



Advanced Electronic Security and Safety System using Artificial Intelligence

A Thesis submitted to the Department of Electrical and Electronic Engineering of
BRAC University in partial fulfilment of the requirements for the Bachelor of
Science degree in Electrical and Electronics Engineering

S. M. Shuharto Jalal – 11321048

Md. Sajid Mahamud – 12121102

Supervised by

Avijit Das

BRAC University, Dhaka

Declaration

We hereby declare that the thesis title “Advanced Electronic Security and Safety System using Artificial Intelligence” submitted to the Department of Electrical and Electronics Engineering has been written on the works and result found by us. The work has not been presented elsewhere for assessment.

Signature of Supervisor

Avijit Das

S. M. Shuharto Jalal

Signature of Authors

Md. Sajid Mahamud

Acknowledgment

We are deeply grateful and honored to have a supervisor like Avijit Das, who continuously supported us with his valuable comments, discussions, positive feedbacks, proper guidance, and this thesis would not have been done without his assistant. We are also thankful to Anamul Haque sir who provide his valuable time and help us in various difficulties what we faces in our thesis. There are some other people Masharul Bin Mahfuz, Abu Nayem, Md. Hasib, and Sukanto Roy, whose endless help give this project in a proper structure. Moreover EEE faculties, students, other thesis members and friends also help us to complete our thesis within the time. Also some CSE programmers of the university give us feedback and direction to do the program in proper way. We are glad these fellow colleagues were always with us.

Abstract

Beholding the current situation of our country, lack of security and safety is a major issue with increasing crime rapidly where miscreants take advantage of the traditional vulnerable security system. This system can introduce a new advanced way to take care of most safety and security issues precisely by using three primary levels of authentication which includes finger print detection, RFID scanning and passcode. Furthermore the security system is destined to be more enhanced featuring face detection of both admin and perpetrator and feed a live video. A smart way of fire detection and alarm mechanism is intended to provide an assured safety. The system is also designed to communicate with the admin regarding the status of the security system and creates a platform to control the system remotely. The entire system converges to a control panel which is the primary controller for the security system, where the integrated system can be monitored.

Content

Declaration	ii
Acknowledgment	iii
Abstract	iv
List of Figures	viii
List of Table	x
Abbreviation	xi
Chapter 1	1
Introduction	1
1.1 Introduction to Security and Safety System:	1
1.2 Impact of security and safety system:	2
1.3 Motivation:	2
1.4 Project Overview:	3
1.5 Summary:	4
Chapter 2	5
Theoretical Overview of Security System	5
2.1 Introduction:	5
2.1.1 Monitored security system:	5
2.1.2 Unmonitored security system:	6
2.1.3 Wireless home security cameras:	7
2.1.4 Electronic security systems:	7
2.2 Overview of the System:	8
2.2.1 Fingerprint Authorization:	9
2.2.2 Password Authorization:	11
2.2.3 RFID Authorization:	11
2.2.4 Face Detection:	12
2.2.5 Fire-Detection Systems:	14
2.3 Summary:	14
Chapter 3	15
Hardware Components	15

3.1 Introduction:	15
3.2 Component used:	15
3.2.1 Arduino Mega 2560:	16
3.2.2 Fingerprint Scanner:	18
3.2.3 125 KHz RFID Module:	19
3.2.4 RFID Tag:	20
3.2.5 LCD Display:	21
3.2.6 16 Key Capacitive Keypad:	22
3.2.7 Potentiometer:	23
3.2.8 Simcom Sim900a GSM+GPRS module:	24
3.2.9 Electric Solenoid Mini Door Lock DC 12V	24
3.2.10 Buzzer:	25
3.2.11 LED Lights-5mm:	25
3.2.12 Raspberry Pi 2 Model B:	26
3.2.13 Raspberry Pi camera module:	27
3.2.14 Arduino UNO:	28
3.2.15 Flame Sensor:	29
3.2.16 Switches:	29
Chapter 4	30
Working Process	30
4.1 Introduction:	30
4.2 Pin Configuration and Symmetric Diagram:	30
4.3 Overview and Block Diagram of the System:	32
4.4 Digital Door Lock System:	34
4.5 Face Detection System:	38
4.6 Fire Detection and Alarm System:	38
Chapter 5	39
Software Configuration	39
5.1 Introduction:	39
5.2 Software Algorithm:	39
5.3 Program Flow Diagram:	41
5.4 Software:	42
5.4.1 Arduino IDE:	42

