VISVESVARAYA TECHNOLOGICAL UNIVERSITY
BELGAUM-590 014

A Project Report
On
PADLOCK

Submitted in partial fulfillment of the requirement for the award of the degree of

BACHELOR OF ENGINEERING
in
COMPUTER SCIENCE AND ENGINEERING

Submitted by

R. NITHYA, USN: 1VE13CS057
RASHMI. R, USN: 1VE13CS063
S.SUJATHA, USN: 1VE13CS066
T.K. KRUPA, USN: 1VE13CS091

Under the Guidance of
Mr. VENKATAGIRI. J
Asst. professor,
Department of Computer Science and Engineering
Sri Venkateshwara College of Engineering, Bangalore-562 157

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SRI VENKATESHWARA COLLEGE OF ENGINEERING,
BANGALORE - 562 157.

2016-2017

VISVESVARAYA TECHNOLOGICAL UNIVERSITY
BELGAUM-590 014

A Project Report
On
PADLOCK

Submitted in partial fulfillment of the requirement for the award of the degree of

BACHELOR OF ENGINEERING
in
COMPUTER SCIENCE AND ENGINEERING

Submitted by

R. NITHYA, USN: 1VE13CS057
RASHMI. R, USN: 1VE13CS063
S.SUJATHA, USN: 1VE13CS066
T.K. KRUPA, USN: 1VE13CS091

Under the Guidance of
Mr. VENKATAGIRI. J
Asst. professor,
Department of Computer Science and Engineering
Sri Venkateshwara College of Engineering, Bangalore-562 157

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SRI VENKATESHWARA COLLEGE OF ENGINEERING,
BANGALORE - 562 157.

2016-2017

SRI VENKATESHWARA COLLEGE OF ENGINEERING,
Vidyanagar, Bangalore – 562 157
Department of Computer Science and Engineering

CERTIFICATE

This is to certify that the project entitled **"PADLOCK"** carried out by **Ms. R.Nithya (1VE13CS057), Ms. Rashmi.R (1VE13CS063) , Ms. S.Sujatha (1VE13CS066) and Ms. T.K. Krupa(1VE13CS091)** a bonafide student of Sri Venkateshwara College of Engineering, in partial fulfillment for the award of Bachelor of Engineering in Computer Science and Engineering of **Visvesvaraya Technological University, Belgaum** during the academic year 2016-2017. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the Report deposited in the departmental library. The project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the said Degree.

Signature of the Guide	Signature of the HOD	07-06-2017
Mr. Venkatagiri. J	**Dr. Shrishail Math**	**Signature of the Principal**
Asst. professor	HOD-CSE, SVCE	**Dr. Suresha**
Dept. of CSE, SVCE	Bangalore	Principal, SVCE
Bangalore		Bangalore

Name of the examiners: **Signature with date**

1. Dr. Suresha
2. Shruthi. J

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without complementing those who made it possible, whose guidance and encouragement made our efforts successful.

My sincere thanks to highly esteemed institution **SRI VENKATESHWARA COLLEGE OF ENGINEERING** for grooming up me in to be software engineer.

I express our sincere gratitude to **Dr. SURESHA**, Principal, SVCE, Bengaluru for providing the required facility.

I am extremely thankful to **Dr. SHRISHAIL MATH,** HOD of CSE, SVCE for providing support and encouragement.

I am grateful to my guide **Mr. VENKATAGIRI. J,** Asst. Professor Dept. of CSE, SVCE who helped me to complete this project successfully by providing guidance, encouragement and valuable suggestion during entire period of the project.

Finally I am grateful to my parents and friends for their invaluable support guidance and encouragement.

R. NITHYA (1VE13CS057)

RASHMI R (1VE13CS063)

S. SUJATHA (1VE13CS066)

T.K.KRUPA (1VE13CS091)

PADLOCK: AN INNOVATIVE METHOD OF ACCESSING CONTROL FOR HOME SECURITY

ABSTRACT

Security systems are often being breached by intelligent thieves and hence there is always a need of new methods to be invented to provide proper security to the homes and also anywhere else. Use of innovative technologies will improve the security to a great extent till the technology becomes open to all. The aim of this paper is to provide the door access control and security by using Biometrics. Basically the paper is divided into two categories: one for the owner and the other for the guest

The goal of our project is to design and assemble a biometric access control system that uses fingerprint scanning and recognition to authenticate the user. Upon successful authentication, the user will be allowed to access the safe. On the other hand, if the access is denied, it will give a warning message that the access is denied and the buzzer alarm rings and thus the un-authorized person will not have access to the lock. The fingerprint scanning device utilizes serial communication. This device will be connected to our microprocessor using the UART ports. The system will consist of an Atmel Atmega32 microprocessor ARDUINO development board, LCD display, Biometric fingerprint sensor, serial-to-USB, buzzer, GSM, Keypad , DC motor, Driver circuit, Arduino to PC interfacing and a power supply. GSM is used to give a temporary access to a friend or a guest.

CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
1.	**INTRODUCTION**	1
2.	**SYSTEM SPECIFICATION**	
	2.1.HARDWARE REQUIREMENTS	
	2.1.1 ARDUINO	2
	2.1.2 LCD	9
	2.1.3 GSM	11
	2.1.4 BIOMETRIC	16
	2.1.5 DRIVER CIRCUIT	20
	2.1.6 DC MOTOR	23
	2.1.7 KEYPAD	25
	2.2.SOFTWARE REQUIREMENTS	
	2.2.1 PROGRAMMING	26
	2.2.2 MEMORY	26
	2.2.3 INPUT/OUTPUT	26
	2.2.4 COMMUNICATION	27
	2.2.5 SFG DEMO	28
3.	**PROJECT DESIGN**	
	3.1 PURPOSE	31
	3.2 DESCRIPTION	31
	3.3 FLOW CHART	32
4.	**IMPLEMENTATION**	
	4.1 ALGORITHM	33
	4.2 SOURCE CODE	34
5.	**SNAPSHOTS**	41

6.	**TESTING**	
	6.1 TESTING	42
	6.2 TESTING PLANS	42
7.	**CONCLUSION**	44
	FUTURE ENHANCEMENT	44
	REFEFRENCES	45

LIST OF FIGURES

SL NO.	FIGURE NAME	PAGE NO.
1.	Arduino Board	3
2.	An official Arduino Uno R2 with descriptions of the I/O locations	4
3.	Pin configurations of Arduino	6
4.	LCD	9
5.	GSM phases	11
6.	Biometric Device	15
7.	Types of Biometric Sensor	16
8.	Fingerprint Recognition	16
9.	Face Recognition	17
10.	Iris Recognition	17
11.	Voice Recognition	17
12.	Signature Recognition	18
13.	Conversion of fingerprint to binary format	18
14.	Circuit diagram of driver circuit	19
15.	Pin configuration of L293D driver circuit	20
16.	DC motor	22
17.	Keypad	23
18.	Code snippet of communication in Arduino software	25
19.	SFG demo dialogue box	26
20.	Selecting the ports Dialogue box	26
21.	Open Device success box	26

22.	Warning message dialogue box if open device fails	27
23.	Enrolling the fingerprint with the address	27
24.	warning message dialogue box	27
25.	Success in enrolling the fingerprint	28
26.	Success to enroll box	28
27.	warning message	28
28.	Block Diagram of the project	29
29.	Flowcharts for owner and guest	30
30.	Minutiae Algorithm	31
31.	Parts of a fingerprint considered for matching	31
32.	Process of the flow of minutiae algorithm	32
33.	Angles and bifurcations for converting into binary form	32
34.	Message on LCD for Access granted	39
35.	Message on LCD for Access denied	39
36.	Snapshot of the whole working project with network	39
37.	Snapshot of the whole project	40
38.	Snap of the message received in the phone through GSM	40

LIST OF TABLES

SL NO.	TABLE NAME	PAGE NO.
1.	Technical specifications of Arduino board	5
2.	PORT Function Multiplexing	8
3.	Pin configurations of LCD	9
4.	Illustration of circuit diagram of driver circuit	19

PADLOCK: AN INNOVATIVE METHOD OF ACCESSING CONTROL FOR HOME SECURITY

CHAPTER 1

INTRODUCTION

Automation offers lifestyle improvement through the combination of various systems into a unified, familiar, intuitive and non-threatening solution. In perspective of safety and the urge to live a more comfortable life, it is anticipated that more people will prefer to choose the smart homes solution in the future, for the range of benefits that is offered. Facilitating the remote-control of household appliances and the home environment along with sophisticated security schemes through biometric identification technologies like thumb expression is a promising way to establish futuristic home-environment which comprises of both security and comfort simultaneously.

Human and Computer interaction has become an increasingly important part of our lives because of colossal technological infusion into our lifestyles. Whether it is our living room, bedroom, or office room, there could be a range of electronic equipment that requires commands to perform some important tasks. Secure your project with biometrics - this all-in-one optical fingerprint sensor will make adding fingerprint detection and verification super simple. These modules are typically used in safes - there's a high powered DSP chip that does the image rendering, calculation, feature-finding and searching. Connect to any microcontroller or system with TTL serial, and send packets of data to take photos, detect prints, hash and search. Fingerprinting is the promising way for providing high end security, hence we are designing this project and also an added advantage is that we can give temporary access to a guest or a friend. This project has applications in various fields, hence this will be a very useful concept proposed and implemented. This can be designed in nanotechnology also for real time usage.

