BIOMETRIC FINGERPRINT IDENTIFICATION FOR BANK LOCKER SECURITY SYSTEM

A project Report Phase-2

Submitted in partial fulfillment of the

requirements for the award of

Bachelor of Engineering Degree in Electronics and Communication Engineering

by

PADMINI.A (39130332)

THARANI.T (39130471)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SCHOOL OF ELECTRICAL AND ELECTRONICS

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited with Grade "A" by NAAC I 12B Status by UGC I
Approved by AICTE JEPPIAAR NAGAR, RAJIV GANDHI SALAI,CHENNAI – 600 119.

APRIL- 2023

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with "A" grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report submitted for final year project is the bonafide work of **PADMINI.A (39130332), THARANI.T (39130471)** who carried out the project entitled "**BIOMETRIC FINGERPRINT IDENTIFICATION FOR BANK LOCKER SECURITY SYSTEM"** under our supervision from NOVEMBER 2022 to APRIL 2023.

INTERNAL GUIDE

Dr.P.KAVIPRIYA M.E,Ph.D

Head of the Department

Dr.T.RAVI, M.E,Ph.D

Submitted for Viva voce Examination held on 19.04.2023

INTERNAL EXAMINER **EXTERNAL EXAMINER**

DECLARATION

We **PADMINI.A, THARANI.T** hereby declare that the Project Report entitled **"BIOMETRIC FINGERPRINT IDENTIFICATION FOR BANK LOCKER SECURITY SYSTEM"** done by us under the guidance of **Dr.P. Kavipriya** at **Sathyabama Institute of Science and Technology** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electronics and Communication Engineering.

DATE: 19.04.2023

PLACE: Chennai

SIGNATURE OF THE CANDIDATE

1. Padmini

2. Tharani

ACKNOWLEDGEMENT

We are pleased to acknowledge our sincere thanks to **Board of Managementof Sathyabama Institute of Science and Technology** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

We convey our thanks to **Dr. N.M. NANDHITHA, M.E., Ph.D., Professor & Dean, School of Electrical and Electronics Engineering** and **Dr.T. RAVI, Ph.D., Professor & Head** of the Department, Dept. of Electronics and Communication Engineering for providing us necessary support and details at the right time during the progressive reviews.

We would like to express my sincere and deep sense of gratitude to our Project Guide **Dr.P.KAVIPRIYA, M.E,Ph.D** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of our to project work.

ABSTRACT

The main purpose of this project is to design and implement high security system of Locker. Security is a prime concern in our day-to-day life. it has been playing a key role in our places like offices, institutions, libraries, laboratories, Locker… etc. Perhaps the most important application of accurate personal identification is securing limited access systems from malicious attacks in order to keep our data confidentially so that no other unauthorized person could have an access on them. Nowadays, at every point of time, we need security systems for protection of valuable data, Locker and even money. The fingerprint and IRIS based security system presented here is an access control system that allows only authorized persons to access a Locker. The implemented of security system based on fingerprint, IRIS and LCD technology which can activate, authenticate, and validate the user and unlock the Locker in real time for locker secure access. Fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity. Fingerprint is sensedby sensor and is validated for authentication. If the fingerprint matches, the door will be opened automatically and LCD will send SERVO contain the IRIS to turn the Locker's engine which will change randomly. This high security system based on fingerprint, IRIS and LCD technology can be organized in the money transfer Lockers or any transfer which needs high security information.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Description
AC	Alternating Current
ADC	Analogy to digital converter
AREF	Analog Reference (voltage)
ATD	Address Transition Detection
ATM	Automated Teller Machine
CCD	charge coupled device
DC	Direct Current
EEPROM	Electrically Erasable Programmable Read only Memory
GND	Ground
GPS	Global Positioning System
LCD	Global System for Mobile Communications
ID	Identification
IDE	Integrated Development Environment
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MIC	Microphone
PIN	Personal Identification
PWM	Pulse width Modulation
RFID	Radio Frequency Identification
RTOS	Real time operating system
RXD	Receive Data
SERVO	Short Message Service
SIM	Subscriber Identity Module
SRAM	Static Random Access Memory
TXD	Transmit Data
USART	Universal Synchronous Asynchronous Receiver and Transmitter
USB	Universal Serial Bus

CHAPTER 1

INTRODUCTION

1.1INTRODUCTION ABOUT BIOMETRIC

This chapter will focus on the brief introduction of the project to be Lockerbie out. The important overview or description including the problem statement, project objectives, and expected result are well emphasized in this part.

The technological advancement in the field of electronics and telecommunication has brought more and more arrangements in the domestic and industrial environment. Security systems can avoid the unauthorized entry of peoples into the protected area and it stores the detailsabout the authorized peopled entered in the area on the computer through a wireless transmitter. Up gradations in this system can be done easily to improve the efficiency of the system. Security systems are the demands of the day, which helps to avoid theft and avoids unauthorized entry of peoplesinto the restricted area. Conventional security systems used either knowledge-based methods (passwords or PIN), and token-based methods (passport, driver license, ID Locked) and were prone to fraud because PIN numbers could be forgotten or hacked and the tokens could be lost, duplicated, or stolen. To address the need for robust, reliable, and foolproof personal identification, authentication systems will necessarily require a biometric component. Personal Safes are revolutionary locking storage cases that open with just the touch of your finger. These products are designed as secure storage for medications, jewelry, weapons, documents, and other valuable or potentially harmful items. These utilize fingerprint recognition technology to allow access to only those whose fingerprints youchoose. It contains all the necessary electronics to allow you to store, delete,and verify fingerprints with just the touch of a button. Stored fingerprints are retained even in the event of complete power failure or battery drain. These eliminates the need for keeping track of keys or remembering a combination password, or PIN. It can only be opened when an authorized user is present, since

there are no keys or combinations to be copied or stolen, or locks that can be picked defined a set of features for fingerprint identification, which since then, has been refined to include additional typesof fingerprint features. This powerful device uses the latest in fingerprint IDscan technology to make sure only authorized drivers with enrolled fingerprints can enter.

1.2 PROBLEM STATEMENT

The existing security system either based on fingerprint or PIN number. Fingerprint alone has some failure for security system because it can be fake. In case of PIN number-based security system, same PIN number is used again and again. Anybody can hack the PIN number or guess.

1.3 PROPOSED SOLUTION

The purpose of this research is to provide a high-level security system using both of two methods the finger print sensor and LCD module in the Locker which need high security using in money transform or high security information to fulfill the security gabs resulted from using just individual security system considering that system will designto be efficient, more secure, and with less cost.

OBJECTIVE

The main objective of this project is to increase the security feature of the Locker by integrating fingerprint and LCD module with the Arduino microcontroller.
To achieve this objective:

1/ Control system using Arduino LCD module is proposed.

2/ Simulation of the proposed system is run.

1.5 METHODOLOGY

The design involves incorporation of a fingerprint identification module which provides high security and authentication features. Inclusion of thismodule along with LCD and GPS module helps to detect and correct the various faults in the device at a faster rate.

The fingerprints are taken and stored in the database using Arduino software. The Arduino Software allows user to enter all as many fingerprints as possible. The user has the permission to add or delete any fingerprint in the database. Then connecting the finger prints sensor and LCD with Arduino.

If the fingerprint is verified, then the user will get IRIS immediately for the further process through LCD Modem. The user will process with the help of that Password. For every time we will receive different random number as a IRIS to our mobile then when the person enters the PIN the Locker will move.

1.6 THESIS LAY OUT

Thesis is summarized in five chapters. The contents of each chapter are explained as follows:

Chapter 1: Introduction explains problem and proposed solution.

Chapter 2: Literature review and cover different system component.

Chapter 3: System design and explain how it work.

Chapter 4: Result and discussion.

Chapter 5: Conclusion recommendation for fit

CHAPTER 2

LITERATURE REVIEW

J. Tapia, C. Perez - Gender Classification from the same iris code used for recognition. In this study, the binary iris code that could be used for identification was first applied to accurately determine gender. The information for gender prediction, according to the author, is dispersed throughout the iris as opposed to being localized in distinct concentric rings. They found that, in comparison to using features that represent the complete iris region, using features that only represent a portion of the iris region increases accuracy. By using measurements of mutual information as a guidance prediction, the author 3 selected iris code bits to use as gender characteristics. This technique, along with person-disjoint training and testing evaluation, can accurately predict gender by combining the best elements of the iris codes from the left and right eyes.

A. Verma- A Multi-Layer Bank Security System, A multi-layer bank security system is a method for validating, supervising, and managing the security at bank storage rooms. To stop unauthorized access to the changing area, many banks today use the authorized access control approach. This work has developed the most effective, multi-level, and extremely reliable protection system for locker rooms. The system has a biometric component that uses gadgets like a fingerprint reader and an iris scanner to manage the security of the locker room's front entrance. Additionally, it has an RFID system that only permits authorized people to enter the dressing room area. Using a stationary passive infrared monitor in the locker room area, unauthorized visitors are kept an eye on. In the event of any unauthorized motion, the camera's picture will be mailed to security authorities, and the alarms will sound to notify local security.

R. Gusain, H. Jain and S. Pratap -"Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology. The purpose of this article is to design a bank locker security system that uses palm vein technology (PVR), iris scanning, and facial recognition to safeguard valuable items. MATLAB software is used by facial recognition systems to identify and validate the authorized user's picture. When someone enters an area that isn't restricted, the camera takes pictures of them, and a computer program matches those photos to a database of authorized people. The iris detection technology makes use of the kind human physical traits. Several places, including ATMs, immigration and border control, public safety, hospitality, and tourism, use this technology for biometric authentication. This research provides recommendations on how to modify the vascular pattern thinning algorithm to enhance the capability of palm vein recognition systems. A method known as palm vein recognition (PVR) analyses a user's palm vein pattern and compares it to information kept in a database in order to confirm their identity.

D. Akila, S. Jayalakshmi, R. Jaya Karthik, S. Mathivilasini and G. Suseendran - Biometric Authentication with Finger Vein Images Based on Quadrature Discriminant Analysis. For a very long time, high-security apps like bank lockers and private locations have used biometric authentication. Here, examination of a person's finger print, iris, etc. can reveal study on their physiological characteristics. Finger vein identification is part of the novel approach to 4 biometric recognitions. Here, a person's finger vein patterns can be used to authenticate them for entry to high-security apps. This research aims to identify finger veins using a quadrature discriminant analysis approach. Finger vein images are pretreated using methods to increase the image's stability for processing later. The QDA process was followed before using the Minimal Distance Classifier.