5.4.2 Software Libraries:	43
5.4.3 Functions & Syntax:	46
5.4.4 AT Commands:	48
5.4.5 AT Command syntax:	49
5.3.6. Set of AT Commands used to program this system:	51
5.4.7 AT Command Tester:	52
Chapter 6	59
Conclusion	59
6.1 Conclusion	59
6.1.1 Limitations	59
6.1.2 Future Implementation	60
References	61
APPENDICES	62

List of Figure

Figure 2.1.1: Monitored security system.....	6
Figure 2.1.2: Unmonitored security system.....	6
Figure 2.1.4: Electronic security systems.....	7
Figure 2.2.1-3: Capacitive scanners.....	10
Figure 3.2.1a: Arduino Mega 2560.....	17
Figure 3.2.1b: USB port of Arduino Mega 2560	18
Figure 3.2.2: Fingerprint Scanner- TTL (GT-511C3)	18
Figure 3.2.3: 125KHz RFID Module– UART.....	19
Figure 3.2.4: RFID Tag.....	20
Figure 3.2.5: LCD Display - 4x4.....	21
Figure 3.2.6: Keypad.....	22
Figure 3.2.7: Potentiometer (10k ohm).....	23
Figure 3.2.9: Electric Solenoid Mini Door Lock DC 12V	24
Figure 3.2.10: Buzzer.....	24
Figure 3.2.11: LED Lights-5mm.....	25
Figure 3.2.12: Raspberry Pi 2 Model B.....	26
Figure 3.2.13: Raspberry Pi camera module.....	26
Figure 3.2.14: Arduino UNO.....	27
Figure 3.2.15: Flame Sensor.....	28
Figure 3.2.16: Switches.....	29
Figure 4.1: Symmetric Diagram.....	33
Figure 5.3.1. Arduino IDE Screenshot.....	42
Figure 5.3.2 Raspberry Pi IDE Screenshot.....	45

Figure 5.3.7a AT Command Tester User Interface.....	53
Figure 5.3.7b AT Command Tester Command Mode.....	54
Figure 5.3.7c AT Command Tester Script Mode.....	55
Figure 5.3.7d AT Command Tester Diagnostics Tab.....	56

List of Table

Table 4.3 Operating Modes of the System	35
Table 5.3.2 Devices/ Modules and their corresponding libraries.....	45
Table 5.3.3 Functions used in programming and their corresponding tasks.....	47
Table 5.3.5 Types of AT commands and responses.....	50
Table 5.3.6 Set of AT Commands used in the programming of this system and their functions.....	52

Abbreviation

RFID = Radio-Frequency Identification

FACP = Fire Alarm Control Panel

ICSP = In Circuit Serial Programming

CCD = Charge Coupled Device

Chapter 1

Introduction

1.1 Introduction to Security and Safety System

Security has been a very significant concern in human society. The rise in crime rates throughout the years has been alarmingly high. In Bangladesh only high profile crimes are prioritized by the law enforcement and crimes like burglary, breaking and entering and petty theft are ignored. Sometimes this is due to the small number of law enforcement officials servicing our country's massive population. Also not every citizens of Bangladesh cannot afford competent and trained private security personnel hence some resort to recruiting underprivileged people from rural areas that can serve as a decent caretaker but cannot provide sufficient security for our homes.

Additionally the evidence for these so called "*petty crimes*" are circumstantial and law enforcement officials are unable to resolve the matter because they have very limited information at their disposal. As a result civilians or victims of crimes, that are considered trivial, don't bother to report the crime.

Countless foreigner travel in Bangladesh for their business purpose and political issues with a poor security and sometimes they trapped by criminals and suffer in many ways. Now a days, in diplomatic area more police forces are deployed by the Bangladesh Government for the security of the foreigners. A high technological home security system in the residential area can be secured more efficiently and aid Bangladesh Government to secure the foreigners effectively and more easily. So, if we can develop our security system by the support of technical knowledge, then all of stolen are closed considerably. For this result damages and losses can be reduced from Bangladesh.

