Design and Simulation of A Fingerprint Based Door Unlock System

J.Dhanasekar[1], L.Navaneethan[2], A.MohanRaj[3], M.Praveen Kumar[4], A.Lingaraj Bharathi[5]
[1]Assistant Professor, Dept of Electronics And Communication Engineering
[2, 3, 4, 5]Dept of Electronics And Communication Engineering
[1, 2, 3, 4, 5] Tamil Nadu, (State), INDIA

Abstract- *Security has always been a major concern for the households and the office environment, and for this concern various approaches are in place to address the problem. Most of the major door lock security systems have several loopholes which could be broken down to gain access to the desired places, and it creates a concern for a secure lifestyle and proper working environment. Additionally, terrorism and unauthorized access to places have become a major issue now-a-days, and there is a need for a secure system to prevent unauthorized access especially in shared access environment. With this consideration, a design and prototype of a biometric fingerprint based door lock system has been presented in this paper. Biometric systems such as fingerprint provide tools to enforce reliable logs of system transactions and protect an individual's right to privacy. The RFID or password based door lock mechanisms can easily be compromised when the RFID card or passwords are shared or stolen, thus for facilities with shared access require biometric based secure system. In the proposed system, fingerprints of the authorized users are enrolled and verified to provide access to a facility that is used by multiple users. A user can also be removed and a new user can be enrolled in the system. This is an Arduino NANO device based flexible working device that provides physical security using the fingerprint sensor technology.*

Keywords- Arduino Nano, Arduino IDE, Proteus 8 professional, Keypad module, Servo Motor.

I. INTRODUCTION

Recently, there has been recorded tremendous increase in the crime rate everywhere in the world. This issue is turning more severe every day. 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 confidential belongings manually. Instead, He finds an alternative solution which provides better, reliable and atomized security. This is an era where everything is connected through network, where anyone can get hold of information from anywhere around the world. Thus chances of one's info being hacked are a serious issue. Due to these risks it's very important to have some kind of personal identification to access one's own info. Now a day's personal identification is becoming an important issue all around. Among mainstream personal identification methods 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.To get away with this problem, we decided to take help from technology and there this project "Arduino Fingerprint Sensor Lock" developed. We know the saying very well- 'Prevention is better than cure', rather than to face the loss it is much better to take necessary actions to eradicate that issue before it happens.

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 based 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 system he 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 the 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 project helps us to implement the fact. The reason behind the fact that project has gained so much popularity in a short interval is mostly because of its simplicity and attractive feature. Today, fingerprint project is linked with security and major task, later it may be employed as fingerprint based driving license, bank accounts operation and so on.

'Matching Algorithm' is the main principle of this project where specified templates of fingerprints are initially stored. Then, the fingerprint of user is compared with the pre-stored templates of fingerprints. It verifies authentication process.

The old practice of using a simple key to unlock a door is time consuming as well as less secure. Replacing those methods with fingerprints, we get access inside a house/room just by placing the correct finger on the sensor. However, only authorized people can open the door because of the special fingerprint technique. If the fingerprint matches with any one of the image from database, the door unlocks.

II. EXISTING SYSTEM

- In the existing system most of the bank transaction process had done by giving the Username and password.
- Customer ID has used in previous system for the security process .
- There are many security problems like fraudulent websites, fake emails from banks, capturing user IDs and passwords, hacking personal bank accounts and steal money etc.
- Deadbolt System
- Password-Authentication
- RFID reader authentication
- Face detector lock
- Retinal scanner
- Iris scanner
- Voice recognition

III. PROPOSED SYSTEM

Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Today, a fingerprint scanner costs about USD 20 when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications. The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small- to medium-scale identification systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities. This is a perfect solution for protecting one from the hassle of stolen/lost key or an unauthorized entry.

1) Fingerprint based Door Lock

Our proposed fingerprint based lock system is a reliable and very secure lock that will not only ensure safer environment but also ease lifestyle. This system can prove very useful in housing buildings, large offices, universities and so on. Because it offers the flexibility to add more features to the system. Users do not need to implement many systems from scratch. They can simply use our fingerprint lock system because fingerprint scanning is more accurate and cost effective method. It is also secure because fingerprint duplication is virtually impossible. Additionally, we have also used password authentication system for security purposes.