A.Natarajan and N. Shanthi - A Survey on Multimodal Biometrics Authentication and Template Protection. Biometric systems occupy a large portion of the security system market. Most applications use biometric technology, including locker and attendance controls at institutions like banks and hospitals. The

templates that are stored there must be protected in addition to the authentication that these biometric systems provide. An overview of numerous biometrics, such as authentication, fusion, and template protection methods, as well as biometrics including fingerprints, faces, hand veins, iris, signatures, etc., is provided in this paper. In order to identify the most distinctive and practical methods for biometric identification and template protection, several traits and practices are investigated. A comparison of the unimodal and multimodal biometric systems is also included in this study. The various unimodal and multimodal biometric systems are assessed using metrics like the Genuine Acceptance Rate, Equal Error Rate, False Acceptance Rate, and False Reject Rate.

S. Sridharan-Authenticated secure biometric based access to the bank safety lockers. This paper focuses on providing a secure, authentic, and user-friendly mechanism for both the customers of the bank holding a locker and the branch head's involvement in all the operations pertaining to the safety lockers. The primary aim of this paper is to provide a solution towards a complete biometric based authentication mechanism for operating the safety lockers. This system rests on improving the current fact that all the lockers that operates currently operates only with the help of two different keys - one the branch head's key and other the user key. Improvement towards the current model that relies heavily on the key of the user is proposed which helps in the functioning of the locker with bio-metric and secret code (password). The main features that are proposed in the new mechanism is the two-level authentication - one by the branch head and one by the user for their identities, secure individual authentication with their bio-metrics and the access only to the concerned individuals for their safety lockers. The branch head responsible for the operation of the safety deposits is assigned in a daily basis by the central regional office of that bank.

A.Chikara, P. Choudekar, Ruchira and D. Asija-Smart Bank Locker Using Fingerprint Scanning and Image Processing. In the present work, a smart locker has been designed for banking sector. The main feature of this work is it keeps track of time, date, and number of accesses of locker by a user in the bank. The smart

lock program will compare your image and fingerprint with the data already stored in the database. After checking the authenticity of the user, the microcontroller (Arduino) will give signal to the lock and it will open. It also gives a message when the number of permissible access turns increases in each duration.

S. Venkatraman, R.R. Varsha and P. Vignesh wary-IOT based Door open or close monitoring for home security with emergency notification system using LoRa Technology. This paper examines and analyzes the security measures that address the difficulties that are faced by the house owners and the bank locker holders. Current door monitoring system methods involves the use of digital locks, Wi-Fi technology to check the status of the door periodically leading to a reduction in theft and robbery or burglary that happens per every 3 minutes in India as per reports. According to the report, Indians continue to place greater emphasis on keeping their online safety systems up-to-date in order to ensure safety of their homes. Using LoRa technology, we can endlessly monitor the status of the door i.e., whether it is open or closed and based on the status further actions like alarming, sending an emergency notification are done to notify and alert the owner and to improve security. Lora Technology reconfigured the IoT by enabling long distance data connections while using very little power. Lora WAN fills a technical gap for mobile-based and a WIFI networks which needs higher power or high bandwidth or even the inability to penetrate deep indoor areas.

CHAPTER 3

AIM AND SCOPE

3.1 INTRODUCTION

This chapter is about fingerprint, Arduino LCD module controller and previous case studies, these studies which have been done previously by other researchers. It is very essential to refer to the variety of sources in order to gain more knowledge and skills to complete this project. These sources include reference books, thesis, and papers.

3.2 PREVIOUS WORKS

Home security system is needed for convenience and safety. This system invented to keep home safe from intruder. In this work, we present the design and implementation of a LCD based wireless home security system, which take a very less power. The system is a wireless home network which contains an LCD modem and magnet with relay which are door security nodes. The system can response rapidly as intruder detect and LCD module will do alert home owner. This security system for alerting a house owner wherever he will. In this system a relay and magnet installed at entry point to precedence produce a signal through a public telecom network and sends a message or redirect a call that that talks about your home update or predefined message which is embedded in microcontroller. Suspected activities are conveyed to remote user through SERVO or Call using LCD technology. focused on the four-step verification project. In this proposed work, RFIDreader reads the ID number from passive tag and sends to the microcontroller, if the id number is valid then only it gives the access to the fingerprint scanner otherwise it stops the process, if the fingerprint is matched then microcontroller sends the IRIS.

person mobile number then the authenticated person enters the both passwords in the keyboard which was already given by the user and received from the microcontroller. if these two passwords are matched then the locker will be opened otherwise the microcontroller sends the warning message to the authenticated person mobile number and it willbe remained in locked position.

Security has been playing a key role in many of our places like offices, institutions, libraries, laboratories etc. in order to keep our data confidentially so that no other unauthorized person could have an access on them. Nowadays, at every point of time, we need security systems for protection of valuable data and even money. This paper presents a fingerprint-based door opening system which provides security which canbe used for many banks, institutes, and various organizations etc..,. There are other methods of verifying authentication through password, RFID but this method is most efficient and reliable. To provide perfect security to the bank lockers and to make the work easier, this project is taking help of two different technologies viz. EMBEDDED SYSTEMS AND BIOMETRICS. Unauthorized access is prohibited by designing a lock that stores the fingerprints of one or more authorized users. Fingerprint is sensed by sensor and is validated for authentication. If the fingerprint matches, the door will be opened automatically otherwise the buzzer connected to an audio amplifier will be activated so that the people near the surroundings will get an alert.

Fingerprint matching has been successfully used by law enforcement for more than a century. The technology is now finding lot of other applications such as identity management and access control. In this context, an automated fingerprint recognition system and identification ofkey challenges are described along with the research opportunities. The description is like a product design in this report implementing RTOS (Real time operating system) under the domain of embedded system.

Fingerprint Recognition is a widely popular but a complex pattern recognition problem. It is very difficult to design accurate algorithms capable of extracting salient features and matching them in a robust way. In this paper, we have come with a novel approach to simplify theexisting problems with a proper Embedded System Design.

Security is the major issue faced by everyone when we are away from our households. In the present scenario satisfactory solution for the aboveproblem is not yet discovered. Presented here is an electronic locking system in which Arduino plays the role of the processing unit. Arduino which is a microcontroller board belongs to at mega family. It is an open-source simple tool. It could sense, monitor, store, and control applications. Access control for the door is achieved using Arduino Uno board. This project exhibits a keyless system for locking and unlocking purposes using a predefined password. The circuit consists of transistor PN2222A, BD139, 4×4 matrix keypad, solenoid lock, LED, SIM900D LCD module. Unauthorized access is ensured by setting an IRIS by the user. It is entered through the 4×4 matrix keypad. If the entered IRIS matches, door will be opened automatically otherwise a message showing incorrect IRIS will be displayed on LCD display and a SERVO will be sent to the owner that the security was tried to be breached. This hardware project achieves security with commonly available components and consumes less power.

With the advancement in wireless technology, many tools have been developed to control a device from a remote location. These tools eliminate the need of physical availability of a person for controlling the device manually. Generally, LCD and GPS technology is used in these tools to locate and control advice. But the tools which use only these technologies for their operation are highly insecure and inefficient.

This Project proposes an alternate approach for wireless control of a device by incorporating a fingerprint identification module along with GPS and LCD modules. The fingerprint module increases the authenticity of the device and enables multiple users to control the device. These modulesare integrated to a simple Arduino microcontroller to demonstrate variousfunctionalities. The proposed approach finds its application in various fields like automobiles, agriculture.

3.3 FINGERPRINT SENSOR

Fig: 3.1 Finger print sensor

The skin on our palms and fingers exhibits a flow like patterns of ridges and valleys. The papillary ridges on the finger, called friction ridges,which help the hand to grasp objects and increase friction and improvethe tactile sensing of the surface structure. These ridge patterns are now scientifically proved as unique for each person. The cuts and burns in a person's finger may alter these patterns temporarily but they reappear after the injury heals.

Fingerprints are now used widely for identification and verification purpose. They are used for attendance purpose inorganizations to avoid proxy for

criminal identification like terrorist, murderer, and violators and in passports (a matter of national high importance) of person.

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Many technologies have been used including optical, capacitive, RF, thermal, piezoresistive , ultrasonic, piezoelectric, MEMS. This is an overview of some of the more commonly used fingerprint sensor technologies.

3.3.1 OPTICAL FINGERPRINT SENSOR

The heart of an optical scanner is a charge coupled device (CCD), the same light sensor system used in digital cameras and camcorders. A CCDis simply an array of light-sensitive diodes called photo sites, which generate an electrical signal in response to light photons. Each photo site records a pixel, a tiny dot representing the light that hit that spot. Collectively, the light and dark pixels form an image of the scannedscene (a finger, for example). Typically, an analogy to digital converter in the scanner system processes the analogy electrical signal to generate a digital representation of this image.

The scanning process starts when you place your finger on a glass plate, and a CCD camera takes a picture. The scanner has its own light source, typically an array of emitting diodes, to illuminate the ridges of the finger. The CCD system generates an inverted image of the finger, with darker areas representing more reflected light (the ridges of the finger) and lighter areas representing less reflected light (the valleys between the ridges). Before comparing the print to stored data, the scanner processor makes sure the CCD has captured a clear image. It checks the average pixel darkness, or the overall values in a small sample, and rejects the scan if the overall image is too dark or too light. If the image is rejected, the scanner adjusts the exposure time to let in light, and then tries the scan again.

If the darkness level is adequate, the scanner system goes on to check the image definition (how sharp the fingerprint scan is). The processor looks at several straight lines moving horizontally and vertically across the image. If the fingerprint image has good definition, a line running perpendicular to the ridges will be made up of alternating sections ofvery dark pixels and very light pixels. If the processor finds that the image is crisp and properly exposed, it proceeds to comparing the captured fingerprint with fingerprints on file.

A disadvantage of this type of sensor is the fact that the imaging capabilities are affected by the quality of skin on the finger. For instance, a dirty or marked finger is difficult to image properly. Also, it is possible for an individual to erode the outer layer of skin on the fingertips to the point where the fingerprint is no longer visible. It can also be easily fooled by an image of a fingerprint if not coupled with a "live finger" detector. However, unlike capacitive sensors, this sensor technology is not susceptible to electrostatic discharge damage.