The purpose of this paper is to provide some solutions to the deficiencies in our household's, offices' and banks' security through the use of technology. Although the security risks cannot be

fully eliminated but safety of homes, offices, banks and industries can be drastically improved by the introduction of simple technological contraptions.

1.2 Impact of security and safety system:

In Bangladesh crimes like burglaries, robberies and residential break-ins occurs in a regular frequency and comprise the major criminal activity all the major city in Bangladesh. Previous statistics about Bangladesh crime report shows around half of the major crime occurs due to backdated security system in the whole country. Sometimes the person who is responsible for the safekeeping are involved with the crimes so now we have to think in other way which is more reliable and technological. Recent data of Bangladesh crime report shows that 74.70% is the level of crime. In past 3 years crime increases 72.94% and home broken and things stolen is 69.05%. This is really regrettable that safety walking along during night is 25.69% and the only moderate is safety walking along road during daylight is 47.32%. Homes without well protected security systems are 2.7 times targeted by burglars. Recently Bangladesh government install surveillance camera several diplomatic areas and important sector of the Dhaka city which may help significant reduce of crime rate compare to past few year.

There are approximately more than 300,000 private security guards and private security agencies whose operation mostly in Dhaka and the other big cities. These sector is providing around Tk 300 crore to the national GDP which is high and also provide employment of many people. We are providing a technological home security system which decrease the crime rate significantly and also offer a new horizon of employment for more people by establishing a new career of the production area in this field as well as increase the GDP of our country significantly.

1.3 Motivation:

Recently there are many crimes like the Holey Artisan Bakery cafe attack in Dhaka On the night of 1 July 2016, at 21:20 local time and Kishoreganj's Sonali Bank branch robbery which motivate

us to think about something innovative and help to reduce these crimes. In order to do that we propose a home security system which minimize some percentage of relevant crimes from our society. By inspiring of this above statement we research and find the solution which moderate us to walk with advance security and safety system. Homes without well protected security systems are targeted by burglars repeatedly so protect home and family from intruders it is very important to have a decent security system. By the help of visual documentation there is an increasing chance of identifying the burglar or thieves for the future record and also video footage helps a record of what have been taken during a burglary. Time is the important factor in any emergency, in case of fire time is of the essence because in just thirty seconds a small flame can turn into a full blown of fire.

1.4 Project Overview:

In the technological race of the world which changing every aspect of the human life that make us think outside the box and do something for our society. We come up with a home security system with the basis of this idea to introduce a new advanced system for the sake of security and safety issues. We think about a three layers of security system where we include fingerprint detection, RFID examining and password checking, beside this security framework video screaming, face detection and fire alarm which are highlighted more preciously in this project.

The overview of our project is when the system is ON and user put his/her finger to the fingerprint scanner it generate an image of the ridges and valleys of the finger and detect whether the person is authorized or unauthorized. If ridges and valleys match then the system permit the user to access next process. In the next level the system will ask for the password, so the user need to type his/her password and the system will check whether the password given is correct or wrong and go with the previous way. Correctly accessed user will face RFID scanner and the successful user or admin get the permission to access the door for ten seconds. Every wrong process of this three layers security check user cannot access the next process and admin will get a message by GSM module. Beside these a live video will scream inside the home and also detect human face. If any face detected by the system it will capture and save the image and also notify admin by sending a message. Fire detected also added in this security system to detect any

flame of fire. If system sense any fire then LED and buzzer will ON and admin will get a notify message from the system.

1.5 Summary:

In the present perspective of our society where crime is increasing rapidly and significant things are stolen from houses, enterprises and business regions, and from banks in Bangladesh. These happen for the poor security framework and lack of security guard. The criminal are expert and well trained to break the secured zone of the traditional guarded security area. By studying different statistical reports of our country we come to know that by installing home security system and making it available to the market government can reduce the crime rate and increase the total GDP. We became motivated by studying the previous few year's criminal reports of our country which results is to make an advance security system to protect people from any uncertain incidence at home. We already discuss about our whole security system in the previous section where we use three layer security system and also added some additional features.

Chapter 2

Theoretical Overview of Security System

2.1 Introduction

A security system mostly designed to prevent unauthorized entry by the intruders, detect invasion, minimized burglary of valuable utilities and property damage as well as personal protection in the residential, commercial and industrial zone. Security system not only add peace of mind but also increase the economic growth of the society.

