بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

Sudan University of Science & Technology

College of Graduate Studies

Design of Car’s Security System Using Fingerprint and Arduino GSM Module

تصميم نظام حماية للسيارات بإستخدام البصمه و نظام الإتصالات المتنقلة

A thesis Submitted for Partial Fulfilment for the Requirement of M.Sc. Degree in Mechatronics Engineering

Prepared by:

Elham Yahia Hassan Mutwaly

Supervised by:

Dr.Alaa Eldein Awooda

July 2018

الايـة

قال تعالى:

﴿ سَنُرِيهِمْ آيَاتِنَا فِي الْآفَاقِ وَفِي أَنفُسِهِمْ حَتَّى يَتَبَيَّنَ لَهُمْ أَنَّهُ الْحَقُّ أَوَلَمْ يَكْفِ بِرَبِّكَ
أَنَّهُ عَلَى كُلِّ شَيْءٍ شَهِيدٌ ﴾

(فصلت:53)

DEDICATION

To who taught me to give without waiting, to who I carry their names proudly. I ask God to extend his age to see the fruits harvest has come after a long and tomorrow and forever...

My Father

To the angel in our life , to the meaning of love and the meaning of compassion and dedication , my smile which is the mystery of my existence and the secret of my success ,To the heart as pure whiteness…

My Mother Granule

To these who have shown me what is the most beautiful of life, to those who remind me of hope when I need it….

My Friend

ACKNOWLEDGEMENT

Always the lines of thanks and praise are extremely difficult when drafting…

Perhaps because they always make us feel satisfied all palaces and not give him the right of these lines …….

Today, I stand the same difficulty

I am trying to formulate words of thanks and appreciation to my teacher and supervisor:

Dr: Alaa Eldin Awouda

Abstract

The main purpose of this project is to design and implement high security system of car. 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, car… 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, car and even money. The fingerprint and password based security system presented here is an access control system that allows only authorized persons to access a car. The implemented of security system based on fingerprint, password and GSM technology which can activate, authenticate, and validate the user and unlock the car 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 sensed by sensor and is validated for authentication. If the fingerprint matches, the door will be opened automatically and GSM will send SMS contain the password to turn the car's engine which will change randomly.

This high security system based on fingerprint, password and GSM technology can be organized in the money transfer cars or any transfer which needs high security information.

المستخلص

يهدف هذا البحث لتصميم وتنفيذ نظام حمايه عاليه لسياره باستخدام البصمه وتقنيه كلمه السر عبر النظام العالمي للاتصالات المتنقله.نظم الحمايه اصبحت تلعب دور اساسي في حياتنا في عدة نواحي حمايه المكاتب،المعاهد، المكاتب ، والعربات ... الخ. ربما اهم تطبيق لتعريف الشخص بدقه يحمي و يحدد الدخول مما يحمي من الهجمات العدائيه لحمايه بياناتنا السريه ومنع اي شخص غير موثوق للدخول و الاطلاع عليها. هذه الايام في اي زمن نحتاج حمايه للحفاظ علي المعلومات القيمه، السيارات و الاموال.

ونظام البصمه وكلمه السر المستخدمه في هذا البحث هو نظام يسمح بدخول الموثوق لهم فقط للسياره و تشغيلها .البصمه هي احد الاشكال التي يتم استخداما للتعريف بالاشخاص فرديا والتعرف عليهم. البصمه تحسس عن طريق حساس وتقوم بالتحقق من الموثوقيه، اذا كانت البصمه مطابقه سيتم فتح باب السياره ويتم ارسال رساله نصيه تحوي كلمه المرورالتي تتغير عشوائيا عبر النظام العالمي للاتصالات المتنقله وعند ادخاله يتم تشغيل السياره .

نظام الحمايه المستخدم في هذا البحث يمكن استخدامه وتطبيقه في سيارات نقل الاموال او نقل المعلومات الفائقه السريه

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
GSM	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
SMS	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 One

Introduction

Chapter One

Introduction

1.1 General Concept

This chapter will focus on the brief introduction of the project to be carried 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 details about 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 peoples into the restricted area. Conventional security systems used either knowledge based methods(passwords or PIN), and token-based methods(passport, driver license, ID card) 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 you choose. 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 types of fingerprint features. This powerful device uses the latest in fingerprint ID scan 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 failurefor 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 GSM module in the car which need high security using in money transform or high security information to fulfill the security gabs resulted from using just individual security system taking into account that system will designed to be efficient, more secure, and with less cost.

1.4 Objective

The main objective of this project is toincrease the security feature of the car by integrating fingerprint and GSM module with the Arduino microcontroller.

To achieve this objective:

1/ Control system using Arduino GSM 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 this module along with GSM 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 GSM with Arduino.

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

1.5 Thesis lay out

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

Chapter 1: Introduction explains problem andproposed solution. Chapter 2: Literature reviewand cover different system component.

Chapter 3: System design and explain how it work.

Chapter 4: Result and discussion.

Chapter 5: Conclusion recommendation for future research.

Chapter Two

Literature Review

Chapter Two

Literature Review

2.1 Introduction

This chapter is about fingerprint, Arduino GSM 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.

2.2 Previous works

Home security system is needed for convenienceand safety. This system invented to keep home safe from intruder. In this work, we present the design and implementation of a GSM based wireless home security system, which take a very less power. The system is a wireless home network which contains a GSM modem and magnet with relay which are door security nodes. The system can response rapidly as intruder detect and GSM 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 tells about your home update or predefined message which is embedded in microcontroller. Suspected activities are conveyed to remote user through SMS or Call using GSM technology. [1]

focused on the four step verification project. In this proposed work, RFID reader 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 password to the authenticated 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 will be remain in locked position.[2]

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 can be 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.[3]

Fingerprint matching has been successfully used by law enforcement for more than a century. Thetechnology is now finding lot of other applications such as identity management and access control. In this context, an automated fingerprint recognition system and identification of key 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 the existing problems with a proper Embedded System Design.[4]

Security is the major issue faced by everyone when we are away from our households. In the present scenario satisfactorysolution for the above problem 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 has the ability to 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 GSM module. Unauthorized access is ensured by setting a password by the user. It is entered through the 4×4 matrix keypad. If the entered password matches, door will be opened automatically otherwise a message showing incorrect password will be displayed on LCD display and a SMS will be sent to the owner that the security was tried to be breached. This hardware project achieves security with commonly available components and also consumes less power.[5]

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 aperson for controlling the device manually. Generally GSM 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 paper proposes an alternate approach for wireless control of a device by incorporating a fingerprint identification module along with GPS and GSM modules. The fingerprint module increases the authenticity of the device and enables multiple users to control the device. These modules are integrated to a simple Arduino microcontroller to demonstrate various functionalities .The proposed approach finds its application in various fields like automobiles, agriculture.[6]

2.3 Fingerprint Sensor

Figure (2,1) 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 improve the tactile sensing of thesurface 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 also in passports (a matter of national high importance) of person.[4]

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.[7]

2.3.1 Optical Fingerprint Sensor

The heart of an optical scanner is a charge coupled device (CCD), the same light sensor system used in digitalcamerasand camcorders. A CCD is simply an array of light-sensitive diodes called photo sites, which generate an electrical signal in response to lightphotons. 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 scanned scene (a finger, for example). Typically, an analogytodigitalconverter 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 light-emittingdiodes, to illuminate the ridges of the finger. The CCD system actually 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 more or less 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 of very 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.[8]

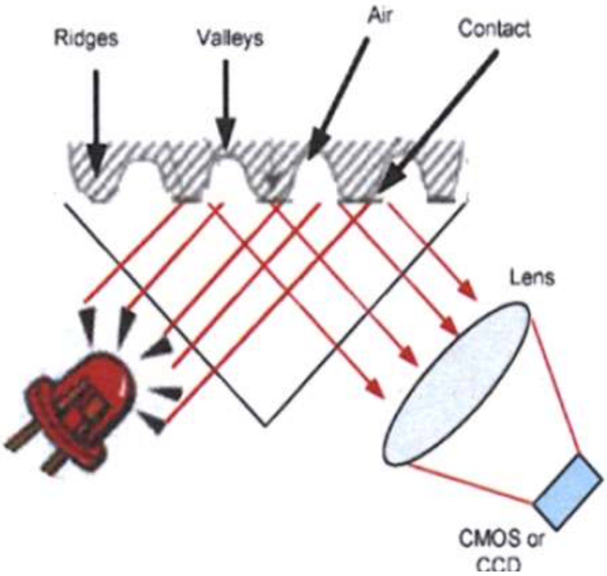


Figure (2.2) optical fingerprint

2.3.2 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. LeEco became the first company to introduce this in Smartphone. [8]

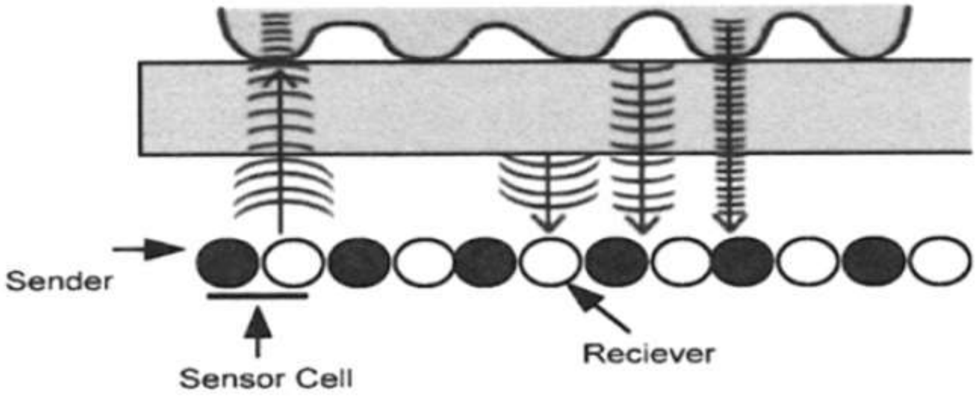


Figure (2,3) Ultrasonic fingerprint sensor

2.3.3 Capacitance Fingerprint Sensor

Like optical scanners, capacitive fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead of sensing the print 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 anumber of transistors, resistors and capacitors

Like any amplifier, an inverting amplifier alters one current based on fluctuations in another current. Specifically, the inverting amplifier alters a 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 twoconductor plates.