2) Fingerprint Identification

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. 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 finger have been shown to be identical. The three basic pattern of fingerprint ridges are the arch, loop, and whorl.

- Arch: The ridges enter from one side of the finger, ris in the center forming an arc, and then exit the other side of the finger.
- Loop: The ridges enter from one side of a finger, form curve, and then exit on that same side.
- Whorl: Ridges form circularly around a central point on the finger. In the whorl pattern, ridges form

circularly around a finger.

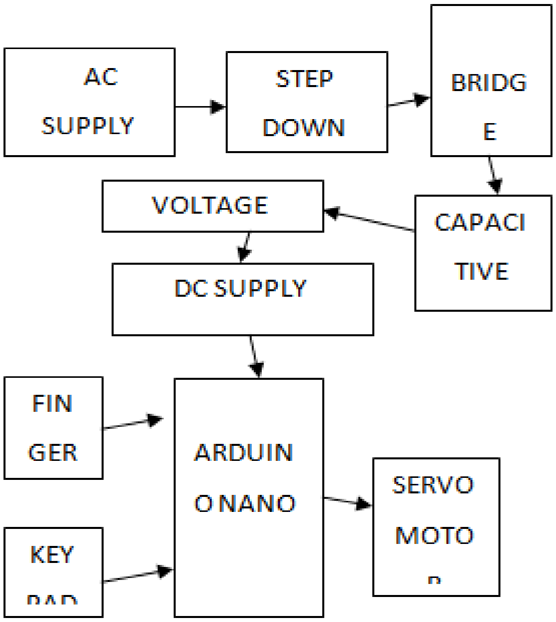
A fingerprint recognition system can be used for both verification and identification. In verification, the system compares an input fingerprint to the enrolled fingerprint of a specific user to determine if they are from the same finger (1:1 match). In identification, the system compares an input fingerprint with the prints of all enrolled users in the database to determine if the person is already known under a duplicate or false identity (1:N match). Detecting multiple enrollments, in which the same person obtains multiple credentials such as a passport under different names, requires the negative identification functionality of fingerprints. When it came to designing the lock, we wanted to achieve simplicity in terms of the entire lock itself as well as in the internal components. The lock will be hanging on the wall beside the doorway that will include a fingerprint sensor.

We have added a keypad that can be used to enter a password for alternative access in case of the fingerprint sensor does not present. We are using on optical fingerprint sensor. Optical fingerprint sensors use reflective light to scan the surface of the finger with almost 100% accuracy. The sensor we are using is called R305 Fingerprint Sensor.

For this project the main components are:

- Arduino NANO
- Fingerprint sensor
- Servo motor
- 4X4 Matrix keypad

IV. BLOCK DIAGRAM



V. COMPONENTS REQUIRED

A) HARDWARE REQUIREMENT

- Power supply
- Microcontroller
- Fingerprint sensor
- Keypad
- Servo Motor

B) SOFTWARE REQUIREMENT

- Arduino IDE
- Proteus 8 Professional

<u>LANGUAGE:</u>

- Embedded C

1) ARDUINO NANO CONTROLLER

Arduino is an open source microcontroller which can be easily programmed, erased and reprogrammed at any instant of time. Introduced in 2005 the Arduino platform was designed to provide an inexpensive and easy way for hobbyists, students and professionals to create devices that interact with their environment using sensors and actuators. Based on simple microcontroller boards, it is an open source computing platform that is used for constructing and programming electronic devices. It is also capable of acting as a mini computer just like other microcontrollers by taking inputs and controlling the outputs for a variety of electronics devices. It is also capable of receiving and sending information over the internet with the help of various Arduino shields, which are discussed in this paper. Arduino uses a hardware known as the Arduino development board and software for developing the code known as the Arduino IDE (Integrated Development Environment). Built up with the 8-bit Atmel AVR microcontroller's that are manufactured by Atmel or a 32-bit Atmel ARM, these microcontrollers can be programmed easily using the C or C++ language in the Arduino IDE. Unlike the other microcontroller boards in India, the Arduino boards entered the electronic market only a couple of years ago, and were restricted to small scale projects only.