There are different types of security systems. Some are:

1. Monitored security system
2. Unmonitored security system
3. Wireless home security cameras
4. Electronic security system

2.1.1 Monitored security system:

Monitored system alarm is the most commonly used and has some pros and cons like this system alarm a call center when user gets triggered. Then the call center call the police. But the problem is that this system goes through outdoor phone line. If the burglar smart enough he can locate the line to cut them before breaking in and the call center would never be notified about that. So to minimize the problem you can use a cellular phone or radio as an alternative.

Another problem is that the burglar has quite a bit of time to get in and get a few valuables by the time when the call center and the police get notified. This system is more expensive than any other system.

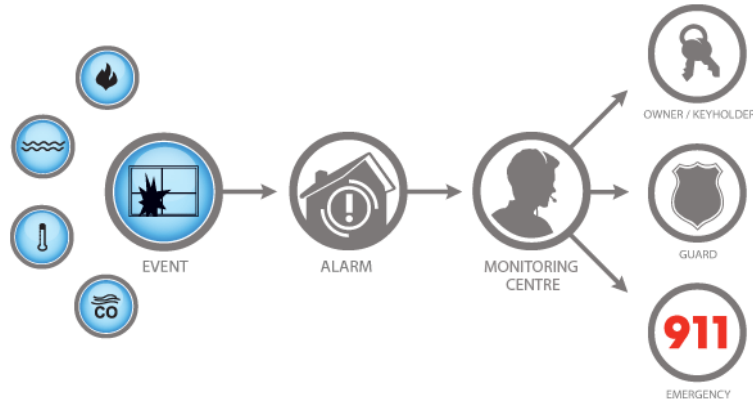


Figure 2.1.1: Monitored security system

2.1.2 Unmonitored security system:

Unmonitored security system is a system where sets off a loud distress signal inside and outside the house when alarm is tripped. This system relies on your neighbors nearby to call the police if you are not home. A major benefit to this system is you will not have to spend money monitoring fees, making it much more economical. The system can be installed with flashing lights so that people can know from where the alarm is being sounded.

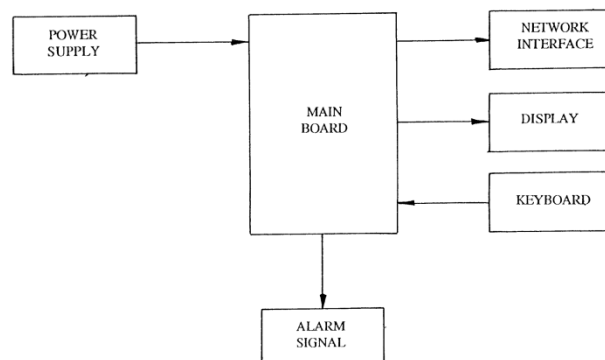


Figure 2.1.2: Unmonitored security system

2.1.3 Wireless home security cameras:

One of the newest invention in security system is wireless home security camera system which is not that much expensive compared to the other traditional CCTV cameras and the system may cost less than \$100. It can be connected almost any place inside or outside the home or business areas. The camera are so small that cannot be noticeable or detectable to the intruders or burglars at home and can also be installed outdoors anywhere like light fixtures, landscaping, stereo speakers, clocks or pinhole locations around the home or anyplace. Wireless cameras should be set up adjacent enough to the home base or camera receiver to get the information being transmitted.

2.1.4 Electronic security systems:

Electronic security systems developed with one or more danger sensing units which placed at the front of the system and generate some kind of electrical output when danger is sensed. The output of the sensor unit is nourish from a data link to a decision making signal processing unit, and this unit's output is nourish via another data link, to a 'danger' response unit such as an alarm or an electromechanical trigger or shutdown device. A simple electronic door-bell or shop-entry alarm system is an example of electronic security system.