As you may have recognized, the two conductor plates form a basic capacitor, an electrical component that can store up charge The surface of the finger acts as a third capacitor plate, separated by the insulating layers in 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 total capacitance (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 it is 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, similar to 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 makes up the visual impression of a fingerprint .This makes the system harder to trick. Additionally, since they use a semiconductor chip rather than a CCD unit, capacitive scanners tend to be more compact than optical device.[8]

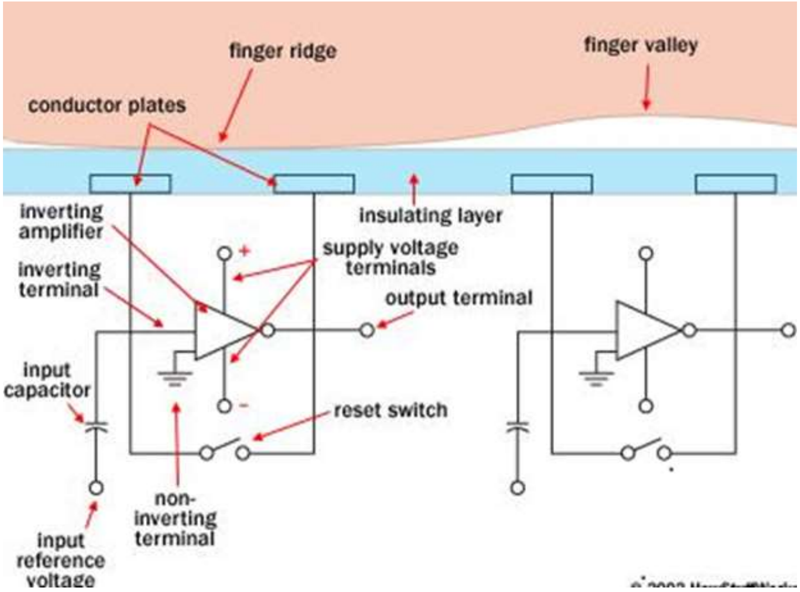


Figure (2.4) Capacitance Fingerprint Sensor

2.3.4 Identification technologies

A fingerprint-based personal authentication system operates in two distinct modes: enrollment and authentication (identification), as is shown in figure (2,5).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 the identity of the subject or decide the person is not enrolled in the database.[9]

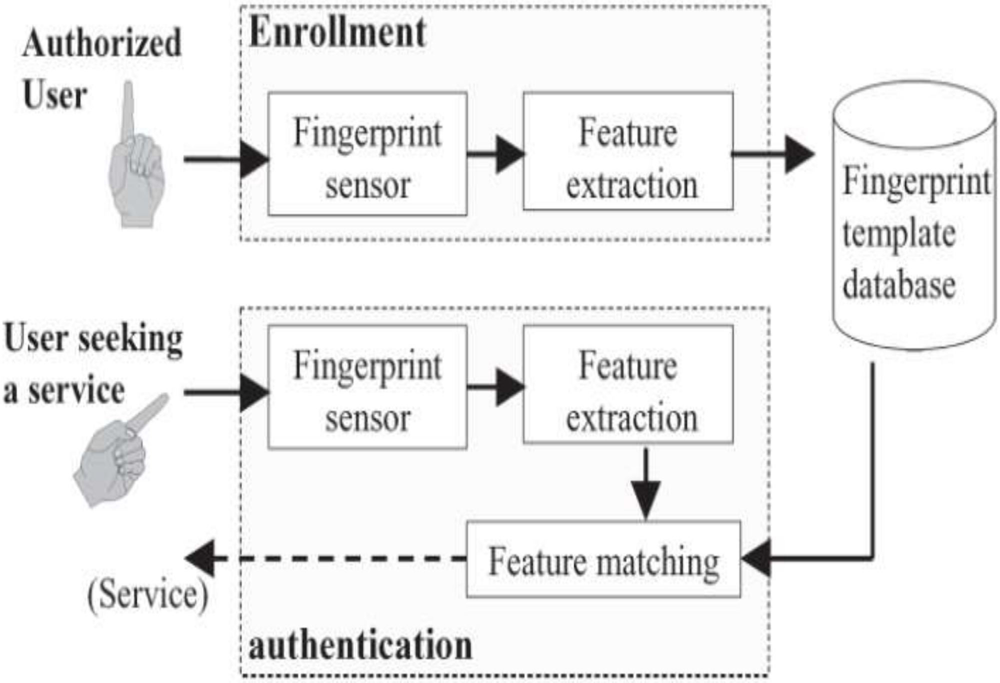


Figure (2,5)Identification technologies

2.4 Arduino Microcontroller

Arduino is open Source electronic prototyping platform based on flexible easy touse 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 hardware board 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.[10]