People associated with electronics are now gradually coming up and accepting the role of Arduino for their own projects. This development board can also be used to burn (upload) a new code to the board by simply using a USB cable to upload. The Arduino IDE provides a simplified integrated platform which can run on regular personal computers and allows users to write programs for Arduino using C or C++ so many Arduino boards available in the market, selecting a particular development board needs a variety of survey done with respect to their specifications and capabilities, which can be used for the project execution according to its specified applications.

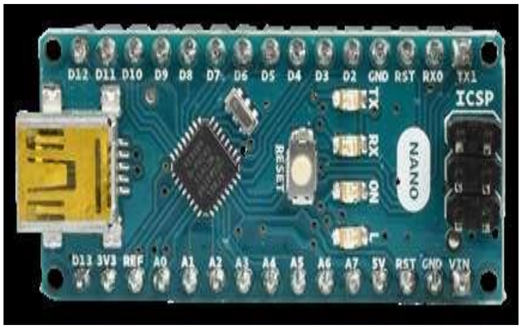
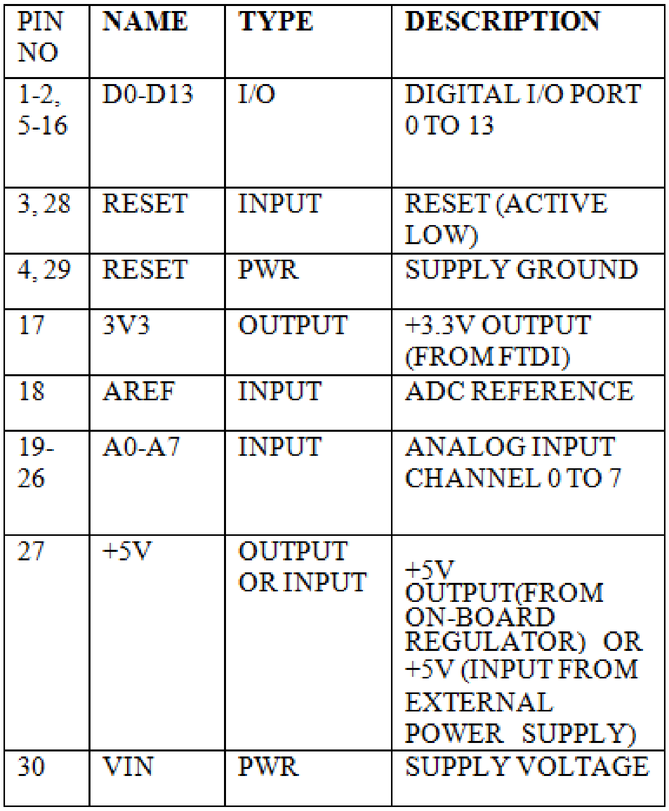

D12 D11 D10 D9 D8 D7 D6 D5 D4 D3 D2 GND RST RX0 TX1
ICSP
TX
RX
ON
L
RESET
NANO
D13 3V3 REF A0 A1 A2 A3 A4 A5 A6 A7 5V RST GND VIN

Fig 1. Arduino board

i) PIN DESCRIPTION

Table 1. Nano pin description



PIN NO	NAME	TYPE	DESCRIPTION
1-2, 5-16	D0-D13	I/O	DIGITAL I/O PORT 0 TO 13
3, 28	RESET	INPUT	RESET (ACTIVE LOW)
4, 29	RESET	PWR	SUPPLY GROUND
17	3V3	OUTPUT	+3.3V OUTPUT (FROM FTDI)
18	AREF	INPUT	ADC REFERENCE
19-26	A0-A7	INPUT	ANALOG INPUT CHANNEL 0 TO 7
27	+5V	OUTPUT OR INPUT	+5V OUTPUT(FROM ON-BOARD REGULATOR) OR +5V (INPUT FROM EXTERNAL POWER SUPPLY)
30	VIN	PWR	SUPPLY VOLTAGE

2) R305 FINGERPRINT SENSOR MODULE

There are different types of fingerprint modules available in the market like R305, R307. For a better understanding of this sensor, here we are going to discuss an overview of R305 fingerprint sensor module.