CHAPTER 2

SYSTEM SPECIFICATION

2.1 HARDWARE REQUIREMENTS:

2.1.1 ARDUINO

2.1.1.1Overview

Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. You can tell your board what to do by sending a set of instructions to the microcontroller on the board. To do so you use the Arduino programming language (based on Wiring), and the Arduino Software (IDE), based on Processing.

2.1.1.2 Why Arduino?

Thanks to its simple and accessible user experience, Arduino has been used in thousands of different projects and applications. The Arduino software is easy-to-use for beginners, yet flexible enough for advanced users. It runs on Mac, Windows, and Linux.

Arduino also simplifies the process of working with microcontrollers, but it offers some advantage for teachers, students, and interested amateurs over other systems:

- **Inexpensive** - Arduino boards are relatively inexpensive compared to other microcontroller platforms.
- **Cross-platform** - The Arduino Software (IDE) runs on Windows, Macintosh OSX, and Linux operating systems. Most microcontroller systems are limited to Windows.

- **Simple, clear programming environment** - The Arduino Software (IDE) is easy-to-use for beginners, yet flexible enough for advanced users to take advantage of as well.
- **Open source and extensible software** - The Arduino software is published as open source tools, available for extension by experienced programmers. The language can be expanded through C++ libraries, and people wanting to understand the technical details can make the leap from Arduino to the AVR C programming language on which it's based.
- **Open source and extensible hardware** - The plans of the Arduino boards are published under a Creative Commons license, so experienced circuit designers can make their own version of the module, extending it and improving it.

2.1.1.3 Hardware descriptions of Arduino

Arduino is open-source hardware. The hardware reference designs are distributed under a Creative Commons Attribution Share-Alike 2.5 license and are available on the Arduino website. Layout and production files for some versions of the hardware are also available. The source code for the IDE is released under the GNU General Public License, version 2.

Although the hardware and software designs are freely available under copyleft licenses, the developers have requested that the name "Arduino" be exclusive to the official product and not be used for derived works without permission.

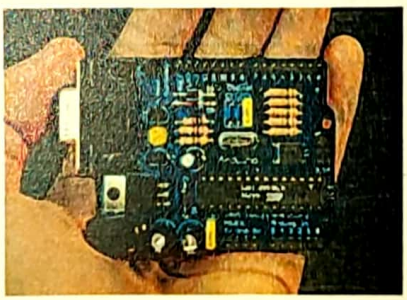

Figure 1: Arduino Board

An early Arduino board[11] with an RS-232 serial interface (upper left) and an Atmel ATmega8 microcontroller chip (black, lower right); the 14 digital I/O pins are at

the top, the 6 analogue input pins at the lower right, and the power connector at the lower left.

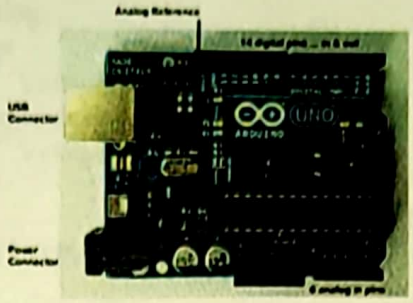

Figure 2: An official Arduino Uno R2 with descriptions of the I/O locations

The Arduino board exposes most of the microcontroller's I/O pins for use by other circuits. The *Diecimila*,[a] *Duemilanove*,[b] and current *Uno*[c] provide 14 digital I/O pins, six of which can produce pulse-width modulated signals, and six analog inputs, which can also be used as six digital I/O pins. These pins are on the top of the board, via female 0.1-inch (2.54 mm) headers. Several plug-in application shields are also commercially available.

2.1.1.4 Digital Pins

The pins on the Arduino can be configured as either inputs or outputs. This document explains the functioning of the pins in those modes. While the title of this document refers to digital pins, it is important to note that vast majority of Arduino (Atmega) analog pins, may be configured, and used, in exactly the same manner as digital pins.

2.1.1.5 Properties of Pins Configured as INPUT

Arduino (Atmega) pins default to inputs, so they don't need to be explicitly declared as inputs with pinMode() when you're using them as inputs. Pins configured this way are said to be in a **high-impedance state**. Input pins make extremely small demands on the circuit that they are sampling, equivalent to a series resistor of 100 megohm in front of the pin.

2.1.1.6 Technical specifications

Microcontroller	ATmega328P
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limit)	6-20V
Digital I/O Pins	14 (of which 6 provide PWM output)
PWM Digital I/O Pins	6
Analog Input Pins	6
DC Current per I/O Pin	20 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	32 KB (ATmega328P) of which 0.5 KB used by bootloader
SRAM	2 KB (ATmega328P)
EEPROM	1 KB (ATmega328P)
Clock Speed	16 MHz
LED_BUILTIN	13
Length	68.6 mm
Width	53.4 mm
Weight	25 g

Table 1: Technical specifications of Arduino board

2.1.1.7 ATmega328p Microcontroller

Introduction

The Atmel picoPower ATmega328/P is a low-power CMOS 8-bit microcontroller based on the AVR® enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATmega328/P achieves throughputs close to 1MIPS per MHz. This empowers system designer to optimize the device for power consumption versus processing speed.

Pin Configurations

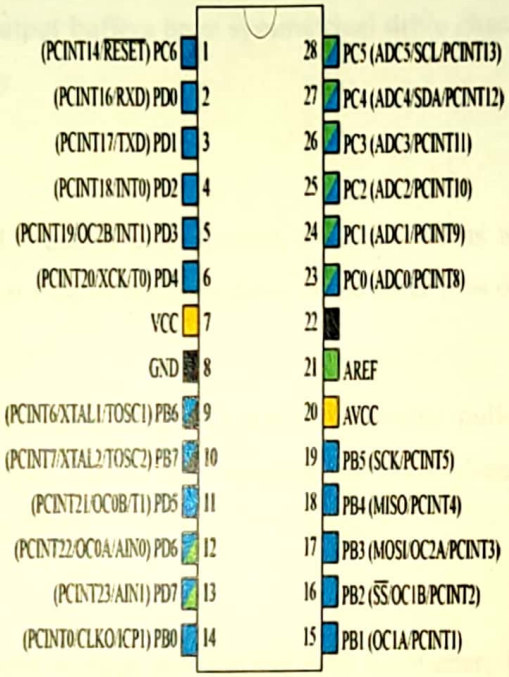

Figure 3: Pin configurations of Arduino

2.1.1.8 Pin Descriptions:

VCC

Digital supply voltage.

GND

Ground.

Port B (PB [7:0]) XTAL1/XTAL2/TOSC1/TOSC2

Port B is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port B output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port B pins that are externally pulled low will source current if the pull-up resistors are activated.

Port C (PC [5:0])

Port C is a 7-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The PC[5:0] output buffers have symmetrical drive characteristics with both high sink and source capability.

PC6/RESET

If the RSTDISBL Fuse is programmed, PC6 is used as an I/O pin. Note that the electrical characteristics of PC6 differ from those of the other pins of Port C.

Port D (PD [7:0])

Port D is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port D output buffers have symmetrical drive characteristics with both high sink and source capability.

AV_{CC}

AV_{CC} is the supply voltage pin for the A/D Converter, PC[3:0], and PE[3:2]. It should be externally connected to V_{CC}, even if the ADC is not used.

AREF

AREF is the analogue reference pin for the A/D Converter

ADC [7:6] (TQFP and VFQFN Package Only)

In the TQFP and VFQFN package, ADC[7:6] serve as analog inputs to the A/D converter. These pins are powered from the analog supply and serve as 10-bit ADC channels.

(32-pin MLF/TQFP) Pin#	(28-pin MLF) Pin#	(28-pin PIPD) Pin#	PAD	EXTINT	PCINT	ADC/AC	OSC	T/C #0	T/C #1	USART 0	I2C 0	SPI 0
1	1	5	PD[3]	INT1	PCINT19			OC2B				
2	2	6	PD[4]		PCINT20			T0		XCK0		
4	3	7	VCC									
3	4	8	GND									
6	-	-	VCC									
5	-	-	GND									
7	5	9	PB[6]		PCINT6		XTAL1/ TOSC1					
8	6	10	PB[7]		PCINT7		XTAL2/ TOSC2					
9	7	11	PD[5]		PCINT21			OC0B	T1			
10	8	12	PD[6]		PCINT22	AIN0		OC0A				
11	9	13	PD[7]		PCINT23	AIN1						
12	10	14	PB[0]		PCINT0		CLKO	ICP1				
13	11	15	PB[1]		PCINT1			OC1A				
14	12	16	PB[2]		PCINT2			OC1B				SS0
15	13	17	PB[3]		PCINT3			OC2A				MOSI0
16	14	18	PB[4]		PCINT4							MISO0
17	15	19	PB[5]		PCINT5							SCK0
18	16	20	AVCC									
19	-	-	ADC6			ADC6						
20	17	21	AREF									
21	18	22	GND									
22	-	-	ADC7			ADC7						
23	19	13	PC[0]		PCINT8	ADC0						
24	20	24	PC[1]		PCINT9	ADC1						
25	21	25	PC[2]		PCINT10	ADC2						
26	22	26	PC[3]		PCINT11	ADC3						
27	23	27	PC[4]		PCINT12	ADC4					SDA0	
28	24	28	PC[5]		PCINT13	ADC5					SCL0	
29	25	1	PC[6]/ RESET		PCINT14							

Table 2: PORT Function Multiplexing

2.1.2 LCD

LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits. These modules are preferred over seven segments and other multi segment LEDs. The reasons being: LCDs are economical; easily programmable; have no limitation of displaying special & even custom characters (unlike in seven segments), animations and so on.