2.4.1 Arduino hardware

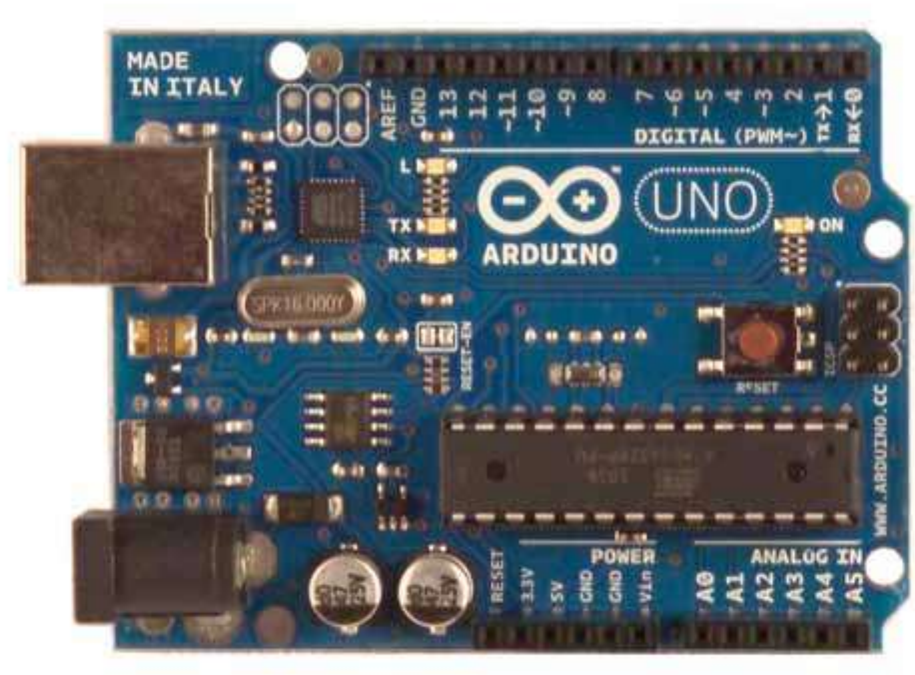


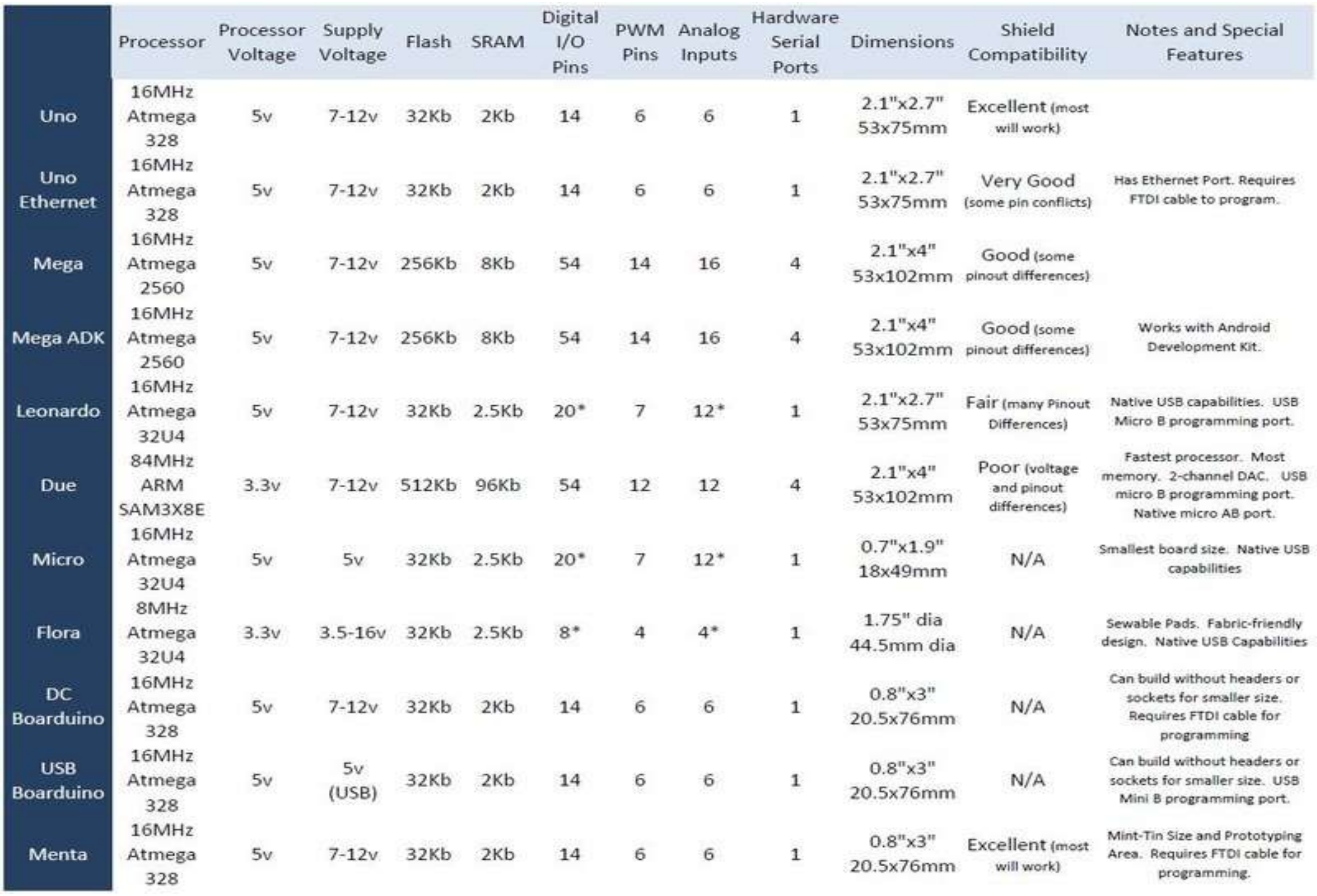
Figure (2.6) Arduino Hardware

- 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 the time of this writing, a number of Arduino boards exist:-

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

Figure (2.7) Arduino Family



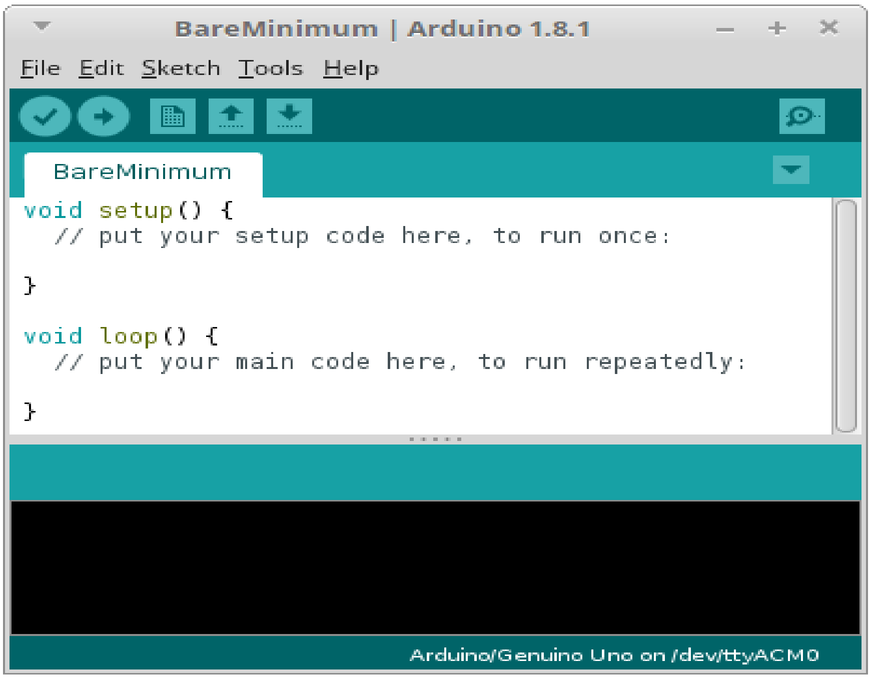
	Processor	Processor Voltage	Supply Voltage	Flash	SRAM	Digital I/O Pins	PWM Pins	Analog Inputs	Hardware Serial Ports	Dimensions	Shield Compatibility	Notes and Special Features
Uno	16MHz Atmega 328	5v	7-12v	32Kb	2Kb	14	6	6	1	2.1"x2.7" 53x75mm	Excellent (most will work)	
Uno Ethernet	16MHz Atmega 328	5v	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.

Figure (2.8) Compare between the different type of Arduino

2.4.2 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 hardware devices come with prewritten software line for sample code, libraries (of functions).

Libraries are a collection of code that makes it easy for you to connect to a 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.[11]



```
void setup() {
  // put your setup code here, to run once:

}

void loop() {
  // put your main code here, to run repeatedly:

}
```

Arduino/Genuino Uno on /dev/ttyACM0

Figure (2.9) Arduino IDE

2.4.3 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 a 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 range is 7 to 12 volts.The power pins are as follows:

1/ VIN. The input voltage to the Arduino board when it's using an external power source (asopposed to 5 volts from the USB connection or 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 suppliedwith 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 don't 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 digital Read()functions.They operate at 5 volts. Each pin can provide or receive amaximum of 40 mA and has an internal pull-up resistor (disconnected by default) of 20-50 Kohms. 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 pinsare connected to the corresponding pins of the ATmega8U2 USB-to-TTL Serial chip.

6/ External Interrupts: 2 and 3. These pins can be configured to trigger an interrupt on a lowvalue, 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 theanalogWrite() function

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

9/ LED: 13. There is a built-in LED connected to digital pin 13. When the pin is HIGH value, theLED is on, when the pin is LOW, it's 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 analogReference() 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 withanalogReference().

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. [12]

2.5 Global System for Mobile communications GSM

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

A GSM modem is a special type of modem that accepts a SIM card and operates over a subscription to a mobile operator just like as a mobile phone. GSM modem is a wireless modem which sends and receives data through radio waves .A GSM modem requires a SIM card from a wireless carrier in order to operate Just like as a GSM mobile phone. GSM modem support standard AT commands as well as extended set of AT commands. With the standard AT commands and extended AT commands, you can do things like:

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

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

Terrestrial GSM networks now cover more than 90% of the world's population. GSM satellite roaming has also extended service access to areas where terrestrial coverage is not available.[13]

2.5.1 GSM Features

· Quad Band GSM/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 GSM L Type Antenna

· Built in SIM (Subscriber Identity Module) Card holder

· Built in Network Status LED

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

2.5.2 Hardware Description of GSM modul

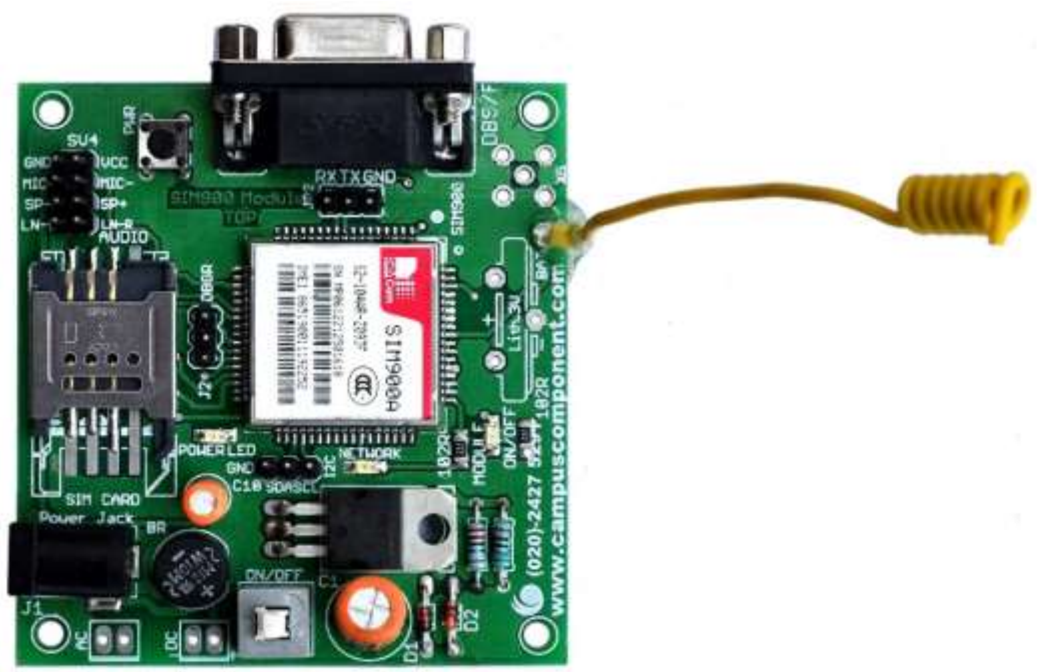


Figure (2.10) GSM module

1/SIM Com SIM900A GSM Module

This is actual SIM900 GSM module which is manufactured by SIM Com. Designed for global market, SIM900 is a quad-band GSM/GPRS engine that works on frequencies GSM 850MHz; EGSM 900MHz, DCS 1800MHz and PCS 1900MHz. SIM900 features GPRS multislot 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 works 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 actually 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 provide maximum 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 Voltage Regulator which provides an output voltage adjustable over a1.2V
to 37V.