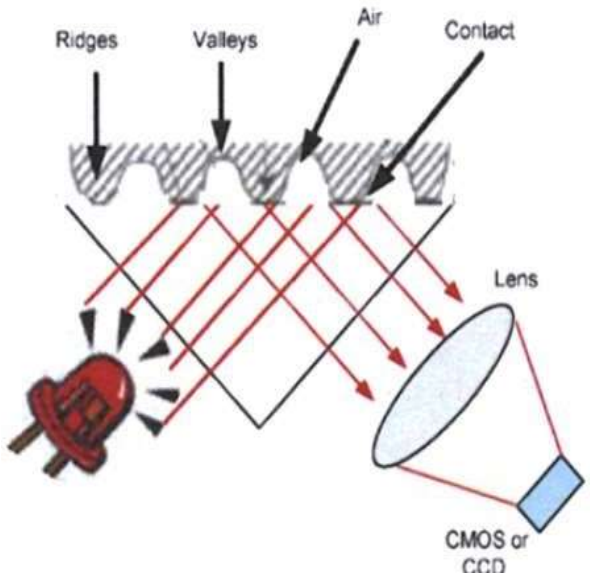

Fig: 3.2 optical fingerprint

3.3.2 ULTRASONIC FINGERPRINT SENSOR

Ultrasonic sensors make use of the principles of medical ultrasonography in order to create visual images of the fingerprint. Unlike optical imaging,ultrasonic sensors use very high frequency sound waves to penetrate the epidermal layer of skin. The sound waves are generated using piezoelectric transducers and reflected energy is also measured using piezoelectric materials. Since the dermal skin layer exhibits the same characteristic pattern of the fingerprint, the reflected wave measurements can be used to form an image of the fingerprint. This eliminates the need for clean, undamaged epidermal skin and a clean sensing surface. Eeco became the first company to introduce this in Smartphone.

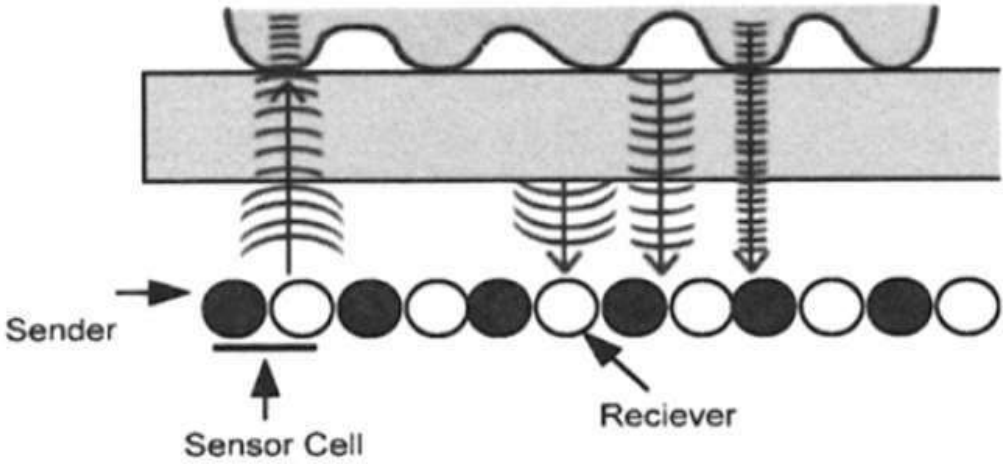

Fig: 3.3 Ultrasonic fingerprint sensor

3.3.3 CAPACITANCE FINGERPRINT SENSOR

Like optical scanners, capacitive fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead ofsensing thprint using light, the capacitors use electrical current. In this method of imaging, the sensor array pixels each act as one plate of a parallel-plate capacitor, the dermal layer (which is electrically conductive) acts as the other plate, and the non-conductive epidermal layer acts as a dielectric.

The sensor is connected to an integrator, an electrical circuit built around an inverting operational amplifier. The inverting amplifier is a complex semiconductor device, made up of several transistors, resistors, and capacitors Like any amplifier, an inverting amplifier alters one current based on fluctuations in another current. Specifically, the inverting amplifier altersa supply voltage. The alteration is based on the relative voltage of two inputs, called the inverting terminal and the non-inverting terminal. In this case, the non-inverting terminal is connected to ground, and the inverting terminal is connected to a reference voltage supply and a feedback loop. The feedback loop, which is also connected to the amplifier output, includes the two conductor plates.

As you may have recognized, the two conductor plates form a basic capacitor, an electrical component that can store up charge The surface ofthe finger acts as a third capacitor plate, separated by the insulating layersin the cell structure and, in the case of the fingerprint valleys, a pocket of air. Varying the distance between the capacitor plates (by moving the finger closer or farther away from the conducting plates) changes the totalcapacitance (ability to store charge) of the capacitor. Because of this quality, the capacitor in a cell under a ridge will have a greater capacitance than the capacitor in a cell under a valley.

To scan the finger, the processor first closes the reset switch for each cell,which shorts each amplifier's input and output to "balance" the integrator circuit. When the switch is opened again, and the processor applies a fixed charge to the integrator circuit, the capacitors charge up. The capacitance of the feedback loop's capacitor affects the voltage at the amplifier's input, which affects the amplifier's output. Since the distance to the finger alters capacitance, a finger ridge will result in a different voltage output than a finger valley.

The scanner processor reads this voltage output and determines whether itis characteristic of a ridge or a valley. By reading every cell in the sensor array. The processor can put together an overall picture of fingerprint, like image capture by an optical scanner.

The main advantage of a capacitive scanner is that it requires a real fingerprint-type shape, rather than the pattern of light and dark that makesup the visual impression of a fingerprint. This makes the system harder totrick. Additionally, since they use a semiconductor chip rather than aCCD unit, capacitive scanners tend to be more compact than optical device.

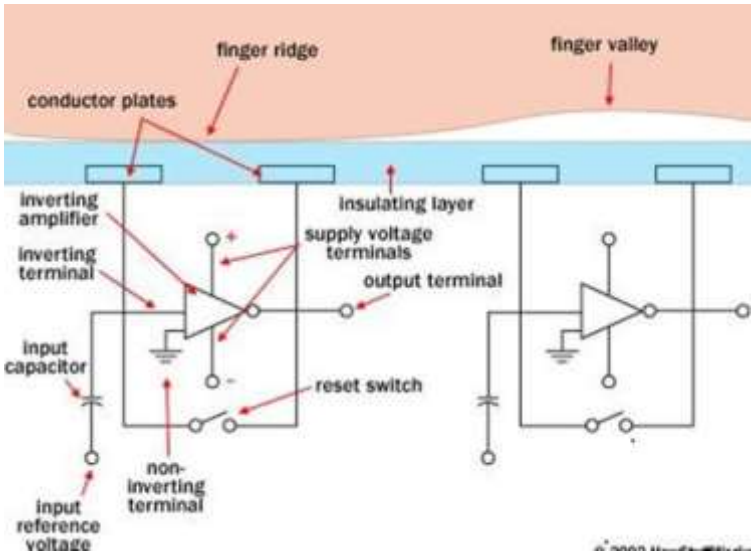

Fig: 3.4 Capacitance Fingerprint Sensor

3.3.4 IDENTIFICATION TECHNOLOGIES

A fingerprint-based personal authentication system operates in two distinct modes: enrollment and authentication (identification), as is shown in figure (3.5). During enrollment, a fingerprint image is acquired from a finger presented by an authorized user using a “fingerprint sensor,” and relevant features are extracted by the features extractor. The set of extracted features, also referred to as a “template” is stored in a database, along with the user’s information necessary for granting service, and some form of ID assigned for the user. When the user seeks for a service,

i.e., in authentication mode, the user inputs his assigned ID and presents his fingerprint to the sensor. The system captures the image, extracts (input) features from it, and attempts to match the input features to the template features corresponding to the subject’s ID in the system database. If the calculated similarity score between the input and the template is larger than the predetermined threshold, the system determines that the subject is who he claims to be and offer the service; otherwise, would reject the claim. In identification mode, on the other hand, the user who seeks for a service presents his fingerprint only without his ID, and the system may either be able to determine theidentity of the subject or decide the person is not enrolled in the database.

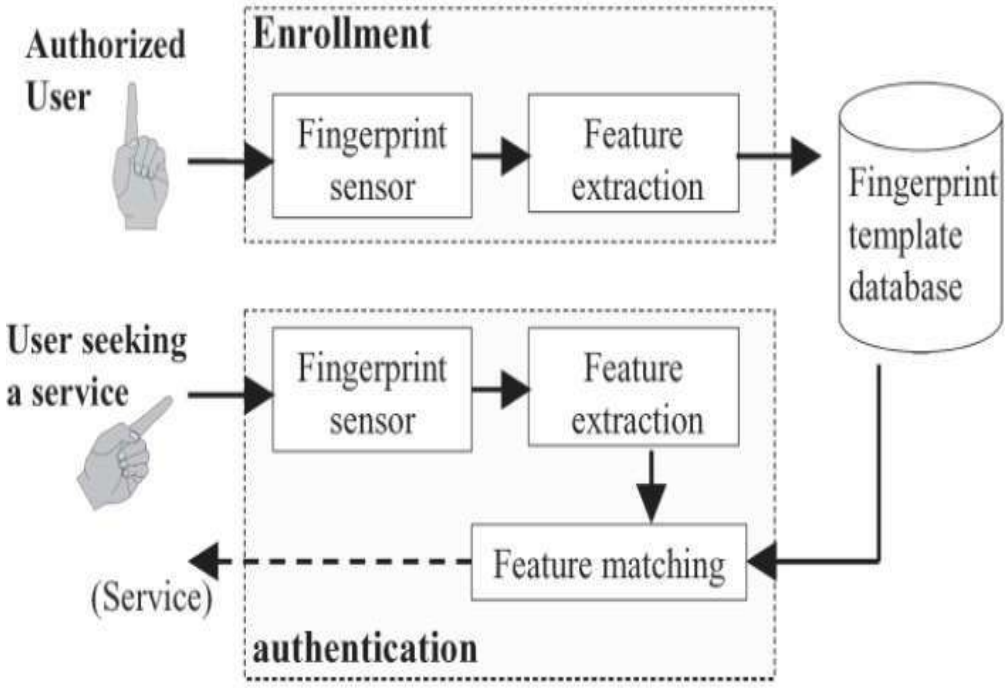

Fig: 3.5 Identification technologies

3.4 ARDUINO MICROCONTROLLER

Arduino is open-Source electronic prototyping platform based on flexible easy to use hardware and software. It is a single-board microcontroller to make using electronics in multidisciplinary projects more accessible. The hardware consists of a simple open-source hardwareboard designed around an 8-bit Atmel AVR microcontroller, or a 32-bit Atmel ARM.

The software consists of a standard programming language compiler and a boot loader that executes on the microcontroller.