A **16x2 LCD** means it can display 16 characters per line and there are 2 such lines. In this LCD each character is displayed in 5x7 pixel matrix. This LCD has two registers, namely, Command and Data.

Pin Diagram:

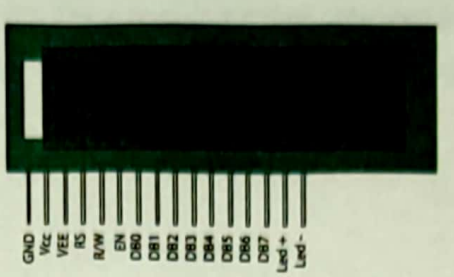

Figure 4: LCD

Pin No	Function	Name
1	Ground (0V)	Ground
2	Supply voltage; 5V (4.7V – 5.3V)	Vcc
3	Contrast adjustment; through a variable resistor	V_{EE}
4	Selects command register when low; and data register when high	Register Select
5	Low to write to the register; High to read from the register	Read/write
6	Sends data to data pins when a high to low pulse is given	Enable
7	8-bit data pins	DB0
8		DB1
9		DB2
10		DB3
11		DB4
12		DB5
13		DB6
14		DB7
15	Backlight V_{CC} (5V)	Led+
16	Backlight Ground (0V)	Led-

Table 3: Pin configurations of LCD

3.1.2.1 Working:

The liquid crystals used in the LCD are Twisted Nemantic (TN), a type of liquid crystals that are twisted at 90o with the surface. In this state, crystals allow the light to pass

through the polarizer but on applying a voltage, they get untwisted and block the light to passing through the polarizer.

The LCD controller in the form of COB IC sends the electric signals to the electrodes which are sandwiched in between the glasses. Electrodes apply the voltage to the corresponding crystals as per the signals received from the ICs. These crystals are then untwisted and blocks the light (from LED strip) making those area darker on the glass. By applying voltage to specific crystals, a desired shape is formed on the LCD.

2.1.3 GSM

GSM (Global System for Mobile Communications, originally ***Groupe Spécial Mobile***), is a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones.

The GSM standard was developed as a replacement for first generation (1G) analog cellular networks, and originally described a digital, circuit switched network optimized for full duplex voice telephony. This was expanded over time to include data communications, first by circuit switched transport, then packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution or EGPRS).

Further improvements were made when the 3GPP developed third generation (3G) UMTS standards followed by fourth generation (4G) LTE Advanced standards.

2.1.3.1 GSM phases

Phase 1

Phase 1 contains the most common services including

-Voice telephony

-International roaming

-Basic fax/data service(up to 9.6 Kbits/s)

-Call forwarding

-Call barring

-Short message service(SMS)

Phase 1 also incorporated features such as ciphering and Subscriber Identity Module (SIM) cards. Phase 1 specifications were then closed and cannot be modified.

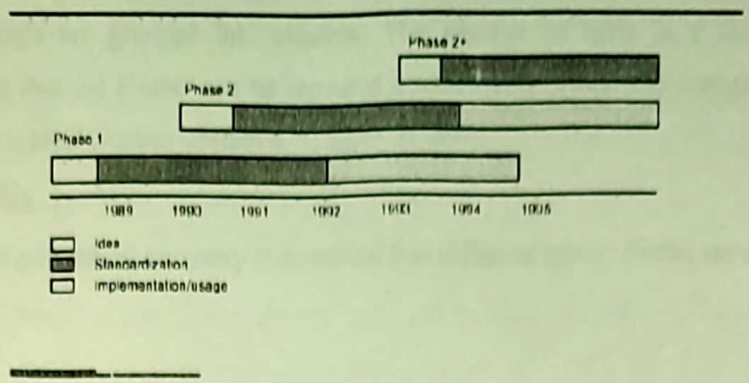

Figure 5: GSM phases

Phase 2

Additional features were introduced in GSM phase 2 including

Advice of charge

-Calling line identification

-Call waiting

-Call hold

-Conference calling

-Closed user groups

-Additional data communication capabilities

Phase 2+

The standardization groups have already begun to define the next phase. 2+. The phase 2+ program will cover multiple subscriber numbers and a variety of business oriented features. Some of the enhancements offered by Phase 2+ include

-Multiple service profiles

-Private numbering plans

-Access to Centrex services

2.1.3.2 Cellular Systems:

The cellular structure

In a cellular system, the covering area of an operator is divided into cells. A cell corresponds to the covering area of one transmitter or a small collection of transmitters. The size of a cell is determined by the transmitter's power.

Cluster

The cells are grouped into clusters. The number of cells in a cluster must be determined so that the cluster can be repeated continuously within the covering area of an operator. The typical clusters contain 4, 7, 12 or 21 cells.

Type of Cells

The density of population a country is so varied that different types of cells are used

- Macro cells
- Micro cells
- Selective cells
- Umbrella cells

Macro Cells

The macro cells are large cells for remote and sparsely populated areas.

Micro Cells

These cells are used for densely populated areas. By splitting the existing areas into smaller cells, the number of channels available is increased as well as the capacity of the cells. The power level of the transmitters used in these cells is then decreased, reducing the possibility of interference between neighbouring cells.

Selective cells

It is not always useful to define a cell with a full coverage of 360 degrees. In some cases, cells with a particular shape and coverage are needed. These cells are called selective cells. Typical examples of selective cells are the cells that may be located at the entrances of tunnels where coverage of 360 degrees is not needed. In this case, a selective cell with coverage of 120 degrees is used.

Umbrella Cells

A freeway crossing very small cells produces an important number of handovers among the different small neighbouring cells. In order to solve this problem, the concept of umbrella cells is introduced. An umbrella cell covers several microcells. The power level inside an umbrella cell is increased comparing to the power levels used in the microcells that form the umbrella cell. When the speed of the mobile is too high, the mobile is handed off to the umbrella cell. The mobile will then stay longer in the same cell (in this case the umbrella cell).

2.1.3.3 Structure of GSM Network:

The network behind the GSM system seen by the customer is large and complicated in order to provide all of the services which are required. It is divided into a number of sections and these are each covered in separate articles.

- The Base Station Subsystem (the base station and their controllers).
- The Network and Switching Subsystem (the part of the network most similar to a fixed network). This is sometimes also just called the core network.
- The GPRS Core Network (the optional part which allows packet based Internet connections).

2.1.3.4 Accessing a GSM network:

In order to gain access to GSM services, a user needs three things:

-A billing relationship with a mobile phone operator. This is usually either where services are paid for in advance of them being consumed(prepaid), or where bills are issued and settled after the service has been consumed(postpaid).

-A mobile phone that is GSM compliant and operates at the same frequency as the operator. Most phone companies sell phones from third-party manufactures.

-A subscriber Identity Module (SIM) card, which is activated by the operator once the billing relationship is established. After activation the card is then programmed with the subscriber's Mobile Subscriber Integrated Services Digital Network Number (MSISDN)(the telephone number).

How speech is encoded during mobile phone calls

During a GSM call, speech is converted from analogue sound waves to digital data by the phone itself, and transmitted through the mobile phone network by digital means. (Though older parts of the fixed Public Switched Telephone Network may use analog transmission.)

The digital algorithm used to encode speech signals is called a codec.

Radio Service (GPRS)

The General Packet Radio Service (GPRS) is a packet-switched data transmission protocol, which was incorporated into the GSM standard in 1997. It is backwards-compatible with systems that use pre-1997 versions of the standard. GPRS does this by sending packets

to the local mobile phone mast (BTS) on channels not being used by circuit-switched voice calls or data connections.

Short Message Service (SMS)

Short Message Service (more commonly known as text messaging) has become the most used data application on mobile phones, with 74% of all mobile phone users worldwide already as active users of SMS, or 2.4 billion people by the end of 2007.

SMS text messages may be sent by mobile phone users to other mobile users or external services that accept SMS.

2.1.3.5 Features of GSM Technology:

There are many features associated with GSM technology due to which it is bar far the most leading mobile communication technology in the world today. GSM technology facilitates with high speed integrated data, voice data, fax, mail, voice mail and mostly used SMS feature.

GSM Services:

It is important to note that all the GSM services were not introduced since the appearance of GSM but they have been introduced in a regular way. The GSM Memorandum of Understanding (MoU) defined four classes for the introduction of the different GSM services.

- E1: Introduced at start of the service.
- E2: Introduced at the end of 1991.
- E3: Introduced at the availability of half rate channels.
- A: These services are optional.