5/**Power On/Off and GSM On Switch**

Power On/Off switch is type of push-on push-offDPDTswitch which is used for only make power supply on/off provided through AC/DC Socket indicated by 'PowerLED'. GSM On Switch is type of Push on DPST tactile switch which is used for only to make GSM module 'On' Indicated by 'Module On/Off LED' while initiating with Network indicated by 'Network Indication LED'.

6/SIM (Subscriber Identity Module) Card Slot

This on board SIM card slot provides User functionality of insert a SIM (GSM only) card of any service provider. Process of inserting and locking SIM card into SIM card slot is given in this manual. While inserting in and removing out SIM card from SIM card 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 three LEDs represents Power On/Off Status, Network Status and Module On/Off Status respectively. Power LED will keep on until the power supply is enable to this board by using push-on push-offswitch. Network Status LED will show whether inserted SIM card successfully connected to service provider's Network or not, in short signal strength. Module On/Off indicator LED will show status of GSM module's power on/off.

8/ RXD, TXD and GND pins (JP2)

These pins are used to connect devices which need to be connected to GSM 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 device's 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 GSM 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.

2.6 Liquid Crystal Display (LCD)

A 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 the 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.

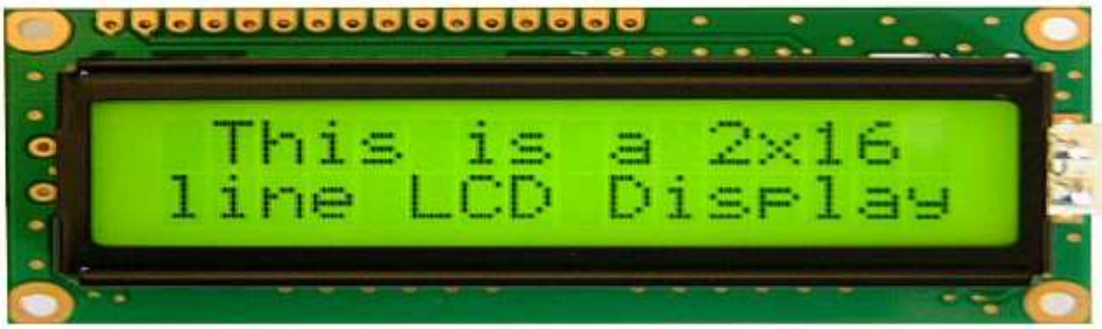


Figure (2.11) Liquid Crystal Display

2.6.1 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, the cell 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.[15]

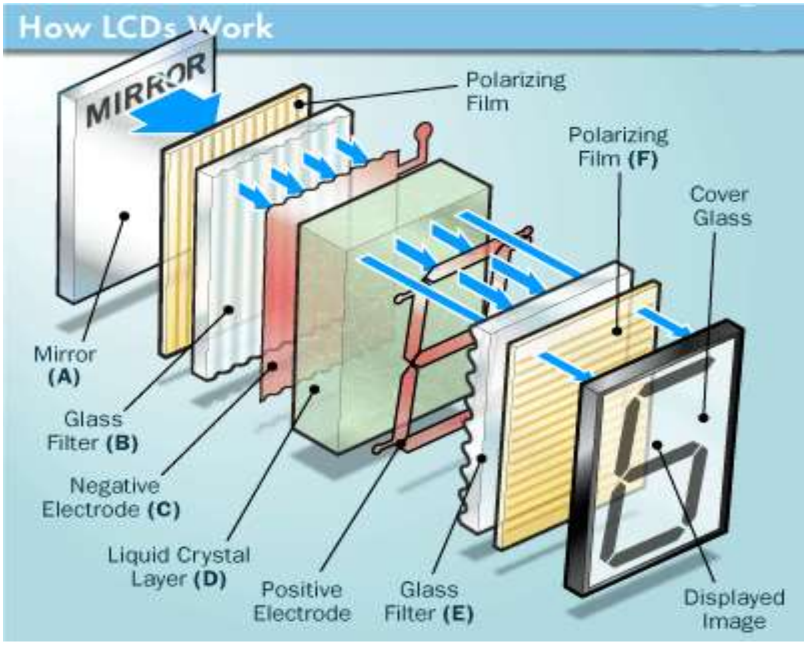


Figure (2.12) structure of an LCD

Chapter Three

System Design and Operation Design

Chapter Three

System Design and Operation Design

3.1 Introduction

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

3.2 Block Diagram of the System

The block diagram consists of fingerprint sensor, LCD, arduino board and GSM. The fingerprint sensor and GSM 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 car’s door will open and the user will get a random number as a password in his mobile through GSM modem which is connected with the arduino.by applying that random number inkeypad then it will show in LCD if it correct then the car’s engine will work.

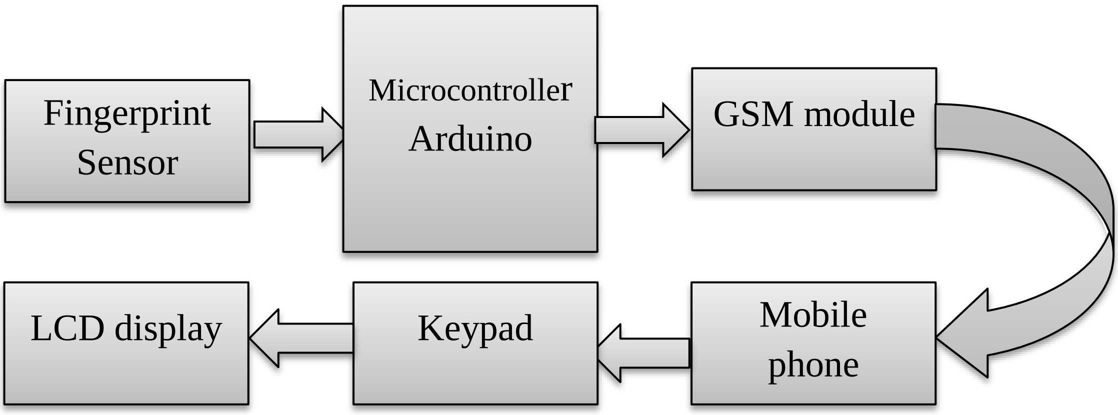


Figure (3.1) Block diagram of the system

3.3 Flow chartof the System

Figure (3.2) shows the flow chart of whole system, which also shows process of how the car’s door open and how get the password to work the engine.

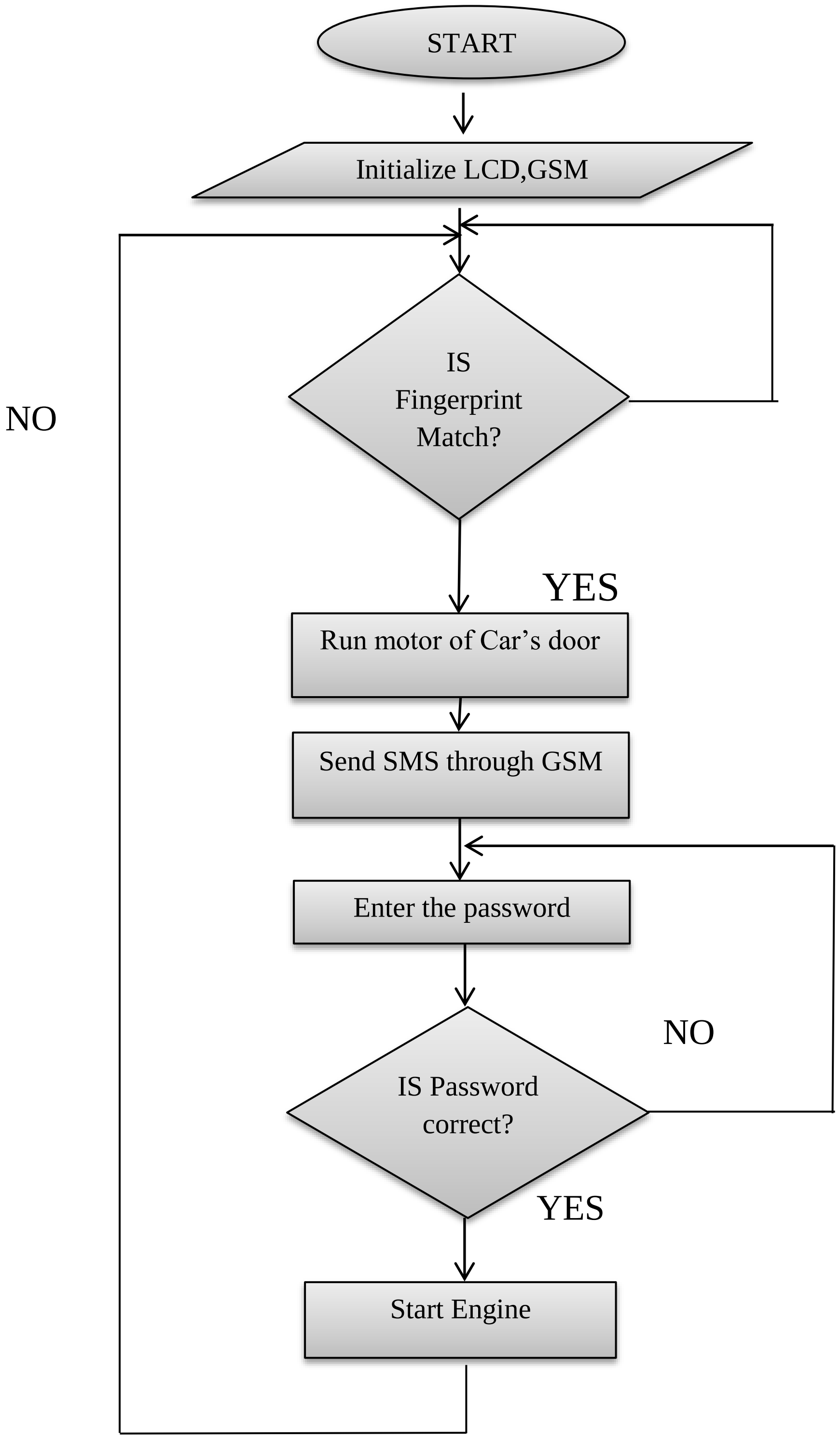


Figure (3.2) The flow chart of System

3.4 Description of the System

The system has being installed using the following components:-

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

3.5 Signal movement

The system is designed as follow:-

1\ The GSM module is connected to the Arduino from the pin RXD in the GSM module with the PD1\TXD and the other pin TXD in the GSM is connected to the virtual terminal in pin RXD and other 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] with pins [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 car 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 car and [OUT1 , OUT2] are connected to the car engine.