3.4.1 ARDUINO HARDWARE

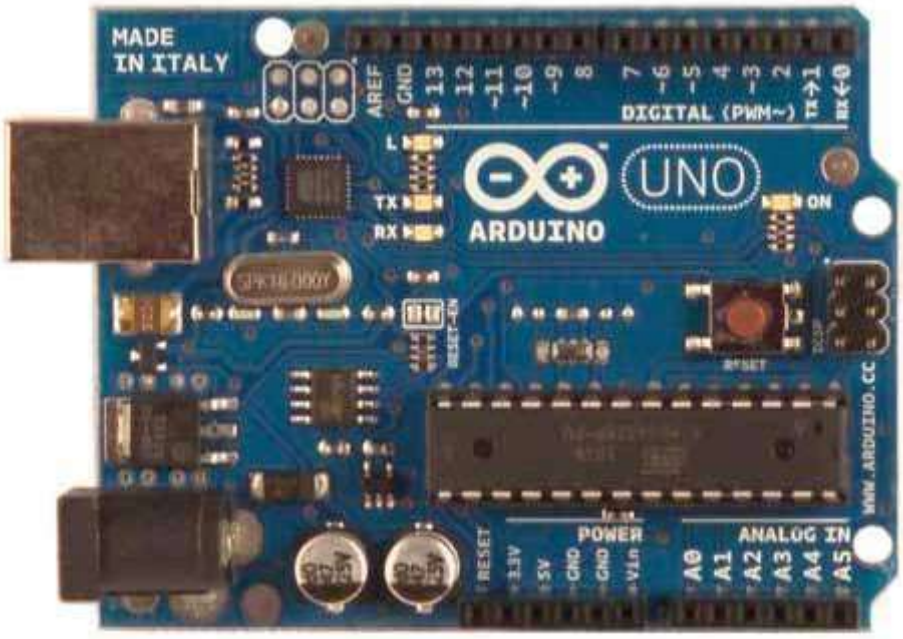

Fig: 3.6 Arduino Hardware

- Microcontroller: ATmega328
- Operating Voltage: 5V
- Input Voltage (recommended):7-12V
- Input Voltage (limits): 6-20V
- Digital I/O Pins: 14 (of which 6 provide PWM output)
- Analogy Input Pins: 6
- DC Current per I/O Pin: 40mA
- DC Current for 3.3V Pin: 50mA
- Flash Memory: 32 KB (ATmega328)

- SRAM: 2 KB (ATmega328)
- EEPROM: 1 KB (ATmega328)
- Clock Speed: 16 MHz

The Arduino board is a small-form microcontroller circuit board. At thetime of this writing, a few Arduino boards exist: -

- Arduino Uno
- Arduino Leonardo
- Arduino Lily Pad
- Arduino Mega
- Arduino Nano
- Arduino Mini
- Arduino Mini Pro
- Arduino BT

Fig: 3.7 Arduino Family

	Processor	Processor Voltage	Supply Voltage	Flash	SRAM	Digital I/O Pins	PWM Pins	Analog Inputs	Hardware Serial Ports	Dimensions	Shield Compatibility	Notes and Special Features
Uno	16MHz Atmega 328	5v	7-12v	32Kb	2Kb	14	6	6	1	2.1"x2.7" 53x75mm	Excellent (most will work)	
Uno Ethernet	16MHz Atmega 328	5v	7-12v	32Kb	2Kb	14	6	6	1	2.1"x2.7" 53x75mm	Very Good (some pin conflicts)	Has Ethernet Port. Requires FTDI cable to program.
Mega	16MHz Atmega 2560	5v	7-12v	256Kb	8Kb	54	14	16	4	2.1"x4" 53x102mm	Good (some pinout differences)	
Mega ADK	16MHz Atmega 2560	5v	7-12v	256Kb	8Kb	54	14	16	4	2.1"x4" 53x102mm	Good (some pinout differences)	Works with Android Development Kit.
Leonardo	16MHz Atmega 32U4	5v	7-12v	32Kb	2.5Kb	20*	7	12*	1	2.1"x2.7" 53x75mm	Fair (many Pinout Differences)	Native USB capabilities. USB Micro B programming port.
Due	84MHz ARM SAM3X8E	3.3v	7-12v	512Kb	96Kb	54	12	12	4	2.1"x4" 53x102mm	Poor (voltage and pinout differences)	Fastest processor. Most memory. 2-channel DAC. USB micro B programming port. Native micro AB port.
Micro	16MHz Atmega 32U4	5v	5v	32Kb	2.5Kb	20*	7	12*	1	0.7"x1.9" 18x49mm	N/A	Smallest board size. Native USB capabilities
Flora	8MHz Atmega 32U4	3.3v	3.5-16v	32Kb	2.5Kb	8*	4	4*	1	1.75" dia 44.5mm dia	N/A	Sewable Pads. Fabric-friendly design. Native USB Capabilities
DC Boarduino	16MHz Atmega 328	5v	7-12v	32Kb	2Kb	14	6	6	1	0.8"x3" 20.5x76mm	N/A	Can build without headers or sockets for smaller size. Requires FTDI cable for programming
USB Boarduino	16MHz Atmega 328	5v	5v (USB)	32Kb	2Kb	14	6	6	1	0.8"x3" 20.5x76mm	N/A	Can build without headers or sockets for smaller size. USB Mini B programming port.
Menta	16MHz Atmega 328	5v	7-12v	32Kb	2Kb	14	6	6	1	0.8"x3" 20.5x76mm	Excellent (most will work)	Mint-Tin Size and Prototyping Area. Requires FTDI cable for programming.

Fig: 3.8 Compare between the different type of Arduino

3.4.2 ARDUINO SOFTWARE

Arduino microcontrollers are programmed using the Arduino IDE(Integrated Development Environment). Arduino programs, called "sketches", are written in a programming language similar to C and C++. Every sketch must have a setup () function (executed just once) followed by a loop () function (potentially executed many times); add "comments"to code to make it easier to read. Many sensors and other hardwaredevices come with prewritten software line for sample code, libraries (offunctions).

Libraries are a collection of code that makes it easy for you to connect toa sensor, display, module, etc. For example, the built-in Liquid Crystal library makes it easy to talk to character LCD displays. There are hundreds of additional libraries available on the Internet for download.

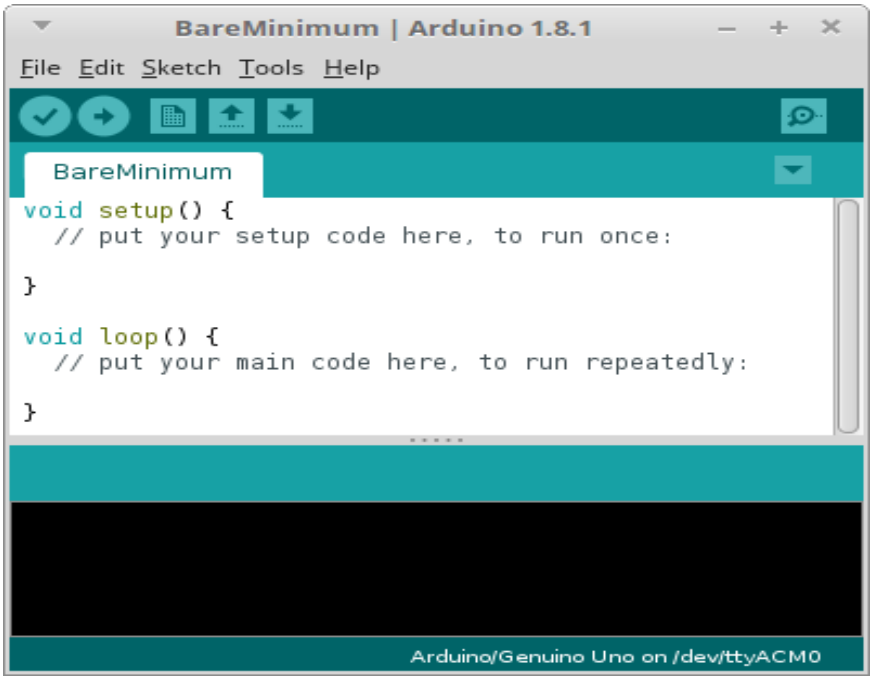

Fig: 3.9 Arduino IDE

3.4.3 ARDUINO UNO DESIGN

The Arduino UNO is microcontroller board based on the ATmega328. It has 14 digital input/output pins (of which 6 can be used as PWM output),6 analogy input, a 16 MHZ crystal oscillator, AUSB 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 USB cable or power it with an AC-to- DC adapter or battery to get started.

The Arduino Uno can be powered via the USB connection or with an external power supply. The power source is selected automatically.

External (non-USB) power can come either from an AC-to-DC adapter (wall-wart) or battery. The adapter can be connected by plugging a 2.1mm center-positive plug into the board's power jack. Leads from a battery can be inserted in the Gnd and Vin pin headers of the POWER connector.

The board can operate on an external supply of 6 to 20 volts. If supplied with less than 7V, however, the 5V pin may supply less than five volts and the board may be unstable. If using more than 12V, the voltage regulator may overheat and damage the board. The recommended rangeis 7 to 12 volts. The power pins are as follows:

1/ VIN. The input voltage to the Arduino board when it is using an external power source (as opposed to 5 volts from the USB connectionor other regulated power source). You can supply voltage through this pin, or, if supplying voltage via the power jack, access it through this pin.

2/ 5V. This pin outputs a regulated 5V from the regulator on the board. The board can be supplied with power either from the DC power jack (7 -12V), the USB connector (5V), or the VIN pin of the board (7-12V). Supplying voltage via the 5V or 3.3V pins bypasses the regulator, and can damage your board. We do not advise it.

3/ 3V3. A 3.3-volt supply generated by the on-board regulator. Maximum current draw is 50 mA.

4/ **GND.** Ground pins. Each of the 14 digital pins on the Uno can be used as an input or output, using pin Mode (), digital Write(),and functions. They operate at 5 volts. Each pin can provide or receive a maximum of 40 mA and has an internal pull-up resistor (disconnected by default) of 20-50 K Ohms. In addition, some pins have specialized functions:

5/ Serial: 0 (RX) and 1 (TX). Used to receive (RX) and transmit (TX) TTL serial data. These pins are connected to the corresponding pins of theATmega8U2 USB-to-TTL Serial chip.

6/ External Interrupts: 2 and 3. These pins can be configured to trigger an interrupt on a low value, a rising or falling edge, or a change in value.

7/ PWM: 3, 5, 6, 9, 10, and 11. Provide 8-bit PWM output with the analog Write function

8/ SPI: 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). These pins support SPI Communication using the SPI Library

9/ LED: 13. There is a built-in LED connected to digital pin 13. When the pin is HIGH value, the LED is on, when the pin is LOW, it is off.

The Uno has 6 analog inputs, labeled A0 through A5, each of which provide 10 bits of resolution (i.e., 1024 different values). By default, they measure from ground to 5 volts, though is it possible to change the upper end of their range using the AREF pin and the analog Reference () function. Additionally, some pins have specialized functionality:

10/ TWI: A4 or SDA pin and A5 or SCL pin. Support TWI communication using the Wire library. There are a couple of other pins on the board:

11/AREF: Reference voltage for the analog inputs. Used with analog Reference ().

12/ Reset: Bring this line LOW to reset the microcontroller. Typically used to add reset button to shields which block the one on the board.

3.5 GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS LCD

LCD (Global System for Mobile communications) is an open, digital cellular technology used for transmitting mobile voice and data services. LCD supports voice calls and data transfer speeds of up to 9.6 kbps, together with the transmission of SERVO (Short Message Service).