Three types of services can be distinguished

- Teleservices
- Bearer services
- Supplementary services

2.1.3.6 Advantages of GSM:-

GSM is more suitable network with robust pitfall. · Low signal inside the building and house. The subscriber globally creates much better in network effect for GSM handset maker's carries and end users. · It can be use repeaters. · A customer has been better voice

quality and low cost amount in alternatives to making cells like (sms) etc. · It is easy to implement. · International roaming is not a big problem. · GSM allows network operation to after roaming service so that customer can use whole over the world.

2.1.3.7 Disadvantages of GSM:-

Many of the technology are patented and should be license from qualcomm. · When customers using particular sites going up and the range of he sites goes down. · Manufactures are not release IS-95 devices due to the lack of the big market and it come in late in market. · IS-95 is normally installed in small tower. · Gsm has fixed max call sites range up to 35 km that is very limited

2.1.4 BIOMETRIC

The word biometric is derived from the Greek words bio and metric. Where bio means life and metric means to measure. Biometrics are used to identify his or her physical and behaviour characteristics of a person. This method of identification is chosen over traditional methods, including PIN numbers and passwords for its exactness and case sensitiveness. Based on the designing, this system can be used as an identification system or authentication system.

Fig 6: Biometric Device

2.1.4.1 Types of Biometric Sensor

Biometric sensors or access control systems are classified into two types such as Physiological Biometrics and Behavioral Biometrics. The physiological biometrics mainly include face recognition, fingerprint, hand geometry, Iris recognition and DNA.

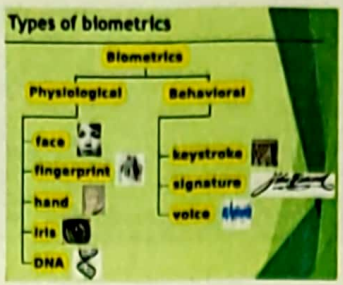

Fig 7: Types of Biometric Sensor

a.) Fingerprint Recognition

Fingerprint Recognition includes taking a fingerprint image of a person and records its features like arches, whorls, and loops along with the outlines of edges, minutiae and furrows. Matching of the Fingerprint can be attained in three ways, such as minutiae, correlation and ridge

- Minutiae based fingerprint matching stores a plane includes a set of points and the set of points are corresponding in the template and the i/p minutiae.
- Correlation based fingerprint matching overlays two fingerprint images and association between equivalent pixels is calculated.
- Ridge feature based fingerprint matching is an innovative method that captures ridges, as minutiae based fingerprint capturing of the fingerprint images is difficult in low quality.

Fig 8: **Fingerprint Recognition**

b.) Face Recognition

Face recognition system is a one type of biometric computer application which can identify or verify a person from a digital image by comparing and analyzing patterns. These biometric systems are used in security systems. Present facial recognition systems work with face prints and these systems can recognize 80 nodal points on a human face.

Fig 9: Face Recognition

c.) Iris Recognition

Iris recognition is a one type of bio-metric method used to identify the people based on single patterns in the region of ring shaped surrounded the pupil of the eye. Generally, the iris has a blue, brown, gray or green color with difficult patterns which are noticeable upon close inspection. Please follow the below link to know more about iris recognition technology.

Fig 10: Iris Recognition

d.) Voice Recognition

Voice recognition technology is used to produce speech patterns by combining behavioral and physiological factors that can be captured by processing the speech technology. The most important properties used for speech authentication are nasal tone, fundamental frequency, inflection, cadence.

Figure 11: Voice Recognition

e.) Signature Recognition

Signature recognition is a one type of biometric method used to analyze and measure the physical activity of signing like the pressure applied, stroke order and the speed. Some biometrics are used to compare visual images of signatures. Signature recognition can be operated in two different ways, such as static and dynamic.

Figure 12: Signature Recognition

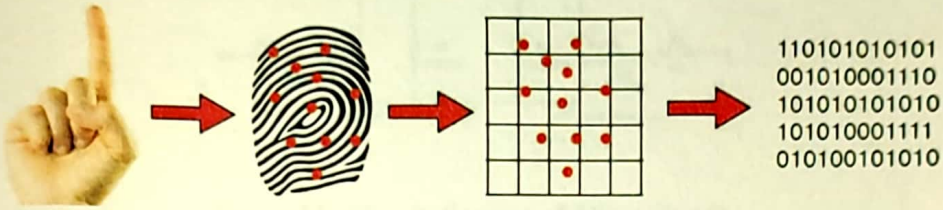

Figure 13: Conversion of fingerprint to binary format

There are several ways an electronic time clock system can verify that somebody is who they say they are. Most systems are looking for one or more of the following:

- What you have
- What you know
- Who you are

2.1.5 DRIVER CIRCUIT

The circuit given here is of a simple H bridge motor driver circuit using easily available components. H Bridge is a very effective method for driving motors and it finds a lot of applications in many electronic projects especially in robotics.

The circuit shown here is a typical four transistor H Bridge. The diodes D1 to D4 provide a safer path for the back emf from the motor to dissipate and thus it protects the

corresponding bipolar transistors from damage. Resistors R1 to R4 limit the base current of the corresponding transistors. Working of this circuit is very easy to understand. When terminal D is grounded and A is pulled to +Vcc, transistors Q1 and Q4 will be on and current passes through the motor from left to right. When terminal B is grounded and C is pulled to +Vcc, transistors Q3 and Q2 will be on and current passes through the motor from right to right making the motor to rotate in the opposite direction.

2.1.5.1 CIRCUIT DIAGRAM:

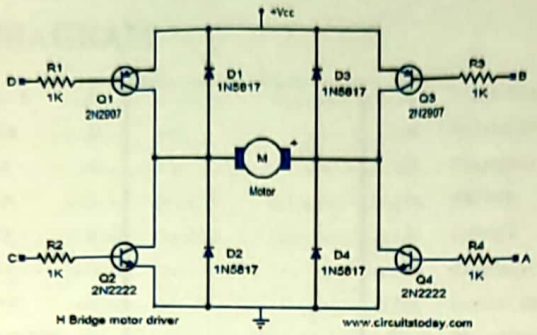

Figure 14: Circuit diagram of driver circuit

Action	A	B	C	D
Coast/Roll/Off	GND or disconnected	+Vcc or disconnected	GND or disconnected	+Vcc or disconnected
Forward	GND or disconnected	GND	+Vcc	+Vcc or disconnected
Reverse	+Vcc	+Vcc or disconnected	GND or disconnected	GND
Brake/Slow Down	+Vcc	+Vcc or disconnected	+Vcc	+Vcc or disconnected

Table 4: Illustration of circuit diagram of driver circuit

A bidirectional **H bridge** DC motor control circuit is shown here. The circuit is based on the IC L298 from ST Microelectronics. L298 is a dual full bridge driver that has a wide

operating voltage range and can handle load currents up to 3A. In the circuit diode D1 to D4 are protection diodes.

2.1.5.2 L293D DESCRIPTION

L293D is a typical Motor driver or Motor Driver IC which allows DC motor to drive on either direction. L293D is a 16-pin IC which can control a set of two DC motors simultaneously in any direction. It means that you can control two DC motor with a single L293D IC. Dual H-bridge *Motor Driver integrated circuit (IC)*.

a.) L293D PIN DIAGRAM

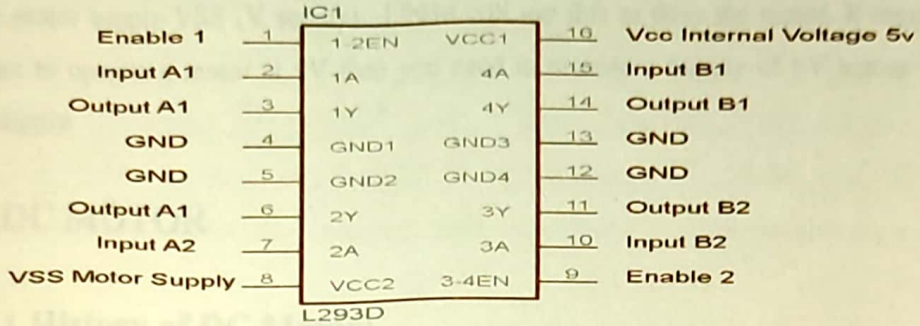

Figure 15: Pin configuration of L293D driver circuit

b.) WORKING OF L293D

There are 4 input pins for this l293d, pin 2,7 on the left and pin 15 ,10 on the right as shown on the pin diagram. Left input pins will regulate the rotation of motor connected across left side and right input for motor on the right hand side. The motors are rotated on the basis of the inputs provided across the input pins as LOGIC 0 or LOGIC 1.

In simple you need to provide Logic 0 or 1 across the input pins for rotating the motor. Lets consider a Motor connected on left side output pins (pin 3,6). For rotating the motor in clockwise direction the input pins has to be provided with Logic 1 and Logic 0.

•**Pin 2** = **Logic 1** and **Pin 7** = **Logic 0** | Clockwise Direction

•**Pin 2** = **Logic 0** and **Pin 7** = **Logic 1** | Anticlockwise Direction

•**Pin 2** = **Logic 0** and **Pin 7** = **Logic 0** | Idle [No rotation] [Hi-Impedance state]

•**Pin 2 = Logic 1** and **Pin 7 = Logic 1** | Idle [No rotation]

In a very similar way the motor can also operated across input pin 15,10 for motor on the right hand side.