Fig 1. R305 Fingerprint sensor module

The R305 is one kind of fingerprint sensor module used in biometrics for security in fingerprint detection as well as verification. These devices are mainly used in safes where there is a high-powered DSP chip used in the rendering of image, feature-finding, searching and calculation by connecting it to any microcontroller with the help of TTL serial, & send data packets to get photos, notice prints, search and hash. The enrolment of new fingers can be stored directly within the flash memory of on board.

The working principle of the fingerprint sensor mainly depends on the processing. The fingerprint processing mainly includes two elements namely enrolment and matching. In fingerprint enrolling, every user requires to place the finger twice. So that the system will check the finger images to process as well as to generate a pattern of the finger and it will be stored. When matching, a user places the finger using an optical sensor then the system will produce a pattern of the finger & compares it with the finger library templates. For 1:1 fingerprint matching, the system will evaluate the exits finger with a precise pattern which is selected within the module. Similarly, for 1: N matching, the scanning system will look for the complete finger records for the finger matching. In both situations, the scanning system will go back to the corresponding result, success otherwise crash.

3) 4X4 KEYPAD MODULE

- When we want to interface one key to the microcontroller then it needs one GPIO pin. But when we want to interface many keys like 9, 12 or 16 etc., then it may acquire all GPIO pins of microcontroller.
- To save some GPIO pins of microcontroller, we can use matrix keypad. Matrix keypad is nothing but keys arrange in row and column.
- E.g. if we want to interface 16 keys to the microcontroller then we require 16 GPIO pins but if we use matrix 4x4 keypad then we require only 8 GPIO pins of microcontroller.

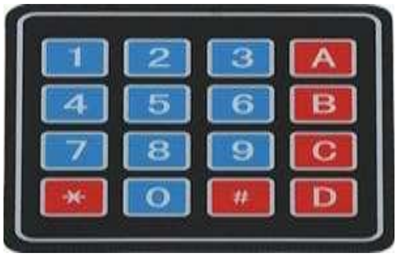


Fig 1. 4x4 Keypad

i) 4X4 KEYPAD MATRIX STRUCTURE

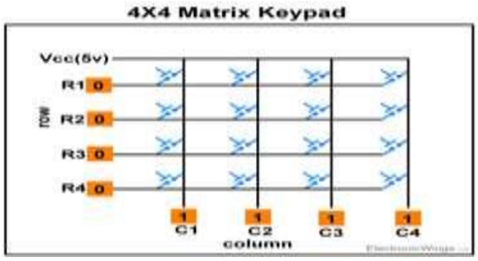


Fig 2. 4X4 Kepad matrixstructure

Keyboards are organized in a matrix of rows and columns. When a key is pressed, a row and a column make a contact Otherwise; there is no connection between rows and columns.

ii) KEYPAD MATRIX WORKING

To detect a pressed key, the microcontroller grounds all rows by providing 0 to the output latch, and then it reads the columns shown in above fig.

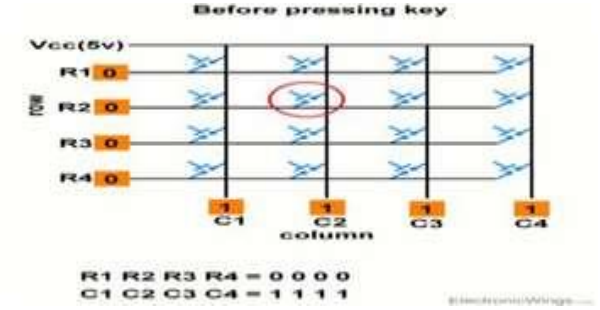


Fig 3. Before pressing key

- If the data read from columns is = 1111, no key has been pressed shown in above fig. and the process continues till key press is detected.
- Now, consider highlighted key in above fig. is pressed. After pressing key, it makes contact of row with column shown below.