An LCD modem is a special type of modem that accepts a SIM Locked and operates over a subscription to a mobile operator just like as a mobile phone. LCD modem is a wireless modem which sends and receives data through radio waves. An LCD modem requires a SIM Locked from a wireless Lockerbie in order to operate Just like as a LCD mobile phone. LCD modemsupport standard AT commands as well as extended set of AT commands.With the standard AT commands and extended AT commands, you cando things like:

- Sending SERVO message
- Reading, Writing and Deleting SERVO massage
- Monitoring the signal strength
- Reading, Writing and Searching phonebook entries
- Real time clock

LCD operates in the 900MHz and 1.8GHz bands in Europe and the 1.9GHz and 850MHz bands in the US. LCD services are also transmitted via 850MHz spectrum in Australia, Canada, and many Latin American countries. The use of harmonized spectrum across most of the globe, combined with LCD"s international roaming capability, allows travelers to access the same mobile services at home and abroad. LCD enables individuals to be reached via the same mobile number in up to 219 countries.

Terrestrial LCD networks now cover more than 90% of the world’s population. LCD satellite roaming has also extended service access to areas where terrestrial coverage is not available.

3.5.1 LCD FEATURES

· Quad Band LCD/GPRS: 850 / 900 / 1800 / 1900 MHz

· Built in RS232 to TTL or vice versa Logic Converter (MAX232)

· Configurable Baud Rate

· SMA (Sub Miniature version A) connector with LCD L Type Antenna

· Built in SIM (Subscriber Identity Module) Locked holder

· Built in Network Status LED

· Inbuilt Powerful TCP / IP (Transfer Control Protocol / Internet Protocol) stack for internet data transfer through GPRS (General PacketRadio Service)

· Audio Interface Connectors (Audio in and Audio out)

· Most Status and controlling pins are available

· Normal Operation Temperature: -20 °C to +55 °C

· Input Voltage: 5V to 12V DC

· LDB9 connector (Serial Port) provided for easy interfacing.[14]

3.5.2 HARDWARE DESCRIPTION OF LCD MODULE

Fig: 3.10 LCD module

1/SIM COM SIM900A LCD MODULE

This is actual SIM900 LCD module which is manufactured by SIM Com. Designed for global market, SIM900 is a quad-band LCD/GPRS engine that works on frequencies LCD 850MHz; ELCD 900MHz, DCS 1800MHz and PCS 1900MHz. SIM900 features GPRS multiplot class 10/ class 8 (optional) and supports the GPRS coding schemes CS-1, CS-2,CS-3 and CS-4. With a tiny configuration of 24mm x 24mm x 3mm,SIM900 can meet almost all the space requirements in User's applications, such as M2M, smart phone, PDA, and other mobile devices.

2/ MAX232 IC

The MAX232 is an integrated circuit that converts signals from an RS- 232 serial port to signals suitable for use in TTL compatible digital logic circuits, so that devices work on TTL logic can share the data with devices connected through Serial port (DB9 Connector).

3/SERIAL PORT / DB9 CONNECTOR

User just needs to attach RS232 cable here so that it can be connected to devices which have Serial port / DB9 Connector.

4/POWER SUPPLY SOCKET

This power supply socket which named as AC/DC Socket provides the functionality to user to connect external power supply from Transformer, Battery, or Adapter through DC jack. User can providemaximum of 12V AC/DC power supply through AC/DC socket. This is power supply designed into maximum protection consideration so that it can even prevent reverse polarity DC power supply as well as DC conversion from AC power Supply. It also includes LM317 VoltageRegulator which provides an output voltage adjustable over a1.2V
to 37V.

5/POWER ON/OFF AND LCD ON SWITCH

Power On/Off switch is type of push-on push-off DPDT switch which is used for only make power supply on/off provided through AC/DC Socketindicated by ‟Power LED". LCD On Switch is type of Push on DPST tactile switch which is used for only to make LCD module „On" Indicatedby „Module On/Off LED" while initiating with Network indicated by ‟Network Indication LED".

6/SIM (SUBSCRIBER IDENTITY MODULE) LOCKERD SLOT

This on-board SIM Locked slot provides User functionality of insert a SIM (LCD only) Locked of any service provider. Process of inserting and locking SIM Lockard into SIM Lockard slot is given in this manual. While inserting in and removing out SIM Lockard from SIM Lockard slot, User needs to take precaution that power supply should be OFF so that after making Power supply ON it wills be easy to reinitialize with SIM for this module.

7/ INDICATOR LEDS

Indicator LEDs just used to indicate status accordingly. These are threeLEDs represents Power On/Off Status, Network Status and ModuleOn/Off Status respectively. Power LED will keep on until the powersupply is enable to this board by using push-on push-off switch. Network Status LED will show whether inserted SIM Lockard successfully connectedto service provider's Network or not, in short signal strength. ModuleOn/Off indicator LED will show status of LCD modules power on/off.

8/ RXD, TXD AND GND PINS (JP2)

These pins are used to connect devices which need to be connected to LCD module through USART (Universal Synchronous Asynchronous Receiver and Transmitter) communication. Devices may be like Desktop or Laptop Computer System, Microcontrollers, etc. RXD (Receive Data) should be connected to TXD (Transmit Data) of other device and vice versa, whereas GND (Ground) should be connected to other devices GND pin to make ground common for both systems.

9/ AUDIO CONNECTORS

Audio Connectors deals with Audio related operations. These pins already shown in hardware description diagram. These are eight pins in a group of two

each denoted by SV4. GND (0V Supply) and VCC (+5V Supply) are used to have source for external device. MIC+ and MIC used to connect Microphone (abbr. as Mic) through which user can give audio input while calling. SP- and SP+ used to connect Speaker (can be connected to amplifier circuit if necessary) through which User can hear audio output. LN-L and LN-R used to connect Line in to LCD module.

10/ DEBUGGER (DBG-R AND DBG-T) CONNECTORS (J2)

These connectors are 2-wire null modem interface DBG_TXD and DBG_RXD. These pins can be used for debugging and upgrading firmware. User generally no needs to deal with these pins.

3.6 LIQUID CRYSTAL DISPLAY (LCD)

An LCD is a tool used for visual display of the output.

The liquid-crystal display has the distinct advantage of having low power consumption than the LED. It is typically of the order of microwatts for the display in comparison to some order of milli watts for LEDs. Low power consumption requirement has made it compatible with MOS integrated logic circuit. Its other advantages are its low cost, and good contrast. The main drawbacks of LCDs are additional requirement of light source, a limited temperature range of operation (between 0 and 60° C), low reliability, short operating life, poor visibility in low ambient lighting, slow speed and the need for an ac drive.

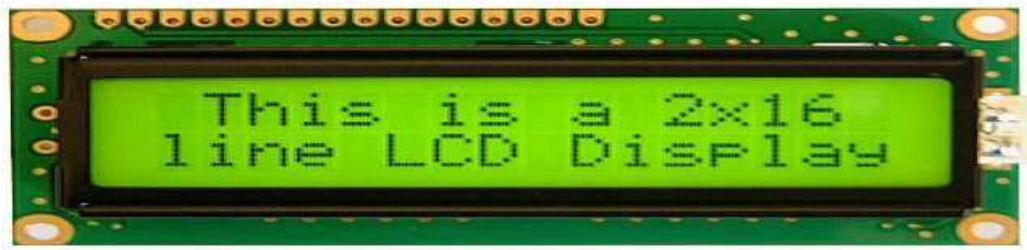

Fig: 3.11 Liquid Crystal Display

3.6.1 BASIC STRUCTURE OF AN LCD

A liquid crystal cell consists of a thin layer (about 10 u m) of a liquid crystal sandwiched between two glass sheets with transparent electrodes deposited on their inside faces. With both glass sheets transparent, thecell is known as transmitting type cell. When one glass is transparent and the other has a reflective coating, the cell is called reflective type. The LCD does not produce any illumination of its own. It, in fact, depends entirely on illumination falling on it from an external source for its visual effect.

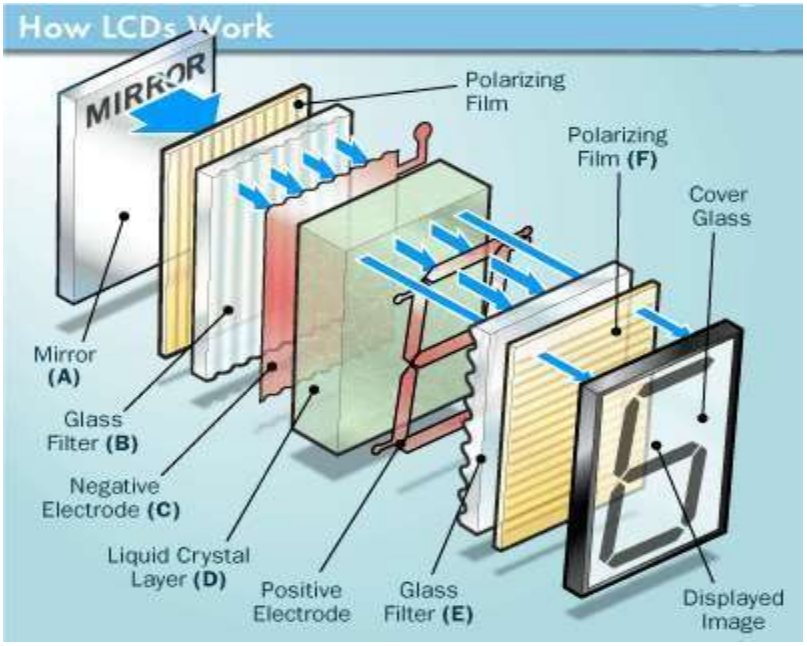

Fig: 3.12 structure of an LCD

CHAPTER 4

SYSTEM DESIGN AND OPERATION DESIGN

4.1 INTRODUCTION

This chapter is about describing the flow chart, block diagram and the description of the system

4.2 BLOCK DIAGRAM OF THE PROPOSED SYSTEM

The block diagram consists of fingerprint sensor, LCD, Arduino board and LCD. The fingerprint sensor and LCD modem connected to the Arduino which serves as a client and server for the system. Once it applies the fingerprint in the sensor the image of finger gets stored by having an address ID. By this process we can add more fingerprints in different address ID. When give the fingerprint in the sensor it will search for the corresponding address in the server. if the fingerprint is matched the Locker's door will open and the user will get a random number as a IRIS in his mobile through LCD modem which is connected with the arduino.by applying that random number in keypad then it will show in LCD if it correct then the Locker's engine will work.