2.1.5.3 VOLTAGE SPECIFICATION

VCC is the voltage that it needs for its own internal operation 5v; L293D will not use this voltage for driving the motor. For driving the motors it has a separate provision to provide motor supply VSS (V supply). L293d will use this to drive the motor. It means if you want to operate a motor at 9V then you need to provide a Supply of 9V across VSS Motor supply.

2.1.6 DC MOTOR

2.1.6.1 History of DC Motor:

At the most basic level, electric motors exist to convert electrical energy into mechanical energy. This is done by way of two interacting magnetic fields -- one stationary, and another attached to a part that can move. A number of types of electric motors exist, but most BEAMbots use DC motors[1] in some form or another. DC motors have the potential for very high torque capabilities, are easy to miniaturize, and can be "throttled" via adjusting their supply voltage. DC motors are also not only the simplest, but the oldest electric motors.

A **DC motor** is a mechanically commutated electric motor powered from direct current (DC). The stator is stationary in space by definition and therefore so is its current. The current in the rotor is switched by the commutator to also be stationary in space. This is how the relative angle between the stator and rotor magnetic flux is maintained near 90 degrees, which generates the maximum torque.

2.1.6.2 Principles of Operation of DC Motor:

In any electric motor, operation is based on simple electromagnetism. A current-carrying conductor generates a magnetic field; when this is then placed in an external magnetic field, it will experience a force proportional to the current in the conductor, and to the strength of the external magnetic field.

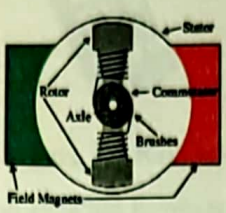

Figure 16: DC motor

Every DC motor has six basic parts -- axle, rotor (a.k.a., armature), stator, commutator, field magnet(s), and brushes. In most common DC motors (and all that BEAMers will see), the external magnetic field is produced by high-strength permanent magnets[1].

2.1.6.8 Advantages of DC Motor:

- Speed control over a wide range both above and below the rated speed
- High starting torque
- Accurate steep less speed with constant torque
- Quick starting, stopping, reversing and acceleration
- Free from harmonics, reactive power consumption and many factors which make dc motors more advantageous compared to an ac induction motors.

2.1.6.9 Disadvantages of DC Motor:

- High initial cost
- Increased operation and maintenance cost due to presence of commutator and brush gear
- Cannot operate in explosive and hazard conditions due to sparking occur at brush (risk in commutation failure)

2.1.7 KEYPAD

2.1.7.1 4x4 Matrix Keypad

Keypad is a commonly used device to get user input. Although simple push switches can be used to get user input, as we have done so, this would require 1I/O line per switch.

Figure 17: Keypad

Keypads are collection of push switches however arranged in the form of a matrix. So there are rows and columns of switches. The two connections of a switch are also connected in the matrix, so that the row has common connection and column has a common connection.

2.1.7.2 Features

- Contact debouncing.
- Easy to interface.
- Interfaces to any microcontroller or microprocessor.
- Data valid output signal for interrupt activation.

2.1.7.3 Applications

- Vending machines.
- Public phones.
- Ticketing.

2.2 Software development

2.2.1 Programming

The Arduino/Genuino Uno can be programmed with the (Arduino Software (IDE)). Select "Arduino/Genuino Uno from the Tools > Board menu (according to the microcontroller on your board). For details, see the reference and tutorials.

The ATmega328 on the Arduino/Genuino Uno comes preprogrammed with a bootloader that allows you to upload new code to it without the use of an external hardware programmer. It communicates using the original STK500 protocol (reference, C header files).

Power

The Arduino/Genuino Uno board 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.

2.2.2 Memory

The ATmega328 has 32 KB (with 0.5 KB occupied by the bootloader). It also has 2 KB of SRAM and 1 KB of EEPROM (which can be read and written with the EEPROM library).

2.2.3 Input and Output

Each of the 14 digital pins on the Uno can be used as an input or output, using pinMode(), digitalWrite(), and digitalRead() functions. They operate at 5 volts.

In addition, some pins have specialized functions:

- 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 the ATmega8U2 USB-to-TTL Serial chip.
- 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. See the attachInterrupt() function for details.
- PWM: 3, 5, 6, 9, 10, and 11. Provide 8-bit PWM output with the analogWrite() function.
- SPI: 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). These pins support SPI communication using the SPI library.
- LED: 13. There is a built-in LED driven by digital pin 13. When the pin is HIGH value, the LED is on, when the pin is LOW, it's off.
- TWI: A4 or SDA pin and A5 or SCL pin. Support TWI communication using the Wire library.

2.2.4 Communication

Arduino/Genuino Uno has a number of facilities for communicating with a computer, another Arduino/Genuino board, or other microcontrollers. The ATmega328 provides UART TTL (5V) serial communication, which is available on digital pins 0 (RX) and 1 (TX). An ATmega16U2 on the board channels this serial communication over USB and appears as a virtual com port to software on the computer. The 16U2 firmware uses the standard USB COM drivers, and no external driver is needed. However, on Windows, a .inf file is required. The Arduino Software (IDE) includes a serial monitor which allows simple textual data to be sent to and from the board. The RX and TX LEDs on the board will flash when data is being transmitted via the USB-to-serial chip and USB connection to the computer (but not for serial communication on pins 0 and 1).

```
#define LED_PIN 13              // Pin number attached to LED.

void setup() {
  pinMode(LED_PIN, OUTPUT);     // Configure pin 13 to be a digital
output.
}

void loop() {
  digitalWrite(LED_PIN, HIGH);  // Turn on the LED.
  delay(1000);                  // Wait 1 second (1000 milliseconds).
  digitalWrite(LED_PIN, LOW);   // Turn off the LED.
  delay(1000);                  // Wait 1 second.
}
```

Figure 18: Code snippet of communication in Arduino software

This program uses the functions *pinMode()*, *digitalWrite()*, and *delay()*, which are provided by the internal libraries included in the IDE environment.

3.2.5 SFG DEMO

SFG DEMO is a software exclusively designed for enrolling the fingerprints to a fingerprint sensor, where it converts the enrolled fingerprint into the binary form. Except for

enrolling, it searches for the fingerprints in its stored database. Below are the steps to use SFG demo for enrolling the fingerprints.

1. Start up the software

Figure 19: SFG demo dialogue box

2. Click **Open Device** (in the bottom left corner). A new window opens up. Select the COM port used by the USB – serial converter (You can get the COM port from the device manager) and press OK when done.

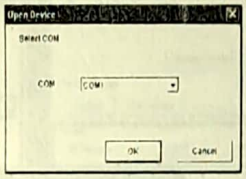

Figure 20: Selecting the ports Dialogue box

You can see the following blue success message and some device statistics such as **Baud rate, Package size and Security level** in the bottom corner. You can change the baud rate in the bottom left hand corner as well as the security level (how sensitive it is) but we suggest leaving those alone until you have everything running and you want to experiment. They should default to 57600 baud and security level 3 so set them if they're wrong

Figure 21: Open Device success box

On the other hand, if there is any connection error or if the default address/password has been modified, you will get an error message.

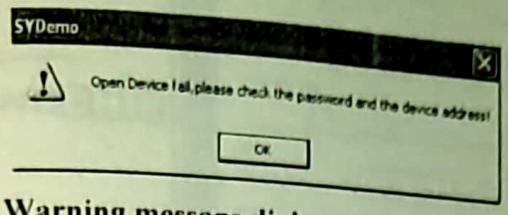

Figure 22: Warning message dialogue box if open device fails

3. Now its time to enroll a new finger! Click the Preview checkbox and press the **Enroll** button next to it (See the red box). **Con Enroll** means Continuous enroll which you can use if you have many fingers to enroll. When the box comes up enter the ID you want to use. You can use up to 162 ID numbers.

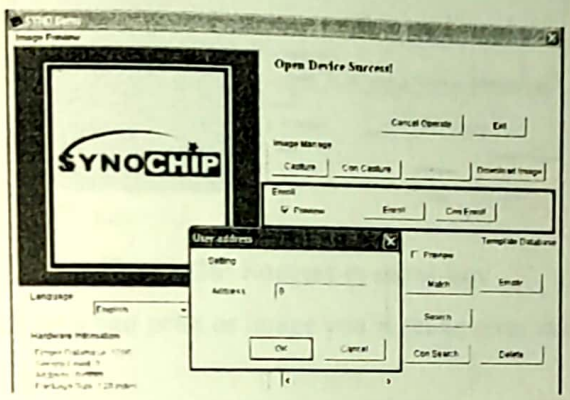

Figure 23: Enrolling the fingerprint with the address

If the given ID is already used, then the software asks for overwrite. Click **Yes** for replacing the existing fingerprint. If you do not wish to replace, then click *No* and give new ID

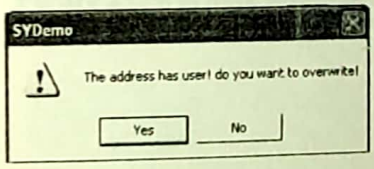

Figure 24: warning message dialogue box

4. Once the ID is given, the software will ask you to press the finger to the sensor. Now the LED blinks rapidly. You can place your finger on the window.