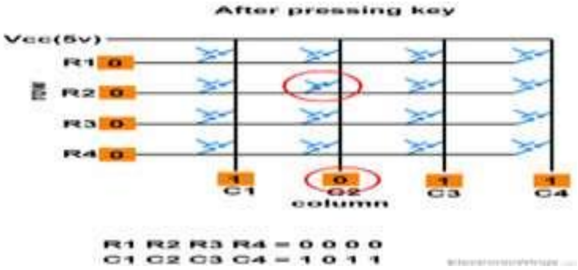


Fig 4. After pressing key

- If one of the column bits has a zero, this means that a key press has occurred.
- For example, if C1:C4 = 1011, this means that a key in the C2 column has been pressed.
- After detecting a key press, microcontroller will go through the process of identifying the key.

4) SERVO MOTOR

A servo motor is an electrical device which can push or rotate an object with great precision. If you want to rotate and object at some specific angles or distance, then you use servo motor. It is just made up of simple motor which run through servo mechanism. If motor is used is DC powered then it is called DC servo motor, and if it is AC powered motor then it is called AC servo motor. We can get a very high torque servo motor in a small and light weight packages. Doe to these features they are being used in many applications like toy car, RC helicopters and planes, Robotics, Machine etc.

Servo motors are rated in kg/cm (kilogram per centimeter) most hobby servo motors are rated at 3kg/cm or 6kg/cm or 12kg/cm. This kg/cm tells you how much weight your servo motor can lift at a particular distance. For example: A 6kg/cm Servo motor should be able to lift 6kg if the load is suspended 1cm away from the motors shaft, the greater the distance the lesser the weight carrying capacity.

Fig 1. Servo motor

The position of a servo motor is decided by electrical pulse and its circuitry is placed beside the motor.

A servo consists of a Motor (DC or AC), a potentiometer, gear assembly and a controlling circuit. First of all we use gear assembly to reduce RPM and to increase torque of motor. Say at initial position of servo motor shaft, the position of the potentiometer knob is such that there is no electrical signal generated at the output port of the potentiometer. Now an electrical signal is given to another input terminal of the error detector amplifier. Now difference between these two signals, one comes from potentiometer and another comes from other source, will be processed in feedback mechanism and output will be provided in term of error signal. This error signal acts as the input for motor and motor starts rotating. Now motor shaft is connected with potentiometer and as motor rotates so the potentiometer and it will generate a signal. So as the potentiometer's angular position changes, its output feedback signal changes. After sometime the position of potentiometer reaches at a position that the output of potentiometer is same as external signal provided. At this condition, there will be no output signal from the amplifier to the motor input as there is no difference between external applied signal and the signal generated at potentiometer, and in this situation motor stops rotating.

5) ARDUINO IDE

Here, we will learn about the different components on the Arduino board. We will study the Arduino NANO board because it is the most popular board in the Arduino board family. In addition, it is the best board to get started with electronics and coding. Some boards look a bit different from the one given below, but most Arduinos have majority of these components in common.

Various kinds of Arduino boards are available depending on different microcontrollers used. However, all Arduino boards have one thing in common: they are programed through the Arduino IDE. The differences are based on the number of inputs and outputs (the number of sensors, LEDs, and buttons you can use on a single board), speed, operating voltage, form factor etc. Some boards are designed to be embedded and have no programming interface (hardware), which you would need to buy separately. Some can run directly from a 3.7V battery, others need at least 5V.

Arduino is a prototype platform (open-source) based on an easy-to-use hardware and software. It consists of a circuit board, which can be programmed (referred to as a microcontroller) and a ready-made software called Arduino IDE (Integrated Development Environment), which is used to write and upload the computer code to the physical board.

The key features are –

- Arduino boards are able to read analog or digital input signals from different sensors and turn it into an output such as activating a motor, turning LED on/off, connect to the cloud and many other actions.
- You can control your board functions by sending a set of instructions to the microcontroller on the board via Arduino IDE (referred to as uploading software).
- Unlike most previous programmable circuit boards, Arduino does not need an extra piece of hardware (called a programmer) in order to load a new code onto the board. You can simply use a USB cable.
- Additionally, the Arduino IDE uses a simplified version of C++, making it easier to learn to program.