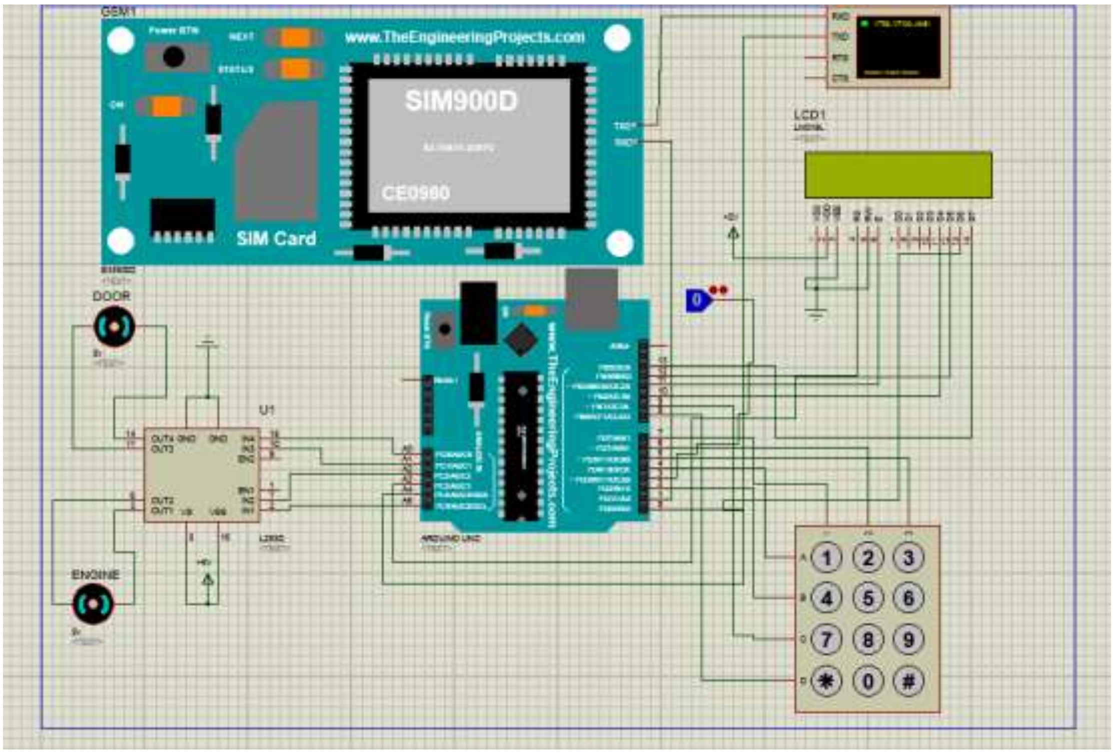


Figure (3.3)circuit diagram of the system

Chapter Four

Result and Discussion

Chapter Four

Result and Discussion

4.1 Introduction

Many users have being configured using the letters (A,B,C) when any of those letters entered which are representing finger prints that 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 car will be open. The second operation The GSM module will send message to the saved number which is corresponding to the fingerprint containing the random password 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 appear on LCD screen the word (success) else then it will be appear the word (wrong).

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

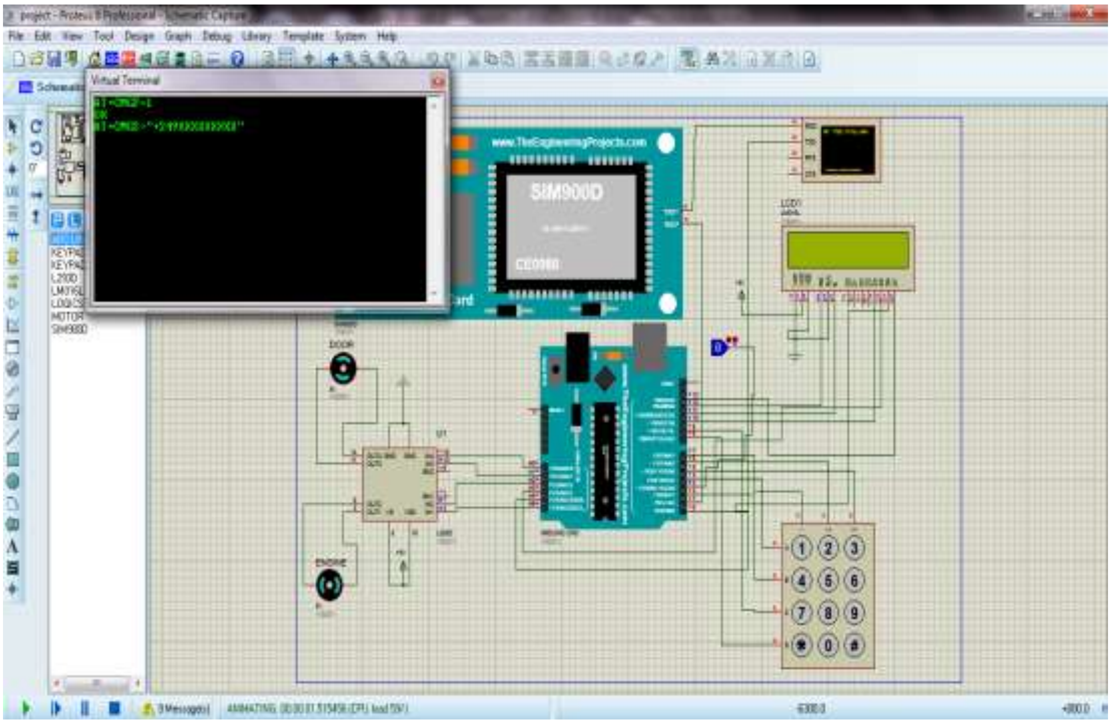
4.2 System Implemention

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

4.2.1 Case (1)

- **Step 1**

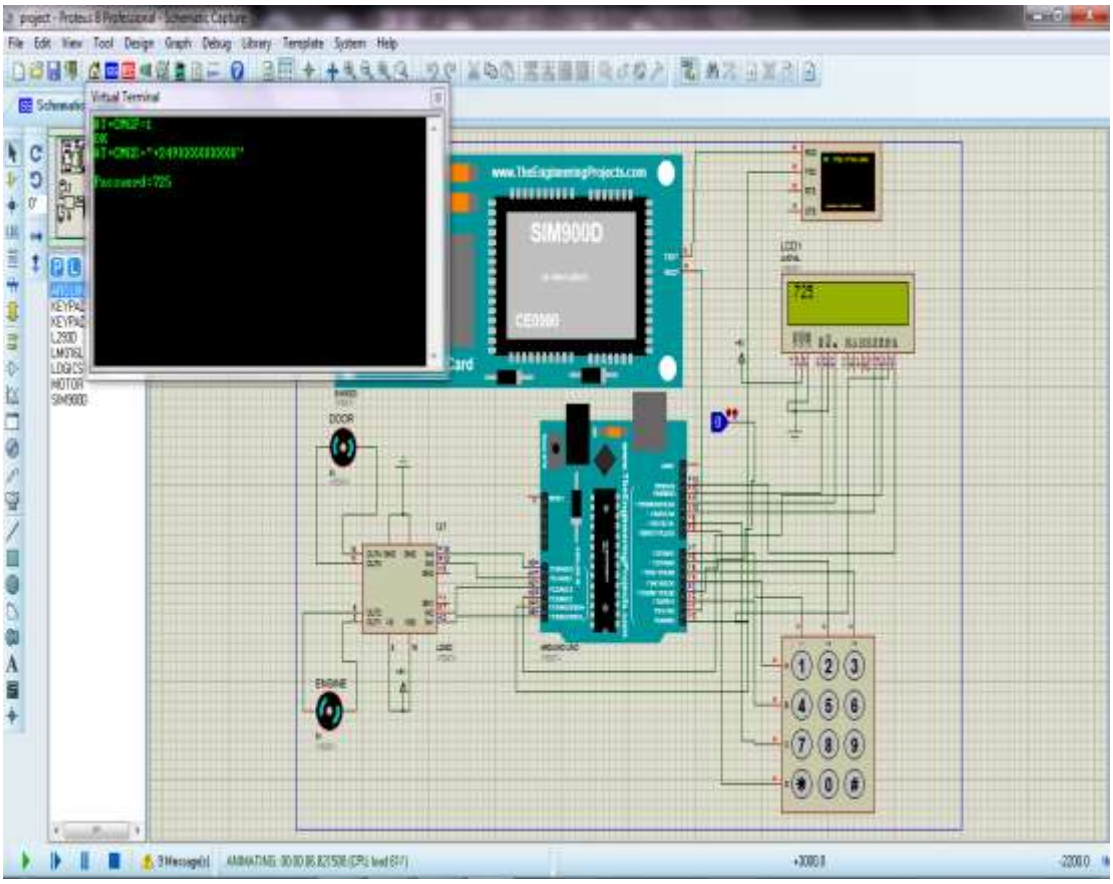
When the simulation is run and the first user (A) has entered to the screen of the virtual terminal. As the result aphone number will appear on the screen and a massage will be sent to this number which contain the password (725) simultaneously the motor will run for 10 seconds and the door will be open as shown in figure (4,1) and Fig (4,2).