You can then see a preview (if you clicked the preview checkbox) of the fingerprint

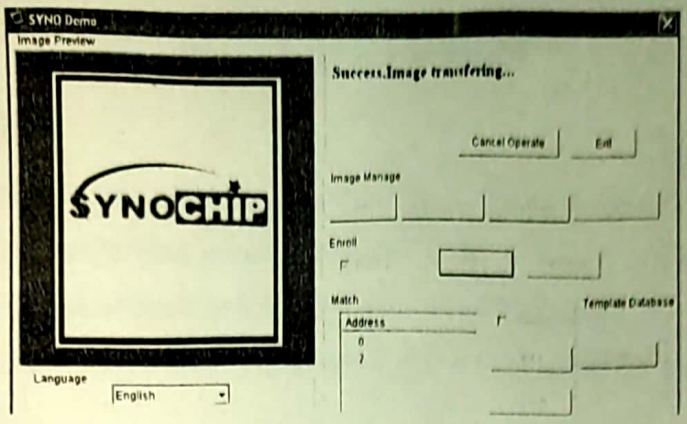

Figure 25: Success in enrolling the fingerprint

You will have to place the finger once again to get a second clean print. Use the same finger. On success you will get a notice.

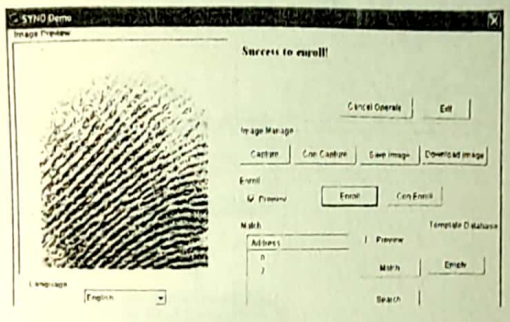

Figure 26: Success to enrol box

If there's a problem such as a bad print or image you'll get an error message and have to do it again.

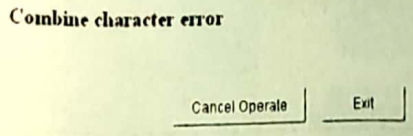

Figure 27: warning message

CHAPTER 3

PROJECT DESIGN

3.1 PURPOSE

-Purpose of designing this project is to design a high end security lock for a smart home, and also this can be used in various applications like : to lock the vehicles wheel, used in prisons, used to lock personal or private lockers, personal rooms etc.

-This design also enables the authorized person to provide a temporary access to the lock to a guest or a friend.

3.2 DESCRIPTION

Block diagram:

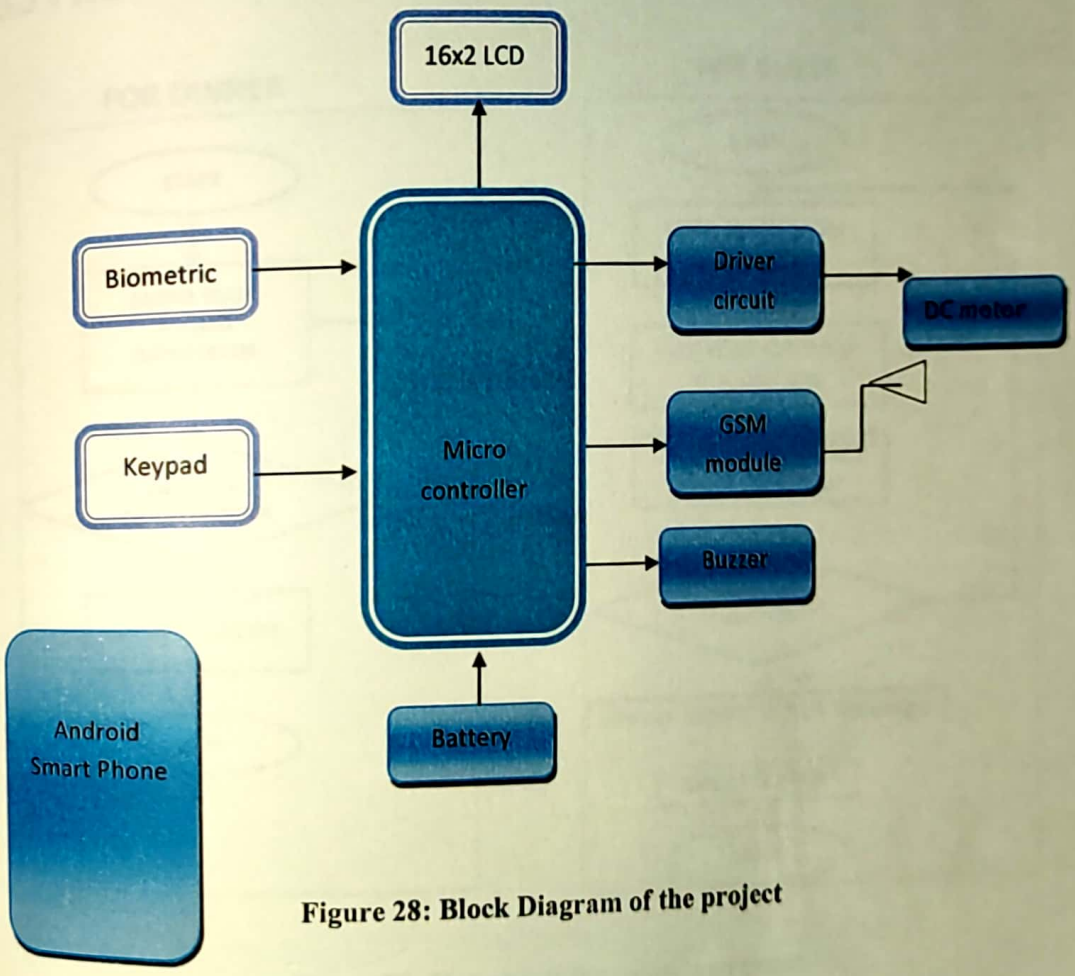

Figure 28: Block Diagram of the project

Working principle:

- In this paper, we propose a novel method of making security method more reliable and secure.
- The security system or workflow is divided into two blocks: one for the owner and the other for the guest.
- The owner can use the biometric and if found correct then the DC motor will rotate whereas the guest has to first enter the thumb expression then he should enter the password given to him through the GSM module.
- If the enter expression is wrong then the buzzer gets activated and the status for each try is displayed on the LCD.