Finally, Arduino provides a standard form factor that breaks the functions of the micro-controller into a more accessible package.

Sketch − The first new terminology is the Arduino program called "**sketch**".Structure

Arduino programs can be divided in three main parts: **Structure, Values** (variables and constants), and **Functions**. In this tutorial, we will learn about the Arduino software program, step by step, and how we can write the program without any syntax or compilation error.

6) PROTEUS 8

It is a software suite containing schematic, simulation as well as PCB designing.

- **ISIS** is the software used to draw schematics and simulate the circuits in real time. The simulation allows human access during run time, thus providing real time simulation.
- **ARES** is used for PCB designing. It has the feature of viewing output in 3D view of the designed PCB along with components.

The designer can also develop 2D drawings for the product. ISIS has wide range of components in its library. It has sources, signal generators, measurement and analysis tools like oscilloscope, voltmeter, ammeter etc., probes for real time monitoring of the parameters of the circuit, switches, displays, loads like motors and lamps, discrete components like resistors, capacitors, inductors, transformers, digital and analog Integrated circuits, semi-conductor switches, relays, microcontrollers, processors, sensors etc.

ARES offers PCB designing up to 14 inner layers, with surface mount and through hole packages. It is embedded with the foot prints of different category of components like

ICs, transistors, headers, connectors and other discrete components. It offers Auto routing and manual routing options to the PCB Designer. The schematic drawn in the ISIS can be directly transferred ARES.

VI. PROCEDURE FOR CONFIGURING ARDUINO FINGERPRINT SENSOR LOCK

1. Assemble the enrollment new user circuit shown below.

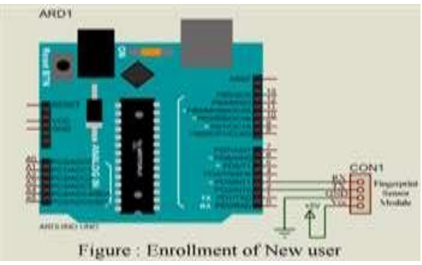


Fig1. Enrollment of new user

2. Upload the enroll.ino code to your arduino board.

Fig 2. Uploading code

3. Open the serial monitor either from menu or by pressing Ctrl+Shift+m key at once.

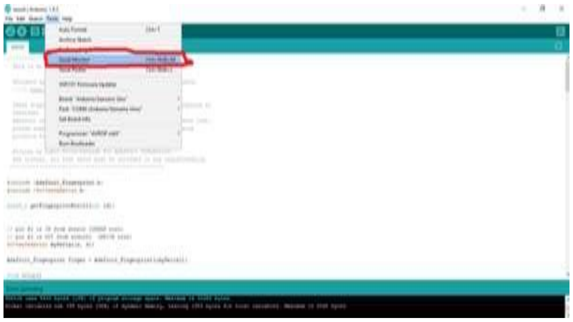


Fig 3. Serial monitor

4. Adjust the Baud rate to 38400 as shown in figure below.

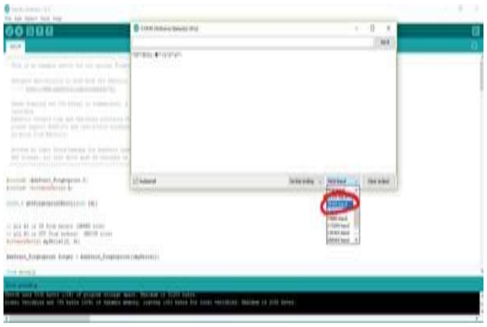
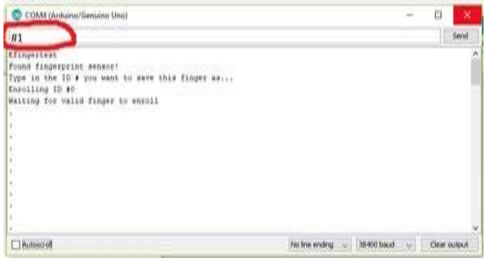