project - Proteus 8 Professional - Schematic Capture
File Edit View Tool Design Graph Debug Library Template System Help
Virtual Terminal
www.TheEngineeringProjects.com
SIM900D
DOOR
ENGINE
LCD1
1 2 3
4 5 6
7 8 9
* 0 #

```
AT+CMGF=1
OK
AT+CMGS="+249XXXXXXXXX"
```

Figure (4,1) Apply for the First user



project - Proteus 8 Professional - Schematic Capture
File Edit View Tool Design Graph Debug Library Template System Help
Virtual Terminal
www.TheEngineeringProjects.com
SIM900D
DOOR
ENGINE
KEYPAD
L298D
LM016L
MOTOR
SIM900D
725
3 Message(s)

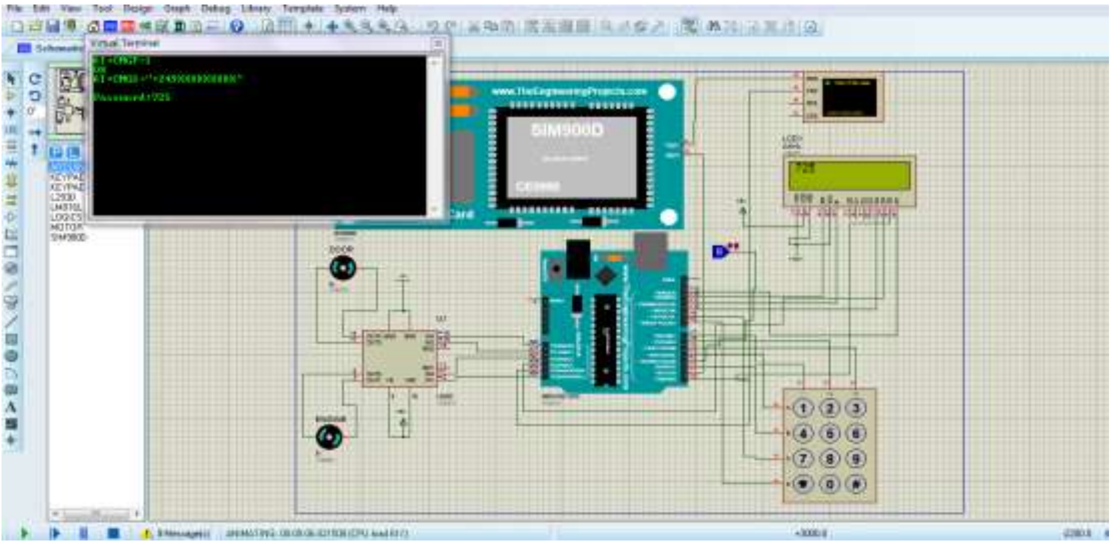
```
AT+CMGF=1
OK
AT+CMGS="+249XXXXXXXXXX"

Password:725
```

Figure (4,2) password massage

- **Step 2**

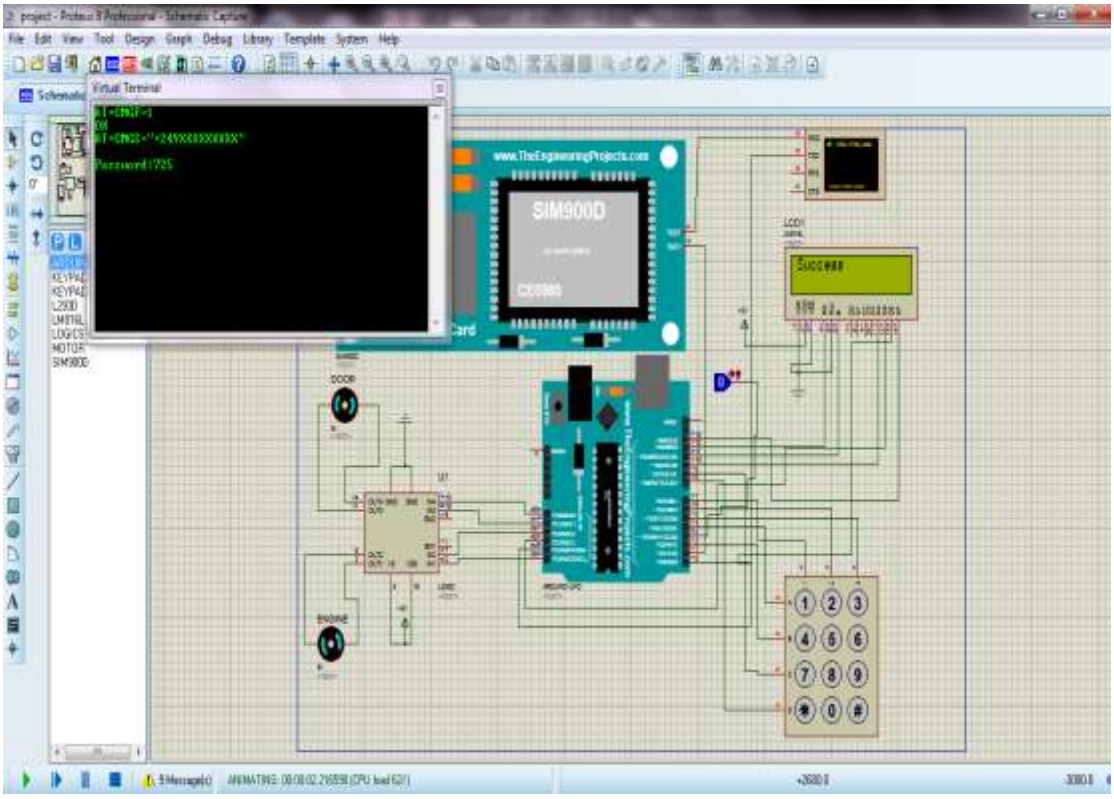
When the password is entered to the keypad it will appear on the LCD screen Fig (4,3) after that the (*) button will be pressed to check if the password is right or wrong if it is right then the word Success will appear on the LCD screen Fig (4,4) and the car engine will work and when the brakes are pressed the button reset will be pressed and the car will stop Fig (4,5)



```
AT+CMGF=1
OK
AT+CMGS="+249XXXXXXXXX"

Password:725
```

Figure (4,3) Applied password

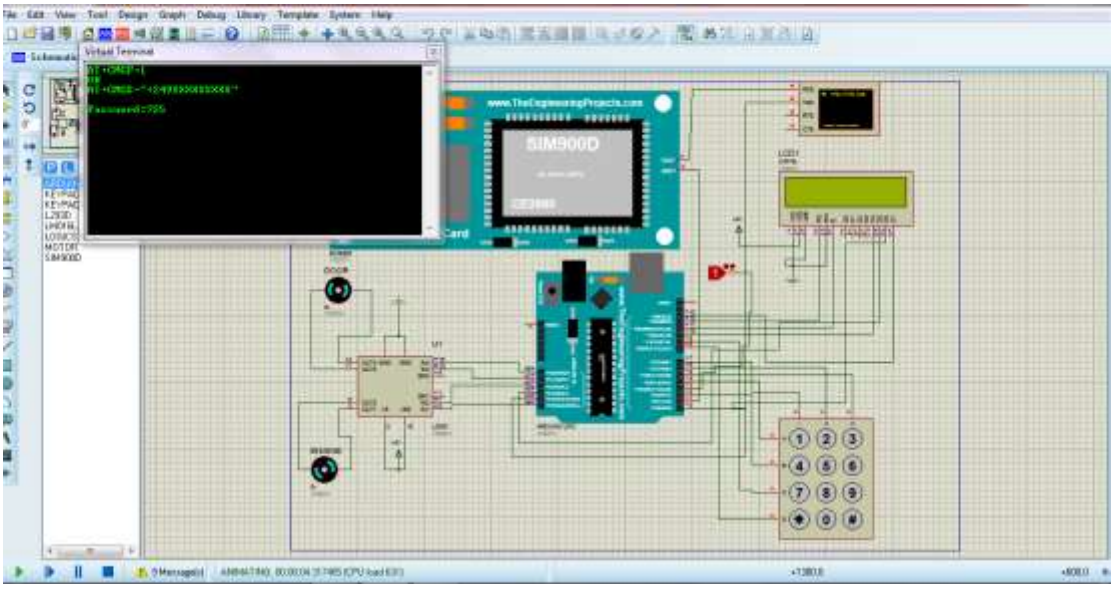


```
AT+CMGF=1
OK
AT+CMGS="+249XXXXXXXXX"

Password:725
```

project - Proteus 8 Professional - Schematic Capture
File Edit View Tool Design Graph Debug Library Template System Help
Virtual Terminal
www.TheEngineeringProjects.com
SIM900D
Success
DOOR
ENGINE
1 2 3
4 5 6
7 8 9
✱ 0 #