3.3 FLOW CHART

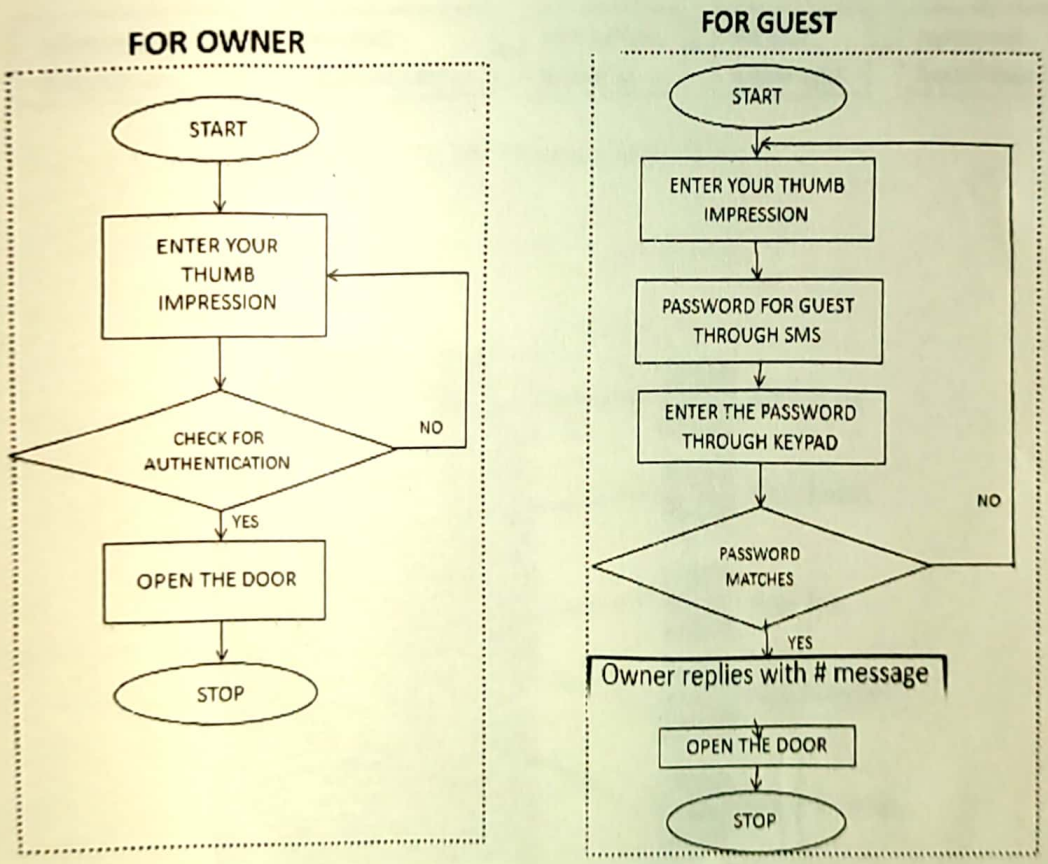

Figure 29: Flowcharts for owner and guest

CHAPTER 4

IMPLEMENTATION

4.1 ALGORITHM:

MINUTAE ALGORITHM

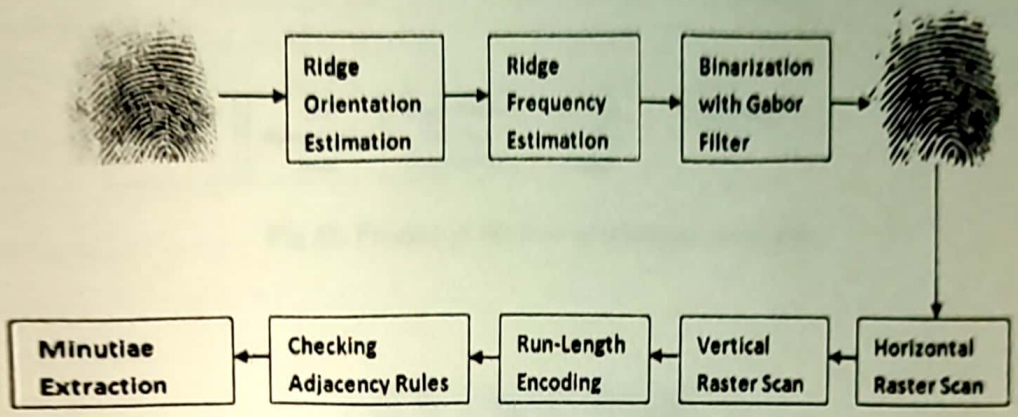

Fig 30: Minutiae Algorithm

Fig 31: Parts of a fingerprint considered for matching

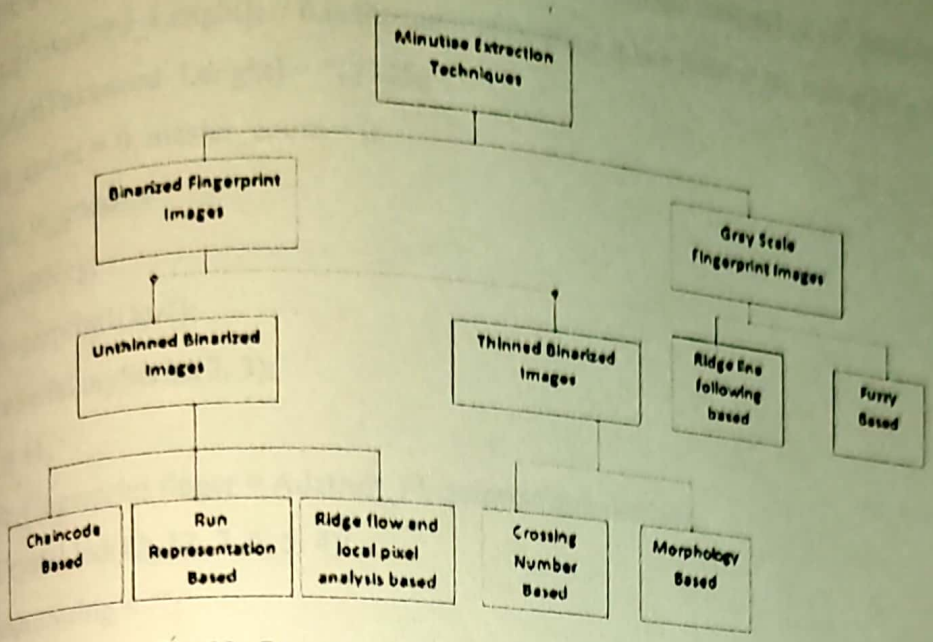

Fig 32: Process of the flow of minutiae algorithm

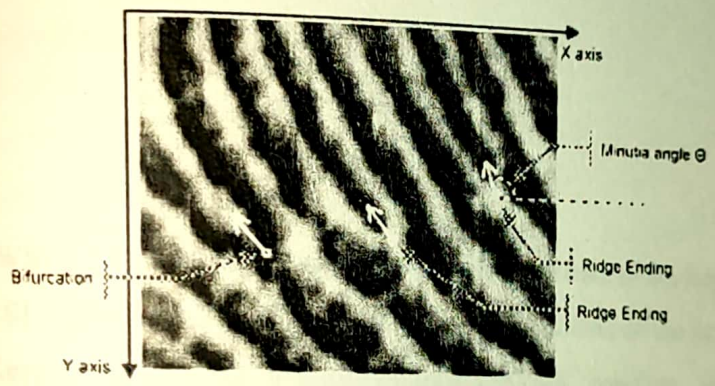

Fig 33: Angles and bifurcations for converting into binary form

4.2 SOURCE CODE

```
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
#include <LiquidCrystal.h>
#include <Keypad.h>
#define Password_Lenght 7 // Give enough room for six chars + NULL char
#define Number "\"+918867949983\""
```

```
const byte ROWS = 4; //four rows
const byte COLS = 3; //four columns//define the cymbols on the buttons of the keypads
char Data[Password_Lenght]; // 6 is the number of chars it can hold + the null char = 7
char Master[Password_Lenght] = "123456";
byte data_count = 0, master_count = 0;
bool Pass_is_good;
char customKey;
int getFingerprintIDez();
SoftwareSerial mySerial(2, 3);
int SW = 11;
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
LiquidCrystal lcd(13, 12, 7, 6, 5, 4);
String inputString = "";
char inByte,inchar;
char hexaKeys[ROWS][COLS] = {
 {'1','2','3'},
 {'4','5','6'},
 {'7','8','9'},
 {'*','0','#'}
};
byte rowPins[ROWS] = { 8, 9, 10,A3}; //connect to the row pinouts of the keypad
byte colPins[COLS] = {A0,A1,A2}; //connect to the column pinouts of the keypad
Keypad customKeypad = Keypad( makeKeymap(hexaKeys), rowPins, colPins, ROWS,
COLS);
void setup()
{Serial.begin(9600);
  Serial.println("AT");
 delay(500);
 Serial.println("ATE0");
 delay(500);
 Serial.println("AT+CMGF=1");
 delay(500);
 Serial.println("fingertest");
```

```
finger.begin(9600);
inputString.reserve(200);
lcd.begin(16, 2);
lcd.print(" fingerprint sensor");
delay(200);
if (finger.verifyPassword()) {
 Serial.println("Found fingerprint sensor!");
 lcd.setCursor(0, 1);
 lcd.write("Fingerprint");
} else {  Serial.println("Did not find fingerprint sensor :(");
 lcd.setCursor(0, 1);
 lcd.write("NO Fingerprint");
  while (1);
}
Serial.println("Waiting for valid finger...");
lcd.setCursor(0, 1);
lcd.write("Waiting Fingerprint");
 pinMode(SW, INPUT);
  pinMode(A5,OUTPUT);
   pinMode(A4, OUTPUT);
}

void loop()                    // run over and over again
{
  int   SWSTATE = digitalRead(SW);
  lcd.clear();
        if (SWSTATE == 0){ lcd.setCursor(3, 0);
   lcd.print("KEYPAD STATE");
        delay(500);
char customKey = customKeypad.getKey();
 if (customKey){
  lcd.setCursor(0, data_count);
   lcd.write(customKey);
```

```
Serial.println(customKey);
  Data[data_count] = customKey; // store char into data array
 data_count++; // increment data array by 1 to store new char, also keep track of the number
of chars entered
 }
 if(data_count == Password_Lenght-1) // if the array index is equal to the number of expected
chars, compare data to master
 { if(!strcmp(Data, Master)) // equal to (strcmp(Data, Master) == 0)
  { Serial.println("AT+CMGS="Number);
    delay(500);
    Serial.println("Kindly Reply With ACCESS ");
        Serial.write(0x1A);
         delay(500);
     Serial.println("AT+CNMI=2,2,0,0,0");
     delay(500);
    while(1)
    { lcd.setCursor(0, 1);
 lcd.write("WAITING for SMS");
if(Serial.available() >0)
 { inchar=Serial.read();
 if (inchar =='#')
  { lcd.clear();
    lcd.setCursor(0, 1);
 lcd.write("ACCESS Granted");
  digitalWrite(A4, HIGH);
  digitalWrite(A5, LOW);
 delay(5000);
    }
    else
    { lcd.clear();
    lcd.setCursor(0, 1);
 lcd.write(" NO ACCESS ");
  digitalWrite(A4, LOW);
```

```
  digitalWrite(A5, LOW);
  delay(10000);
        }
      }
    }
}
else
{ lcd.clear();
    lcd.setCursor(0, 1);
 lcd.write("Wrong Key");
 delay(10000);
    }
  }
}
else
 {   int i = getFingerprintIDez();
 if ((i == 0) || (i == 1)) // Two users only
 {  lcd.setCursor(0, 1);
 lcd.write("ACCESS GRANTED");
 Serial.println("ACCESS GRANTED");
 delay(500);
  digitalWrite(A4, HIGH);
  digitalWrite(A5, LOW);
 delay(5000);
 }
 delay(50);          //don't ned to run this at full speed.
    }
}
uint8_t getFingerprintID() {
 uint8_t p = finger.getImage();
 switch (p) {
  case 1: FINGERPRINT_OK:
    Serial.println("Image taken");
```

```
  break;
 case 2: FINGERPRINT_NOFINGER:
  Serial.println("No finger detected");
  return p;
 case 3: FINGERPRINT_PACKETRECIEVEERR:
  Serial.println("Communication error");
  return p;
 case 4: FINGERPRINT_IMAGEFAIL:
  Serial.println("Imaging error");
  return p;
 default:
  Serial.println("Unknown error");
  return p;
}
p = finger.image2Tz();
switch (p) {
 case1: FINGERPRINT_OK:
  Serial.println("Image converted");
  break;
 case 2: FINGERPRINT_IMAGEMESS:
  Serial.println("Image too messy");
  return p;
 case 3: FINGERPRINT_PACKETRECIEVEERR:
  Serial.println("Communication error");
  return p;
 case 4: FINGERPRINT_FEATUREFAIL:
  Serial.println("Could not find fingerprint features");
  return p;
 case 5: FINGERPRINT_INVALIDIMAGE:
  Serial.println("Could not find fingerprint features");
  return p;
 default: Serial.println("Unknown error");
  return p;
```

```
 }
 p = finger.fingerFastSearch();
 if (p == FINGERPRINT_OK) {
  Serial.println("Found a print match!");
 } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
  Serial.println("Communication error");
  return p;
 } else if (p == FINGERPRINT_NOTFOUND) {
  Serial.println("Did not find a match");
  return p;
 } else {
  Serial.println("Unknown error");
  return p;
 }
}
int getFingerprintIDez() {
 uint8_t p = finger.getImage();
 if (p != FINGERPRINT_OK)  return -1;
 p = finger.image2Tz();
 if (p != FINGERPRINT_OK)  return -1;
p = finger.fingerFastSearch();
 if (p != FINGERPRINT_OK)  //return -1;
 { lcd.setCursor(0, 0);
 lcd.write("ACCESS Denied");
 Serial.println("ACCESS Denied: FINGER Print not MATCHED");
  digitalWrite(A4, LOW);
  digitalWrite(A5, LOW);
 delay(1000);
 } if (finger.confidence < 80 )  //return -1;
 {return -1;
  }
  return finger.fingerID;
}
```