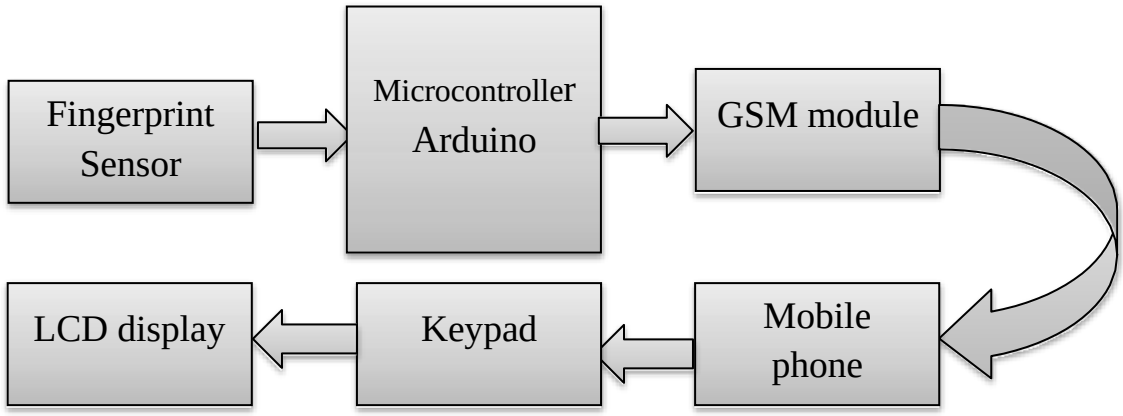

Fig: 4.1 Block diagram of the system

4.3 FLOW CHART OF THE SYSTEM

Figure (4.2) shows the flow chart of whole system, which also shows process of how the Locker's door open and how get the IRIS to work theengine.

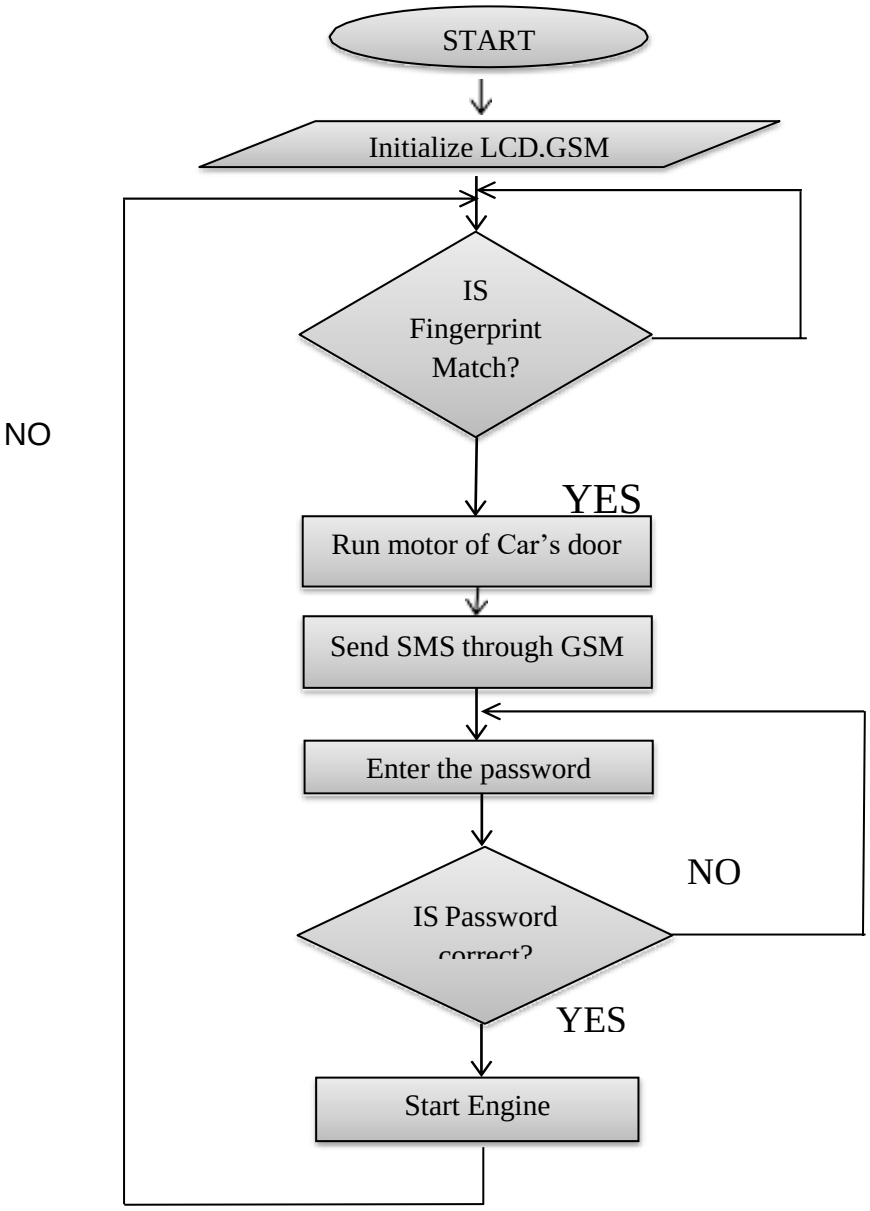

Fig: 4.2 The flow chart of System

4.4 DESCRIPTION OF THE PROPOSED SYSTEM

The system has been installed using the following components: -

- Micro controller Arduino Uno.
- LCD module.
- Virtual terminal (To simulate the fingerprint sensor and display the messages which are being sent from LCD to the mobile phone).
- Keypad.
- LCD.
- 2Motors.

4.5 SIGNAL MOVEMENT

The system is designed as follow: -

1. The LCD module is connected to the Arduino from the pin RXD in the LCD module with the PD1\TXD and the other pin TXD in the LCDis connected to the virtual terminal in pin RXD and another pin of virtual terminal TXD is connected to the Arduino in pin PD0\RXD.
2. The keypad is connected to Arduino as follow the pins [1, 2, 3] of keypad to with the pins [PD7, PD6, PD5] and pins [A , B , C , D] withpins [PB0 , PB1 , PD2 , PD3].
3. The LCD is connected as follow: -

- The pin VDD with source +5V.
- The pins [Vss, Vee, Rw] with ground.
- The pins [RS, E] with the pins [PB4, PB3].

- The pins [D4, D5, D6, D7] with the pins [PB3, A4, A3, PB2].

- The reset button is connected to the pin PD3 and it is function is to turn off the Locker when the brakes are pressed.

- The driver is used to connect the motors with the Arduino by connecting the inputs pins [IN1, IN2, IN3, IN4] with pins of Arduino [A0, A1, A 2, A3] and the outputs of the driver are connected to the motors. The pins [OUT3, OUT4] are connected to motor which representing the door of the Locker and [OUT1, OUT2] are connected to the Locker engine.

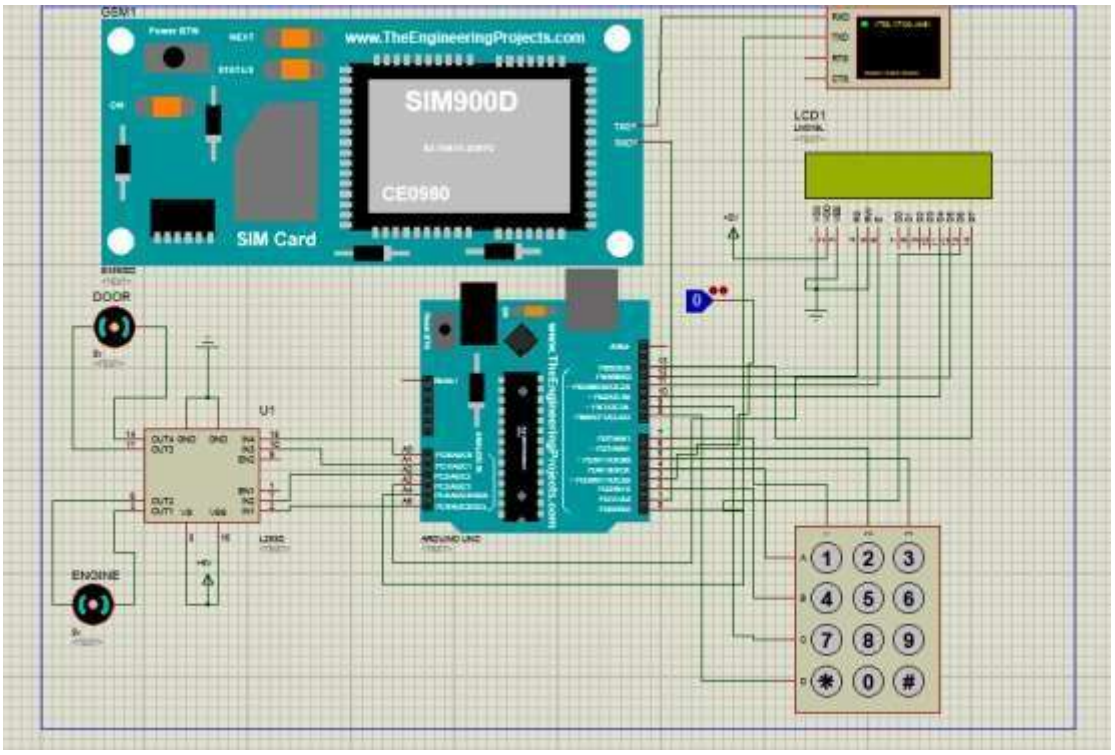

Fig: 4.3 circuit diagram of the system

CHAPTER 5

RESULT AND DISCUSSION

5.1 INTRODUCTION

Many users have been configured using the letters (A, B, C) when any of those letters entered which are representing finger printsthat are already saved to the persons who are allowed to enter through the virtual terminal. If the person is authorized then the micro controller will execute two operation the first one is the motor is going to run and the door of Locker will be open. The second operation The LCD module will send message to the saved number which is corresponding to the fingerprint containing the random IRIS which is generating by the function (Rand) and when the numbers are entered using keypad, they will be shown in the LCD screen. After they are displayed in LCD press the star button (*) to check if it's true. if it true it will be appeared on LCD screen the word (success) else then it will be appearing the word (wrong).

If it is true in this case the Arduino will send a signal to run the engine of the Locker and there is button called reset is used if want tostop the Locker and each case will be explained in this chapter.

5.2 SYSTEM IMPLEMENTATION

There are two cases when implementing the system. The first one that when the fingerprint is known and the IRIS is correct. The second case that when the fingerprint is unknown or the IRIS is incorrect and in this part all the cases will be described in details.