Fig 4. Adjustment of baud rate

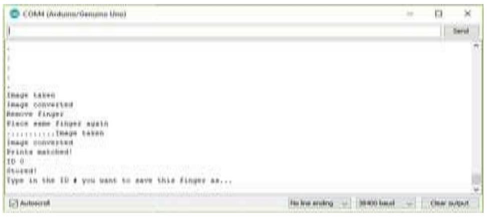
5. Enter the enroll ID followed by # (eg. #1), Put the finger on finger print sensor module and follow the instruction shown in serial monitor.



```
#1
```

```
Efingertest
Found fingerprint sensor!
Type in the ID # you want to save this finger as...
Enrolling ID #0
Waiting for valid finger to enroll
```

Fig 5. Entering enroll id



```
Image taken
Image converted
Remove finger
Place same finger again
:::::::::::Image taken
Image converted
Prints matched!
ID 0
Stored!
Type in the ID # you want to save this finger as...
```

Fig 6. Instructions in serial monitor

Open fingerprint.ino from the software folder and assign the user to their corresponding ID in your source code (door open function) and upload it to your arduino board.

VII. SIMULATION

The whole electrical part of the project was simulated on PROTEUS simulation platform before the soldering work commenced to observe the operation of the whole project. Figures 1-5 shows the simulation screen shots

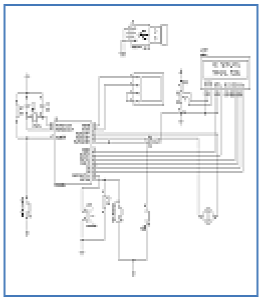


Fig 1. Shows the simulation screen shot before any finger print was stored

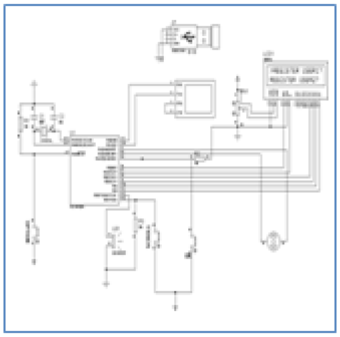


Fig 2. Shows the simulation screen shot at registering finger print

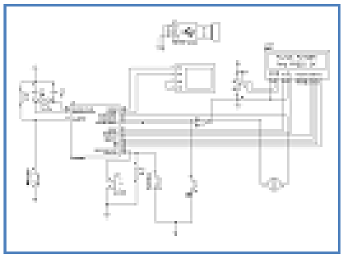


Fig 3. Shows the simulation screen shot after registering finger print (default)

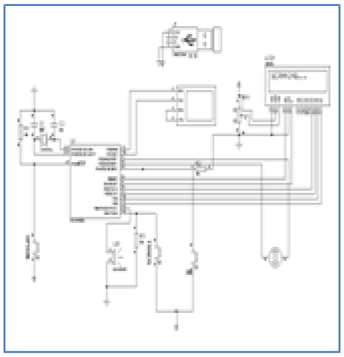


Fig 4. Shows the simulation screen shot while scanning finger print

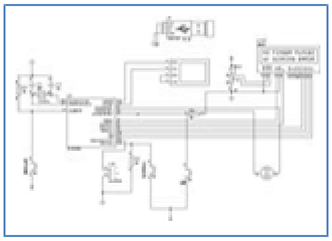


Fig 5. Shows the simulation screen shot while error occurs at scanning finger print

VIII. RESULTS AND DISCUSSION

In this section, we discuss how the system behaved upon completion. We devised various tests to see if the individual functions are performing accordingly. After implementation of the tests, we have collected the results to verify the functionalities of the individual components. Then the system was tested as a whole for any error. After carrying out the tests, the system was given to engineers so that they can try to break the system and use their own fingerprints in the system.

1) FINGERPRINT TESTING

After saving a fingerprint, we wanted to test the accuracy of it. We tried placing the finger partially, inverted, in wet conditions etc. and the sensor was able to match the prints. It failed when the finger was muddy or very oily. But in normal cases, the sensor is able to detect saved prints almost all the times. In our rigorous testing, the success ratio is more than 95%. When the finger is extremely dirty or oily, it did fail for which alternative password system is introduced. But the sensor seems to get the reading right when the finger is less dirty or oily. However, it did not fail when the finger was wet. Marks were present on the sensor lens but that was easily wiped away. Those marks were water particles left after the finger was replaced. The sensor claims to have 99% accuracy rate and it seems to be living up to its promise.

