be added to the system. Thus we do not need to spend so much for just one lock if this can be used to control several doorways. A system to save prints without the use of a computer could have been made, but it will require more parts than the ones we used. In order to maintain security properly, the whole mechanism should be placed inside the door panel or on the other side of the door. A system for batteries could also be made or even solar powered. One of the main advantages of this system is its flexibility. Several other systems can be implemented with this system. The system is very secure. Fingerprints are unique and the sensor is able to identify all of the prints during testing. It provides greater control for access to restricted places. There are some drawbacks of this system such as this system is complicated and difficult to make any change in the hardware as it is a closed system. Also it needs high power to operate so providing continuous power through batteries is a challenge sometimes. A power failure will make it unworkable. In that case, we can, connect the system with an IPS or add rechargeable batteries to the system. [21]

5.2 Future Scope

In future, alarm will be introduced. When intruder tries to break the door, the vibration is sensed by sensor which makes an alarm. This will inform the neighbors about intruders and this will help to take further action to prevent intruder from entering.

5.3 APPLICATIONS

- Very high accuracy.
- Is the most economical biometric PC user authentication technique.
- Easy to use.
- Small storage space required for the biometric template, reducing the size of the database memory required
- It is standardized.

REFERENCES

[1] "(PDF) Password Based Door Lock System Using Arduino," Research Gate. https://www.researchgate.net/publication/330998913_Password_Based_Door_Lock_System_Using_Arduino (accessed Aug. 08, 2021).

[2] Meenakshi, N, M Monish, K J Dikshit, and S Bharath. "Arduino Based Smart Fingerprint Authentication System." In 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), 1–7. CHENNAI, India: IEEE, 2019.

[3] Patil, Karthik A, Niteen Vittalkar, Pavan Hiremath, and Manoj A Murthy. "Smart Door Locking System Using IoT" 07, no. 05 (2020): 5.

[4] Reddy, R Sai Charan, P Vamsi Krishna, M Krishna Chaitanya, M Neeharika, and K Prabhakara Rao. "Security System Based on Knock Pattern Using Arduino and GSM Communication" 4, no. 1 (2018): 5.

[5] Areed, Marwa F. "A Keyless Entry System Based on Arduino Board with Wi-Fi Technology." Measurement 139 (June 2019): 34–39. https://doi.org/10.1016/j.measurement.2019.02.028.

[6] Kishwar Shafin, Md., Kazi Lutful Kabir, Nazmul Hasan, Israt Jahan Mouri, Samina Tasnia Islam, Lazima Ansari, Md. Mahboob Karim, and Md. Afzal Hossain. "Development of an RFID Based Access Control System in the Context of Bangladesh." In 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 1–5. Coimbatore, India: IEEE, 2015.

[7] Anil K. Jain, Arun Ross and Salil Prabhakar. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics, Vol. 14(1), January, 2004.

[8] R. P. Wildes. Iris recognition: an emerging biometric technology. Proceedings of the IEEE, vol. 85, no. 9, pp. 1348-1363, September, 1997.

[9] Anil K. Jain, Jianjiang Feng and Karthik Nandakumar. Matching Fingerprints. IEEE Computer, 43(2), pp. 36-44, February, 2010.

[10] Mary Lourde R and Dushyant Khosla. Fingerprint Identification in Biometric Security Systems. International Journal of Computer and Electrical Engineering, 2(5), October, 2010.

[11] Fernando L. Podio. Personal authentication through biometric technologies. Proceedings 2002 IEEE 4th International Workshop on Networked Appliances (Cat. No.02EX525), Gaithersburg, MD, 2002, pp. 57-66.

[12]] Malabika Sarma has presented the Fingerprint Based Door Acess using Arduino.

[13] Sai K Yashwant has presented the iLock: State-of-the-art Sophisticated Door Lock for Wireless Devices.

[14] Jayasree Baidya has presented the Design and implementation of a fingerprint-based lock system for shared access.

[15] Karma Toshomo has presented Dual Door Lock System Using Radio-Frequency Identification and Fingerptint Recognition.

[16] Meenakshi N, Monish M, Dikshit KJ, Bharath S. Arduino Based Smart Fingerprint Authentication System. In year 2019 the 1st International Conference on Innovations in Information and Communication Technology (ICIICT) 2019 Apr 25 (pp. 1-7). IEEE.

[17] Baidya J, Saha T, Moyashir R, Palit R. Design and implementation of a fingerprint based lock system for shared access. In year 2017 the IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC) 2017 Jan 9 (pp. 1-6). IEEE.

[18] Anu, Bhatia D. A smart door access system using finger print biometric system. International Journal of Medical Engineering and Informatics 2. 2014 Jan 1;6(3):274-80.

[19] Afolabi A, Alice O. On Securing a door with finger print biometric technique. Transactions on Machine Learning and Artificial Intelligence. 2014 Apr 11; 2:86- 96.

[20] Gupta RP. Implementation of Biometric Security in a Smartphone based Demotics'. In year 2018 The International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) 2018 Oct 12 (pp. 80-85). IEEE.

[21] Anu, Bhatia D. A smart door access system using finger print biometric system. International Journal of Medical Engineering and Informatics 2. 2014 Jan 1;6(3):274-80.