Figure (4,4) check the password



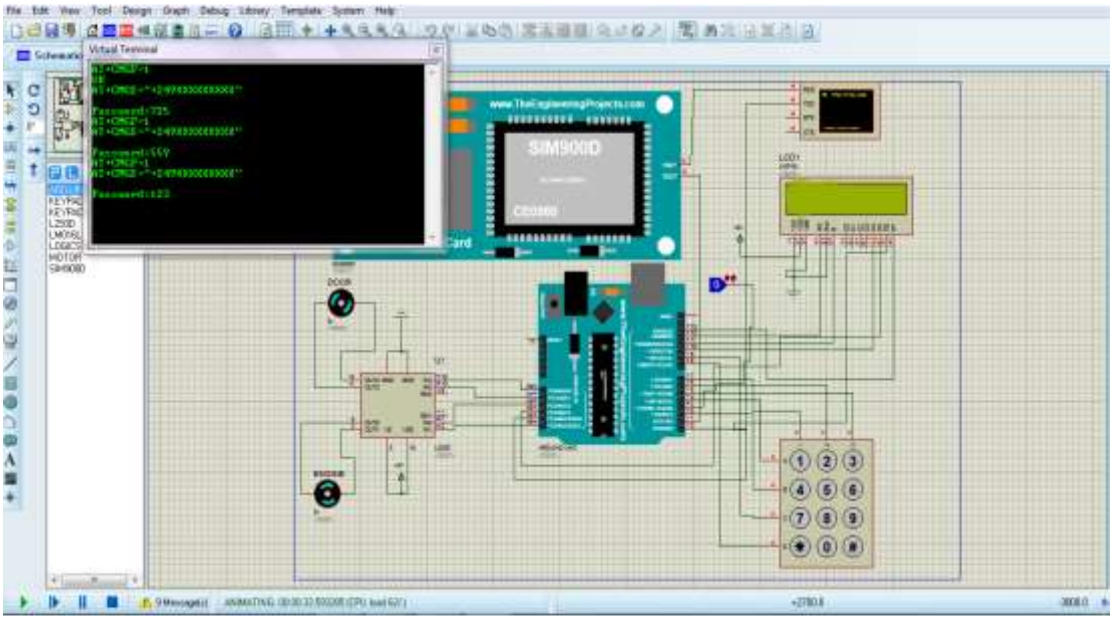
```
AT+CMGF=1
OK
AT+CMGS ="+249XXXXXXXXX"

Password:735
```

Figure (4,5) 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 password they will be generated using the function (RAND) Figure (4,6)



```
AT+CMGF=1
OK
AT+CMGS ="+249XXXXXXXXX"

Password:735
AT+CMGF=1
AT+CMGS ="+249XXXXXXXXX"

Password:559
AT+CMGF=1
AT+CMGS ="+249XXXXXXXXX"

Password:123
```

Figure (4,6) Generated different password

4.2.2 Case 2:-

If unknown fingerprint has been entered then the system will not respond and no action will happen Figure (4,7).

If known fingerprint was entered and wrong password was entered through the keypad then the word (wrong) will appear on the LCD screen and the engine of car will not work Figure (4, 8).But when a wrong password has entered it can be corrected just in case it has been discovered before the check using the button (#) and entering the right password then the button (*) will be pressed for the check Figure (4,9)

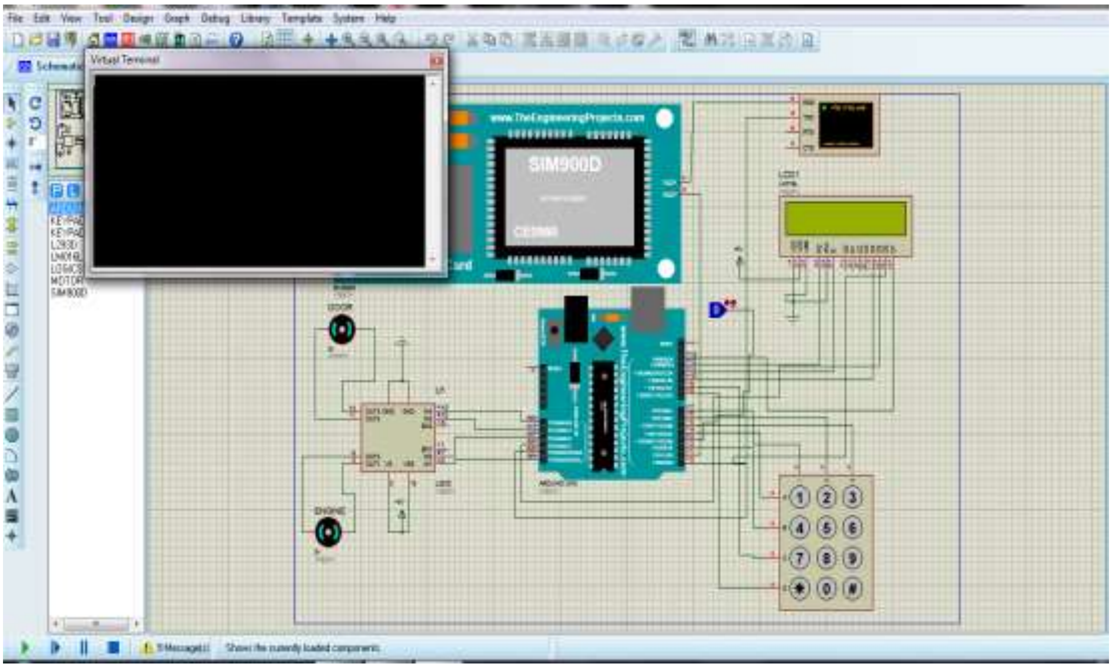
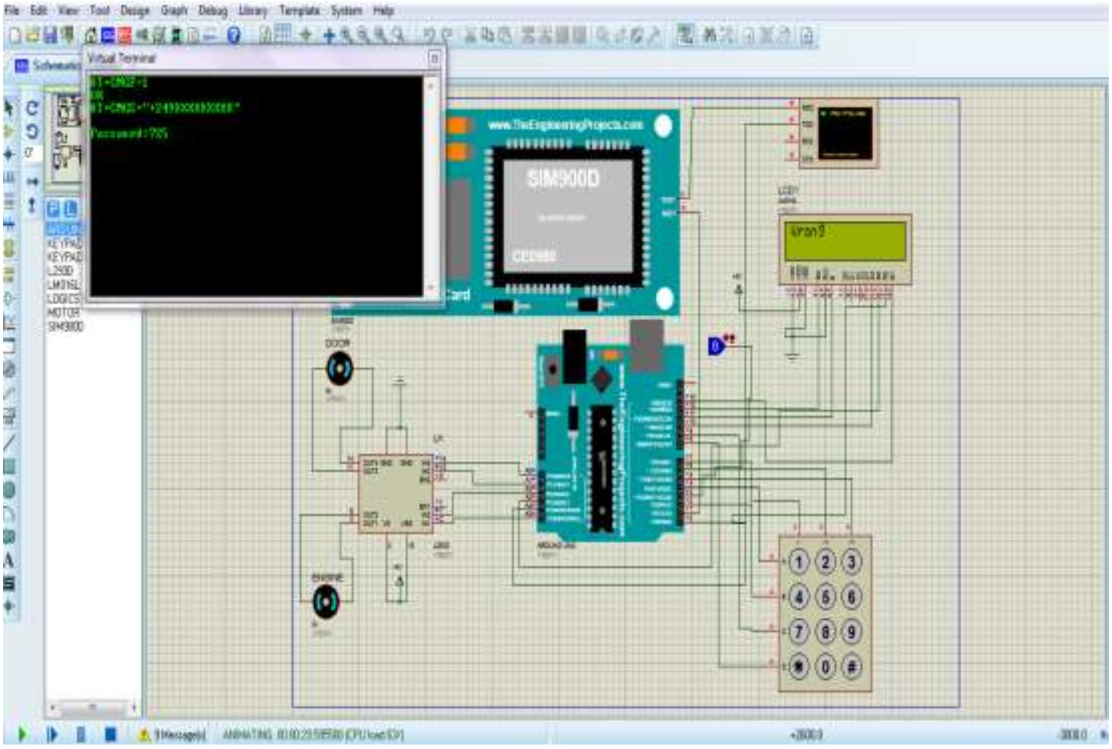