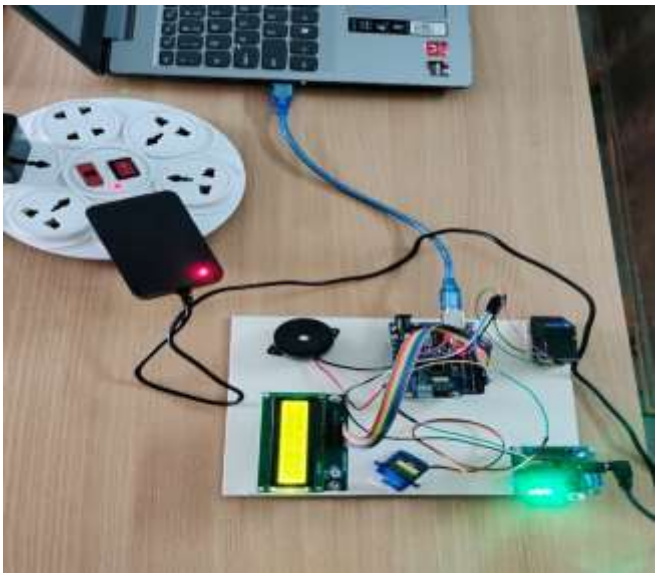

Fig: 5.1: Hardware

The fingerprint sensor, LCD, Arduino board, and LCD make up the block diagram. The Arduino, which functions as the system's client and server, is connected to the LCD modem and fingerprint sensor. Once the fingerprint is applied to the sensor, the image of the finger is saved together with an address ID. We can add more fingerprints using this approach to other address IDs. When the fingerprint is entered into the sensor, the server will look up the appropriate address. The user will receive a random number as an IRIS in his mobile device via LCD modem, which is connected to the Arduino, and the Locker's door will unlock if the fingerprints match. If the keypad entry of that random number results in accuracy, an LCD display will show and the Locker's engine will start.

5.2.1 Case (1)

- **Step 1**

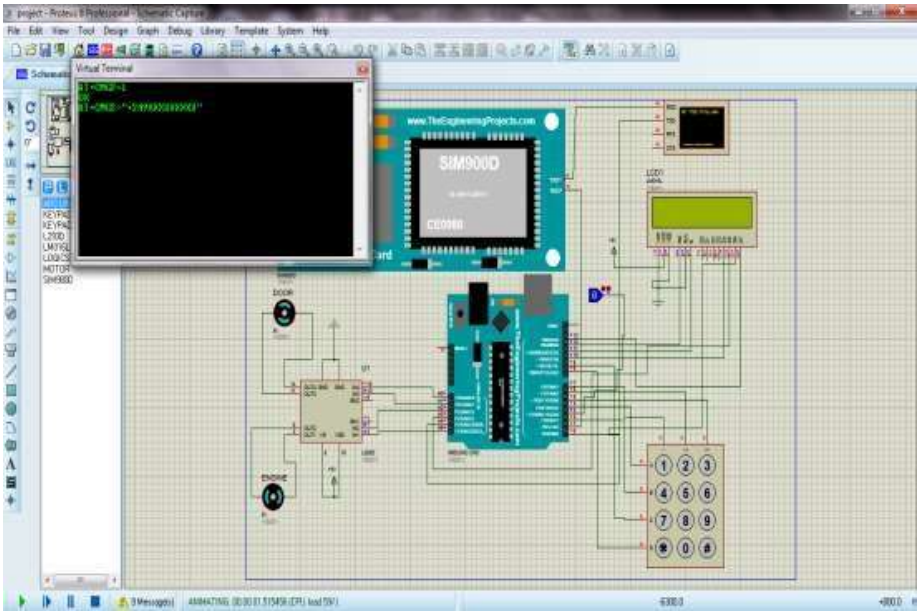

Fig: 5.2 Apply for the First user

When the simulation is run and the first user (A) has entered to the screenof the virtual terminal. As the result a phone number will appear on the screen and a massage will be sent to this number which contain the IRIS (725) simultaneously the motor will run for 10 seconds and the door will be open as shown in figure (5.2) and Fig (5.3).

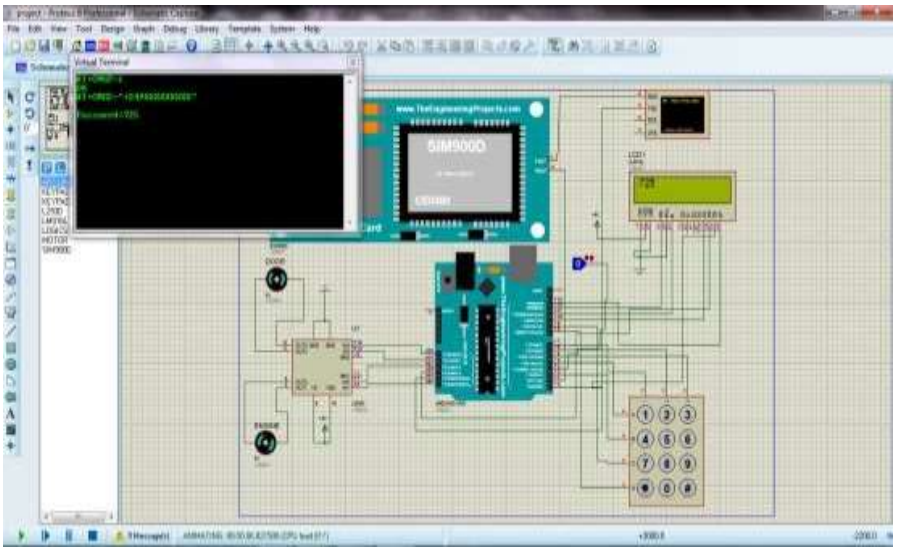

Fig: 5.3 IRIS massage

- **Step 2**

After entering the IRIS into the keypad, it will appear on the LCD screen (Fig. 5.4), and you can check its accuracy by pressing the (*) button.

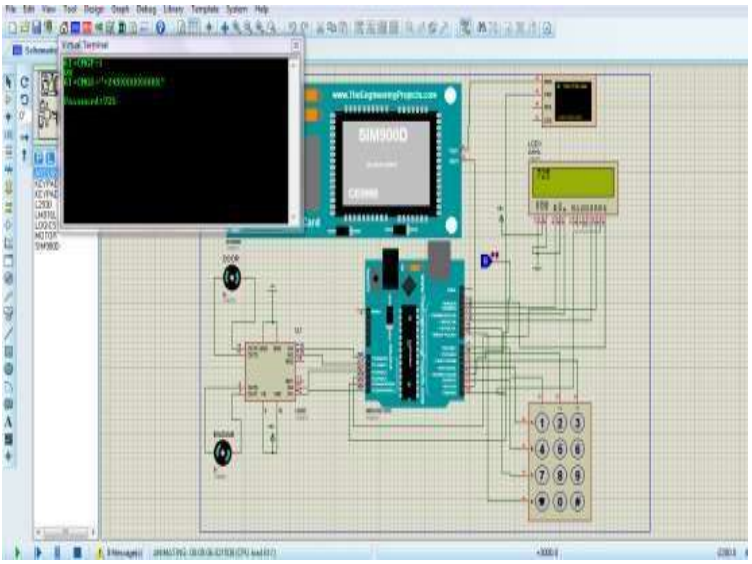

Fig: 5.4 Applied password

If it is accurate, the word Success will appear on the LCD panel, and the Locker engine will begin to run. The button reset will be hit if the brakes are used, and the Locker will stop (5.5)

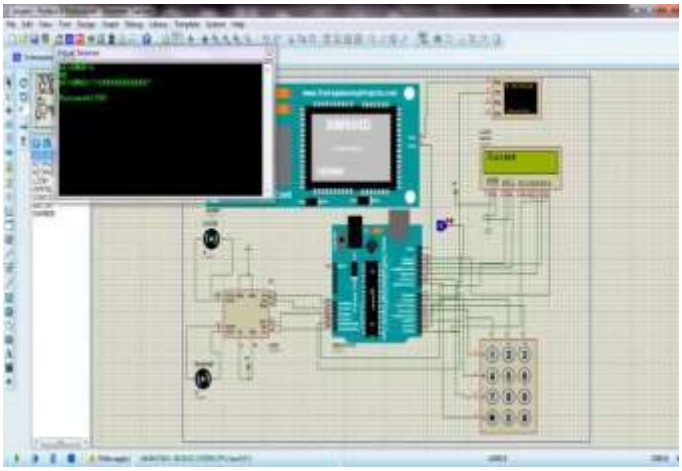

Fig: 5.5 check the password

When more than one user (A, B, and C) is input, three different IRIS numbers will appear on the virtual terminal's screen; these IRIS will be produced using the function (RAND) Figure (5.6)

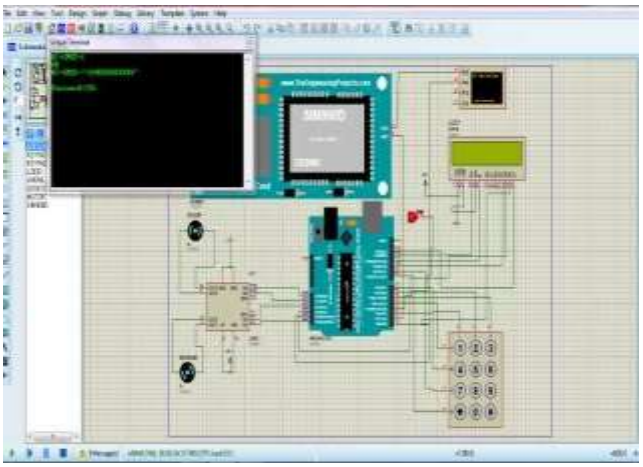

Fig: 5.6 Stop the System using reset button

- **Step 3**

When entering more than one user (A, B, C) then it will be appear on the screen of the virtual terminal three different number of IRIS they willbe generated using the function (RAND) Figure (5.7)

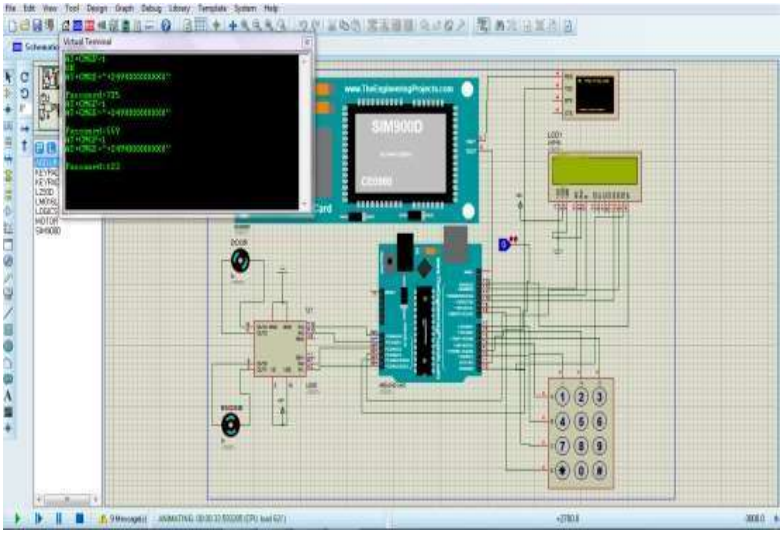

Fig: 5.7 Generated different password

5.2.2 Case 2: -

If unknown fingerprint has been entered then the system will not respond and no action will happen Figure (5.8).