2) KEYPAD TESTING

We have entered the password once. Entered wrong code three times in a row. Expected results achieved. But in practice, the fingerprint is much more secure; this feature is kept for an extreme case of emergencies.

After successfully completing the goal and experimenting with the system, we can conclude that we have created a very reliable and secure lock. To test the accuracy and the functionality of the system we have devised various finger conditions to test the scanner, tested the keypad with test codes and test runs for the switch. The scanner was able to detect over 90% of the fingerprint scans after we have deliberately tested it with extreme finger conditions (dirty, oily, wet, etc.) The keypad have performed accordingly with 100% accuracy. They wanted more functions to be added which is possible with this system, for that we will require the requirement specific hardware and a few modification of code.

IX. FUTURE WORK

The developed system is very much flexible. The system we have created operates on only one lock, but in our current state, we can add more electronic locks, where each lock can be unlocked with specified print IDs. All it will need is more electronic locks and code modifications. There can be some other implementations to this system as well, some of them are given below.

1) MULTI-LOCK/DECODER NETWORK SYSTEM

As mentioned earlier, this system currently has one lock connected to, and we can add up to 5 more. In fact, by using a network of decoders, we can connect as many locks as we want and provide access to up to 126 different individuals. Addionally, 6 different locks can be added. Instead of using those output pins from the no for locks, we can create a system using 7: 128 decoders. In that way, all the memory space of the fingerprint sensor (126 capacity), connect them to individual doorway or doorways with just one system.

2) COMPUTERIZED FINGERPRINT LOCK SYSTEM

This system can be installed on a PC, which will act as the brain behind the system. It can add new IDs and delete old ones and can even unlock doors through the computer. This will require the computer to be in the security control room or somewhere secure. In particular a log system can be easily implemented with the use of a computer with this system.

3) SMARTPHONE BASED FINGERPRINT SECURITY SYSTEM

Smartphones with latest features use fingerprint ID system to allow access to the phone. This 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 WiFi, and an application can be made for the phone allowing them to interact. 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.

4) IMPROVEMENTS

More locks can be added to the system, i.e., we do not need to spend so much for just one lock. 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.

X. CONCLUSION

The design and implementation of fingerprint based lock system is customizable and flexible. This door locking mechanism is comparatively cost-effective than the available lock systems in the traditional market. Our 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. In order to maintain security properly, the keypad should be placed inside the security room. 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 most of the prints during testing. It provides greater control for access to restricted places.

REFERENCES

[1] 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.

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

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

[4] Mary Lourde R and Dushyant Khosla. Fingerprint Identification in Biometric Security Systems.

International Journal of Computer and Electrical Engineering, 2(5), October, 2010.

[5] Zevdin Pala and Nihat Inanc. Smart Parking Applications Using RFID Technology. 1st Annual RFID Eurasia, Istanbul, 2007, pp. 1-3.

[6] D. Vinod kumar and M R K Murthy. Fingerprint Based ATM Security by using ARM7. IOSR Journal of Electronics and Communication Engineering (IOSRJECE), Volume 2(5), October 2012, PP 26-28.

[7] Raffaele Cappelli, Alessandra Lumini, Dario Maio and Davide Maltoni.Fingerprint Image Reconstruction from Standard Templates. IEEE Trans.
Pattern Analysis and Machine Intelligence, 29(9), pp. 1489-1503. September 2007.

[8] Ross J. Anderson. Security Engineering: A Guide to Building Dependable
Distributed Systems, 2nd edition, 2008. John Wiley & Sons, Inc., New
York, NY, USA.

[9] 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.

[10] Yu-Chih Huang. Secure Access Control Scheme of RFID System Application. Fifth International Conference on Information Assurance and
Security, China, 2009.

[11] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain.FVC2002: Fingerprint Verification Competition. Proceedings of International Conference on Pattern Recognition (ICPR), pp.744-747, Quebec City, Canada, August 2002.