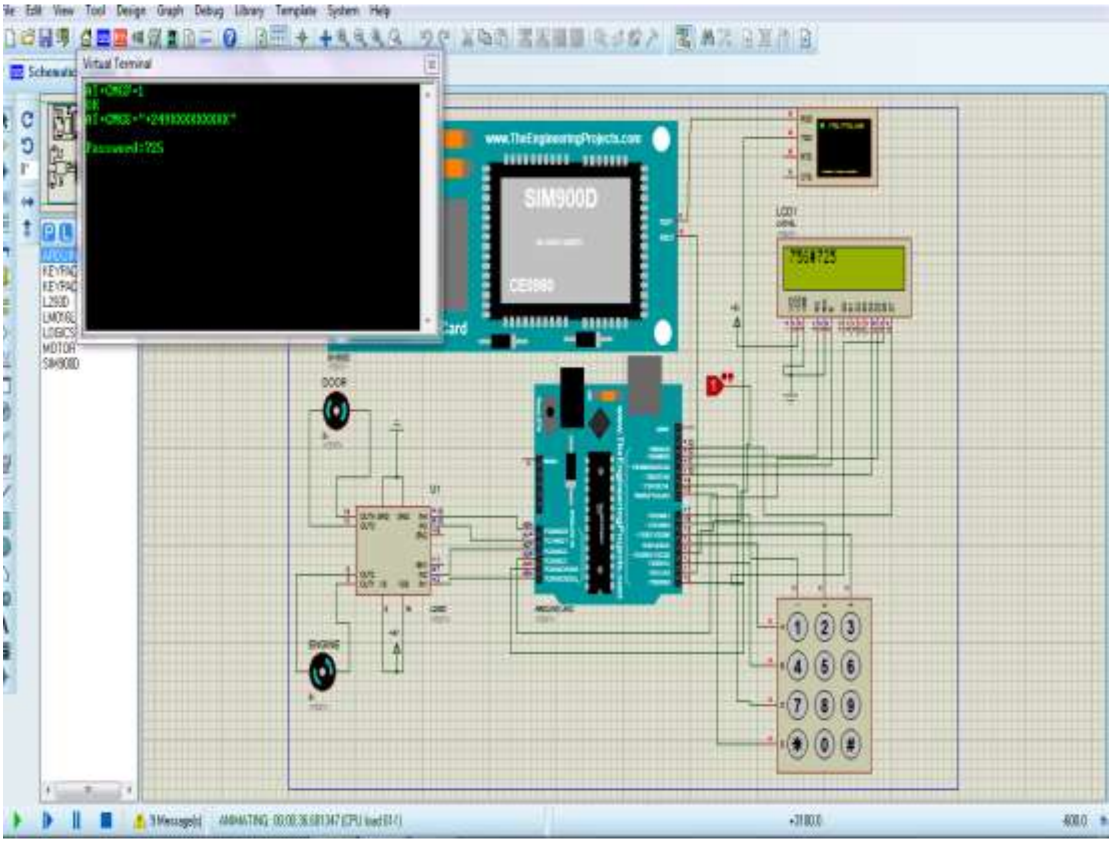
Figure (4,7) Unknown user



```
AT+CMGF=1
OK
AT+CMGS="+249XXXXXXXXX"

Password:725
```

Figure (4,8) The Wrong password



```
AT+CMGF=1
OK
AT+CMGS="+249XXXXXXXXX"

Password:725
```

Figure (4,9) Corrected password

Chapter Five

Conclusion and Recommendations

Chapter Five

Conclusion and Recommendations

5.1 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 system 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.

5.2 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 car in anywhere.

III/ Develop fingerprint mechanism to enhance the securities feature of ATM so that user can access ATM without card through his fingerprint.

References

[1] Abhishek S. Parab ,Implementation of Home Security System using GSM module and Microcontroller,2015

[2]Raghu Ram.Gangi,locker, opening and closing system using RFID,fingerprint ,password and GSM, April 2013

[3]A. AdityaShankar, P.R.K.Sastry, A. L.VishnuRam,A.Vamsidhar, Finger Print Based Door Locking System**,** March, 2015.

[4] Devendra Kumar Yadav, Sumit Singh, Mishra’ Fingerprint Based Attendance System Using Microcontroller and Lab View,June 2015

[5]Aniket A. Kale , Karan Khar, SupriyaRajankar , Arduino Based Door Access Control, March 2017

[6] MadhuR ,GSM/GPS based Device Switching with Fingerprint Module Integration using Arduino September 2016

[7]ShahzadMemon ,MojtabaSepasian , WamadevaBalachandra ,Review of Fingerprint Sensing Technologies ,2008

[8] TomHarris , How Fingerprint Scanners Work

[9] kaoru Uchida ,Fingerprint Identification,2015.

[10] RupinderSaini ,NarinderRana, Comparison of Various Biometric Methods ,March 2014

[11] James Flaten, MN Space Grant Consortium, Christopher Gosch, Chad Serba, Introduction to Arduino.

[12] Arduino FAQ – With David Cuartielles. Malmö University. April 5, 2013. Retrieved

[13] V.Ramya , B. Palaniappan , V. Sumathi ,GSM Based Embedded System for Remote Laboratory Safety Monitoring and Alerting, November 2012

.[14] Ackruti Cham, GSM Interfacing Board, 2011.

[15]Castellano, Joseph, Liquid Crystal Displays and the creation of an Industry 2005.world Scientific Publishing.

Appendixes

APPENDIX

Arduino IDE program

```
#include <LiquidCrystal.h>//مكتبة الشاشة
LiquidCrystal lcd(12,11,10,A3,A4,13);
#include <Password.h>
#include <Keypad.h>
int m1=A0;
int m2=A1;
int m3=A2;
int m4=A5;
Password password = Password  ("");
Password password2 = Password ("");
Password password3 = Password ("");
int x;
long randNumber;
const byte ROWS = 4; //متغيرين لعدد الصفوف والاعمده
const byte COLS = 3;
char keys[ROWS][COLS] = {
  {'1', '2', '3'},
  {'4', '5', '6'},//ادخال الصفوف والاعمدة
  {'7', '8', '9'},
  {'*', '0', '#'}
};
```

```
byte rowPins[ROWS] = {4, 2, 9,8};//مداخل الصفوف والاعمده في الاردوينو

byte colPins[COLS] = {7,6,5};

// Create the Keypad

Keypad keypad = Keypad( makeKeymap(keys), rowPins, colPins, ROWS, COLS );

void setup(){

  lcd.begin(16, 2);

  Serial.begin(9600);

  keypad.addEventListener(keypadEvent);

pinMode(m1,OUTPUT);

pinMode(m2,OUTPUT);

pinMode(m3,OUTPUT);

pinMode(m4,OUTPUT);

pinMode(3,INPUT);

}

void loop(){

  keypad.getKey();

  x=Serial.read();

  if (digitalRead(3)==HIGH)

  {

    digitalWrite(m3,LOW);

  digitalWrite(m4,LOW);

  }

  if (x=='c')

{
  Serial.println("AT+CMGF=1");    //Sets the GSM Module in Text Mode
  Serial.println("AT+CMGS=\"+249XXXXXXXXX\"\r"); // Replace x with mobile number
  digitalWrite(m1,HIGH);
  digitalWrite(m2,LOW);
   delay(400);
   digitalWrite(m1,LOW);
     randNumber = random(100,999);
   Serial.print("Password:"); Serial.println(randNumber);
   int num = randNumber;
char cstr[16];
itoa(num, cstr, 10);
     password.reset();
   password.set(cstr);
}
else if (x=='a')
{
    Serial.println("AT+CMGF=1");    //Sets the GSM Module in Text Mode
  Serial.println("AT+CMGS=\"+249XXXXXXXXX\"\r"); // Replace x with mobile number
  digitalWrite(m1,HIGH);
  digitalWrite(m2,LOW);
   delay(400);
   digitalWrite(m1,LOW);
   randNumber = random(100,999);
 Serial.print("Password:"); Serial.println(randNumber);
   int num = randNumber;
char cstr[16];
itoa(num, cstr, 10);
     password3.reset();
   password3.set(cstr);
}
else if (x=='b')
{
  Serial.println("AT+CMGF=1");    //Sets the GSM Module in Text Mode
  Serial.println("AT+CMGS=\"+249XXXXXXXXX\"\r"); // Replace x with mobile number
 digitalWrite(m1,HIGH);
  digitalWrite(m2,LOW);
   delay(400);
   digitalWrite(m1,LOW);
   randNumber = random(100,999);
     Serial.print("Password:"); Serial.println(randNumber);// The SMS text you want to send
   int num = randNumber;
char cstr[16];
itoa(num, cstr, 10);
     password2.reset();
   password2.set(cstr);


}

}

void keypadEvent(KeypadEvent eKey){

  switch (keypad.getState()){

    case PRESSED:

          lcd.print(eKey);

          switch (eKey){

            case '*': checkPassword(); break;

            case '#': password.reset();

             password2.reset();

              password3.reset();break;

            default: password.append(eKey);

            password2.append(eKey);

            password3.append(eKey);

     }

  }

}

void checkPassword(){

  if (password.evaluate()){

    lcd.clear();

   lcd.print("Success");

   digitalWrite(m3,HIGH);
  digitalWrite(m4,LOW);
   delay(1000);
    lcd.clear();
    //Add code to run if it works
  }
    else if (password2.evaluate()){
    lcd.clear();
   lcd.print("Success");
   digitalWrite(m3,HIGH);
  digitalWrite(m4,LOW);
   delay(1000);
    lcd.clear();
    //Add code to run if it works
  }
  else if (password3.evaluate()){
    lcd.clear();
   lcd.print("Success");
   digitalWrite(m3,HIGH);
  digitalWrite(m4,LOW);
   delay(1000);
    lcd.clear();
    //Add code to run if it works
  }
  else{
    lcd.clear();
   lcd.print("Wrong");
    delay(1000);
    lcd.clear();
   //add code to run if it did not work
  }
                                }
```