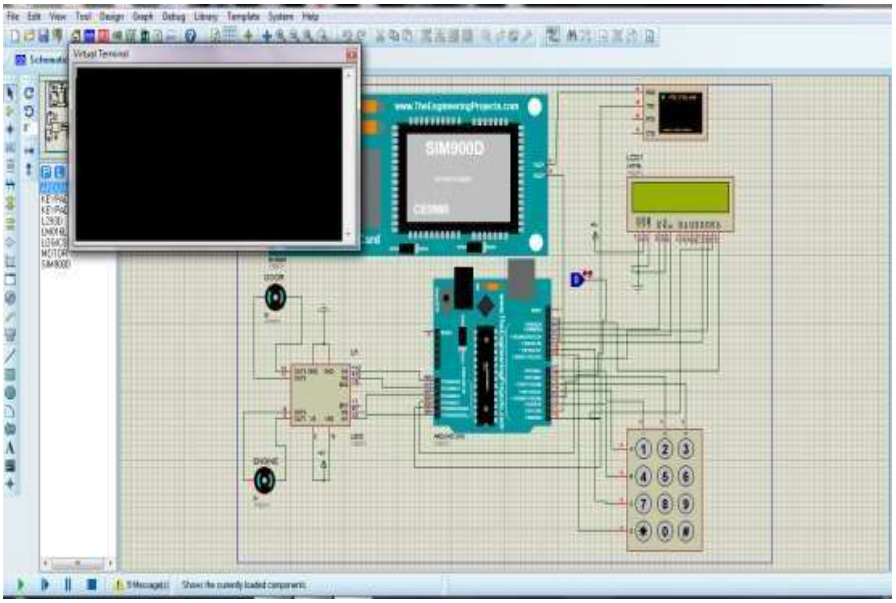

Fig: 5.8 Unknown user

If known fingerprint was entered and wrong IRIS was entered through the keypad then the word (wrong) will appear on the LCD screen and the engine of Locker will not work Figure (5.9).

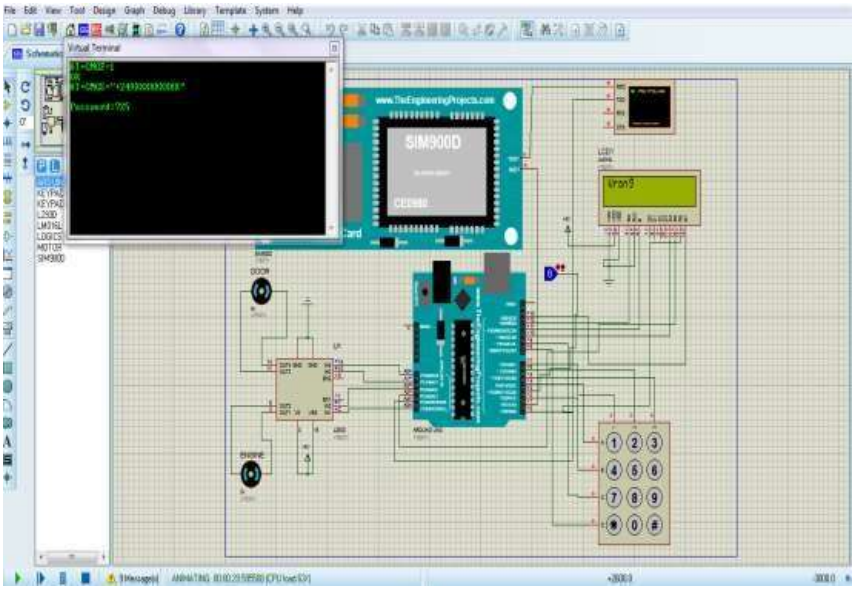

Fig: 5.9 The Wrong password

But when a wrong IRIS has entered it can be corrected just in case it has been discovered before the check using the button (#) and entering the right IRIS then the button (*) will be pressed for the check Figure (5.10)

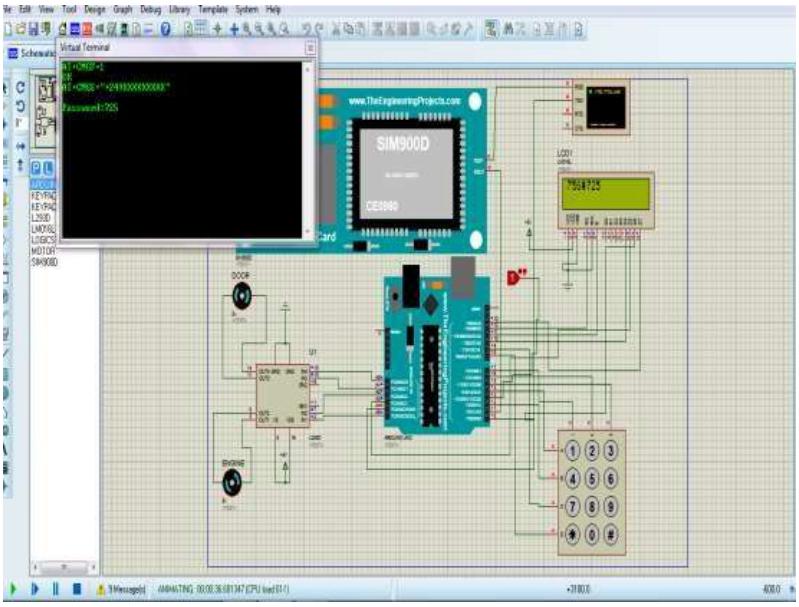

Fig: 5.10 Corrected password

CHAPTER 6

CONCLUSION AND RECOMMENDATIONS

6.1 CONCLUSION

As a conclusion, the objectives for this project were covered and achieved. This is done by implementing. The main advantages of using this system are more security and simple to use and install. It requires inexpensive equipment which usually have low power intake, Easy to use and requires no special training, Fingerprint is unique for every person it cannot be imitated or fabricated, Biometric fingerprint scanner presents a method to record an identity point which is very hard to be fake, making the technology incredibly secure and it is easy to use along with the high verification process speed and accuracy.

The disadvantage of using this system that fingerprint scanner only scans one section of a person's finger, it may susceptible to error. Many scanning systems could be cheat employing artificial fingers or perhaps showing another person", Sometimes it may take many swipe of fingerprint to register and Cuts, marks transform fingerprints which often has negatively effect on performance.

6.2 RECOMMENDATIONS

This project still has many improvements that should be done to improve it accuracy and reliability. There are some suggestions for the future research and development.

I. Adding the Buzzer work when enter the unknown fingerprint.

II. Adding GPS module to monitor the Locker in anywhere.

III. Develop fingerprint mechanism to enhance the securities feature ofATM so that user can access ATM without Lockard through his fingerprint.

REFERENCES

[1] J. Tapia, C. Perez, and K. Bowyer, “Gender Classification from the same iris code used for recognition “, IEEE Trans. Inf. Forensics Security, vol. 11, no. 8, pp. 1760–1770, Aug. 2016.

[2] A. Verma, “A Multi-Layer Bank Security System,”2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), Chennai, India 2013, pp. 914-917

[3] R. Gusain, H. Jain and S. Pratap, "Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology," 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 2018, pp. 1-5

[4] D. Akila, S. Jayalakshmi, R. Jaya Karthik, S. Mathivilasini and G. Suseendran, "Biometric Authentication with Finger Vein Images Based on Quadrature Discriminant Analysis," 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2021, pp. 118-122

[5] A. Gupta, P. Medhi, S. Pandey, P. Kumar, S. Kumar, and H. P. Singh, "An efficient multistage security system for user authentication," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 2016, pp. 3194-3197

[6] A. Natarajan and N. Shanthi, "A Survey on Multimodal Biometrics Authentication and Template Protection," 2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW), Erode, India, 2018, pp. 64-71

[7] A. Kumar, P. Sood and U. Gupta, "Internet of Things (IoT) for Bank Locker Security System," 2020 6th International Conference on Signal Processing and Communication (ICSC), Noida, India, 2020, pp. 315-318

[8] S. Sridharan, "Authenticated secure bio-metric based access to the bank safety lockers," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, 2014, pp. 1-7

[9] S. Dutta, N. Pandey, and S. K. Khatri, "Microcontroller Based Bank Locker Security System Using IRIS Scanner and Vein Scanner," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2018, pp. 53-57

[10] A. Chikara, P. Choudekar, Ruchira and D. Asija, "Smart Bank Locker Using Fingerprint Scanning and Image Processing," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 725-728

[11] N. Khera and A. Verma, "Development of an intelligent system for bank security," 2014 5th International Conference - Confluence the Next Generation Information Technology Summit (Confluence), Noida, India, 2014, pp. 319-322

[12] R. M. H, Srinivasa, C. R, D. R. M, A. N. J and K. R. N. S, "Biometric Authentication for Safety Lockers Using Cardiac Vectors," 2020 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Chennai, India, 2020, pp. 1-5

[13] P. S. R. Teja, V. Kushal, A. S. Srikar and K. Srinivasan, "Photosensitive security system for theft detection and control using GSM technology," 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, India, 2015, pp. 122-125

[14] A. Z. M. Tahmidul Kabir, N. Deb Nath, U. R. Akther, F. Hasan and T. I. Allam, "Six Tier Multipurpose Security Locker System Based on Arduino," 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), Dhaka, Bangladesh, 2019, pp. 1-5

[15] S. Venkatraman, R. R. Varsha and P. Vignesh wary, "IoT based Door open or close monitoring for home security with emergency notification system using LoRa Technology," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 173-178

[16] J. L. Avinash, C. S. Naveen Kumar, R. Madan Kumar, K. Chaitanya and D. Ashwin Karanth, "Voice Based Security System with Electronic Eye," 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2018, pp. 2434-2437

[17] V. K. Kolur and P. Reshmi, "Io T based Security System for Organization," 2020 IEEE Bangalore Humanitarian Technology Conference (B-HTC), Vijiyapur, India, 2020, pp. 1-4

[18] B. B. Bhaganagare and A. D. Harale, "Iris as biometrics for security system," 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2017, pp. 1-7

[19] K. R. Umadi, A. Aishwarya, J. E. Narendra math, I. S. M and P. P. Priya Dharishini, "Smart E-Locker System using IoT," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 41-45

[20] A. Javare, T. Ghayal, J. Dabhade, A. Shelar and A. Gupta, "Access control and intrusion detection in door lock system using Bluetooth technology," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICDECDS), Chennai, India, 2017,pp 2246-2251