CHAPTER 5

SNAPSHOTS

Figure 34: Message on LCD for Access granted

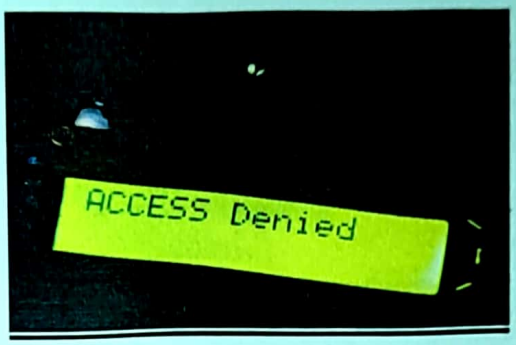

Figure 35: Message on LCD for Access denied

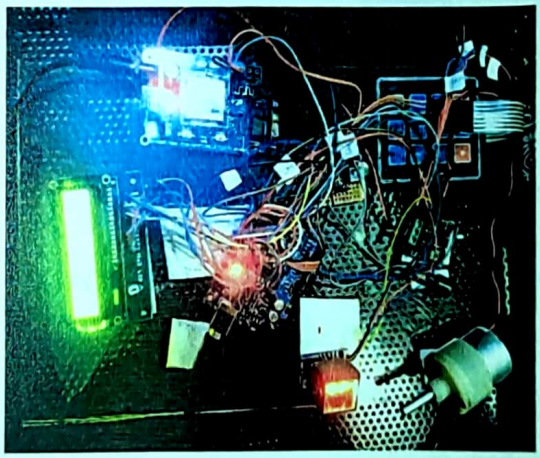

Figure 36: Snapshot of the whole working project with network

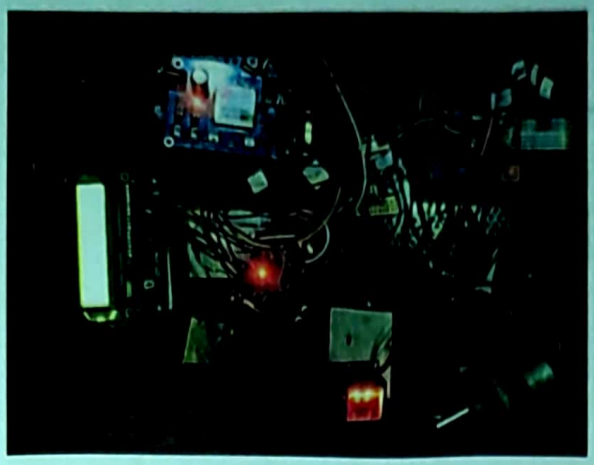

Figure 37: Snapshot of the whole project

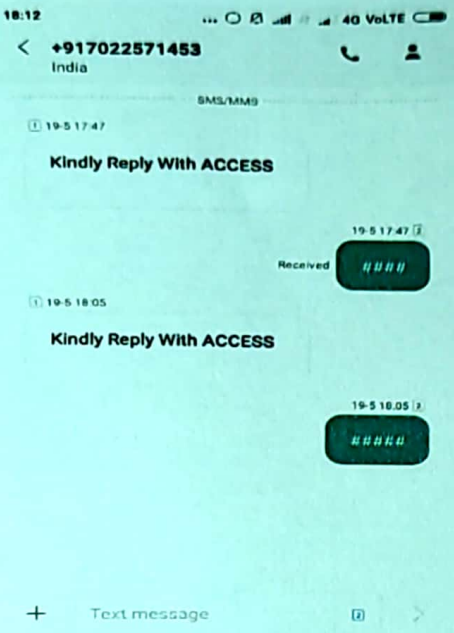

Figure 38: Snap of the message received in the phone through GSM

CHAPTER 6

TESTING

6.1 TESTING

Software testing is a critical element of the ultimate review of specification design and coding. Testing of software leads to the uncovering of errors in the software functional and performance requirements are met. Testing also provides a good indication of software reliability and software quality as a whole. The result of different phases of testing are evaluated and then compared with the expected results. If the errors are uncovered they are debugged and corrected. A strategy approach to software testing has the generic characteristics:

- Different testing techniques are appropriate at different points of time.
- Testing and debugging are different activities, but debugging must be accommodated in the testing strategy.

Following three approaches of debugging were used:

- Debugging by Induction
- Debugging by Deduction
- Backtracking

6.2 TEST PLANS

In this test plan all major activities are described below:

- Unit testing.
- Integration testing.
- Validation testing.
- System testing.

Unit testing

-Test Name: Test of Biometric module.

-Expected Output: "detection" of fingerprint

-Actual Output: "detection" of fingerprint

Integration testing

-Test Name: Compilation of the whole circuit setup

-Expected Output: Access granting or denying the access.

-Actual Output: Access granting or denying the access.

System testing

-Test Name: System testing on various components of the hardware and the software used.

-Expected output: Software recognises the fingerprint and access granting.

-Actual output: Software recognises the fingerprint and access granting.

CHAPTER 7

CONCLUSION

As fingerprint scanners become more common on consumer devices, biometric authentication will continue to develop as a popular technique for identifying users to cloud-based applications. As biometric authentication becomes more common, maintaining the privacy of a user's authenticating template will be critical since revocation is essentially impossible.

FUTURE ENHANCEMENT

We can develop this project to implement in all the other possible ways so that more high end security can be provided that can avoid thieves and frauds. Also we can setup all possible interfaces with other components required in future to Arduino development board and implement a better project design.

REFERENCES

[1] Y. Aumann and Y. Lindell. Security against covert adversaries: Efficient protocols for realistic adversaries. Journal of Cryptology, 18(3):554–343, 2010.

[2] Bank of America. Online Banking and Mobile Banking Features. https://www.bankofamerica.com/online-banking/ mobile-and-online-banking-features/, 2016.

[3] M. Blanton and P. Gasti. Secure and efficient protocols for iris and fingerprint identification. In Proceedings of the European Conference on Research in Computer Security (ESORICS), 2011.

[4] C. Blundo, E. De Cristofaro, and P. Gasti. EsPRESSO: Efficient privacy-preserving evaluation of sample set similarity. Journal of Computer Security, 22(3):355–381, 2014.

[5] J. Bringer, H. Chabanne, M. Favre, A. Patey, T. Schneider, and M. Zohner. GSHADE: Faster privacy-preserving distance computation and biometric identification. In Proceedings of the ACM workshop on Information hiding and multimedia security, 2014.

[6] J. Bringer, H. Chabanne, and A. Patey. SHADE: Secure hamming distance computation from oblivious transfer. In Financial Cryptography and Data Security (FC), 2013.