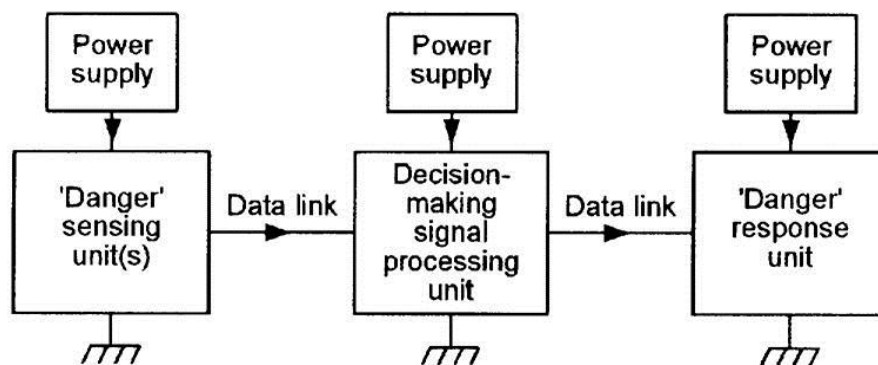


Figure 2.1.4: Electronic security systems

2.2 Overview of the System:

In our project we have done RFID scanner, password authorization, capacitive scanner for fingerprint authorization, face detection and fire alarm. RFID methods utilize radio waves to accomplish this. At a simple level, RFID systems consist of three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which are used to transmit data to the RFID reader (also called an interrogator). Password based security door lock system is an access control system that allows only authorized persons to access a restricted area. This system is best for home security system and also for corporate offices and ATMs. Another type of scanner, known as a capacitive scanner, measures your finger electrically. When your finger rests on a surface, the ridges in your fingerprints touch the surface while the hollows between the ridges stand slightly clear of it. It is projected that biometric facial recognition technology will soon overtake fingerprint biometrics as the most popular form of user authentication. Every face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features. Each human face has approximately 80 nodal points. The fire-detection system today consists of an FACP (fire alarm control panel) – this is the system's brain, and it's capable of making rapid decisions. Detection Devices run the gamut, from smoke detectors and heat detectors to multi-capability detectors, which contain a number of functions in one detector. We will discuss briefly about the total subsystems in the upcoming section of this chapter.

2.2.1 Fingerprint Authorization

Usually three types of scanners used to authorize fingerprint. They are: 1. Optical scanner, 2. Ultrasonic scanner, and 3. capacitive scanner. In our system we use capacitive scanner to authorize fingerprint. To make up a fingerprint both optical scanners and capacitive scanners generate an image of the ridges and valleys. But the difference between optical and capacitive scanners is that optical scanners use light whereas capacitive scanners use electrical current to sense the print.

2.2.1-1 Optical scanners

This method is the oldest method to capture and compare fingerprint which work by capturing an optical image and using algorithms to detect the ridges and valleys and analyzing the darkest and lightest area of the image. Security level increase depending on the sensor resolution so the higher the resolution of the sensor, the better details of the image. It's very dark when your finger is placed over the scanner, that's why optical scanners also incorporate arrays of LEDs as a flash to light up the picture come scan time.

The major drawback with optical scanners is that they aren't difficult to fool. As the technology is only capturing a 2D picture, prosthetics and even other pictures of good enough quality can be used to fool this particular design. This type of scanners really isn't secure enough to trust your most sensitive details.

2.2.1-2 Ultrasonic scanners

The latest fingerprint scanning technology to enter the smartphone space is an ultrasonic sensor which actually capture the details of a fingerprint. The hardware consists of both an ultrasonic transmitter and a receiver. An ultrasonic pulse is transmitted against the finger that is placed over the scanner. Some of this pulse is absorbed and some of it is bounced back to the sensor, depending upon the ridges, pores and other details that are unique to each fingerprint.

2.2.1-3 Capacitive scanners

The most commonly found type of fingerprint scanner used today is the capacitive scanner which works instead of creating a traditional image of a fingerprint, capacitive fingerprint scanners use arrays tiny capacitor circuits to collect data about a fingerprint. As capacitors can store electrical charge, connecting them up to conductive plates on the surface of the scanner allows them to be used to track the details of a fingerprint. The charge stored in the capacitor will be changed slightly when a finger's ridge is placed over the conductive plates, while an air gap will leave the

charge at the capacitor relatively unchanged. An op-amp integrator circuit is used to track these changes, which can then be recorded by an analogue-to-digital converter. Once captured, this digital data can be analyzed to look for distinctive and unique fingerprint attributes, which can be saved for a comparison at a later date. What is particularly smart about this design is that it is much tougher to fool than an optical scanner. The results can't be replicated with an image and is incredibly tough to fool with some sort of prosthetic, as different materials will record slightly different changes in charge at the capacitor. The only real security risks come from either hardware or software hacking.

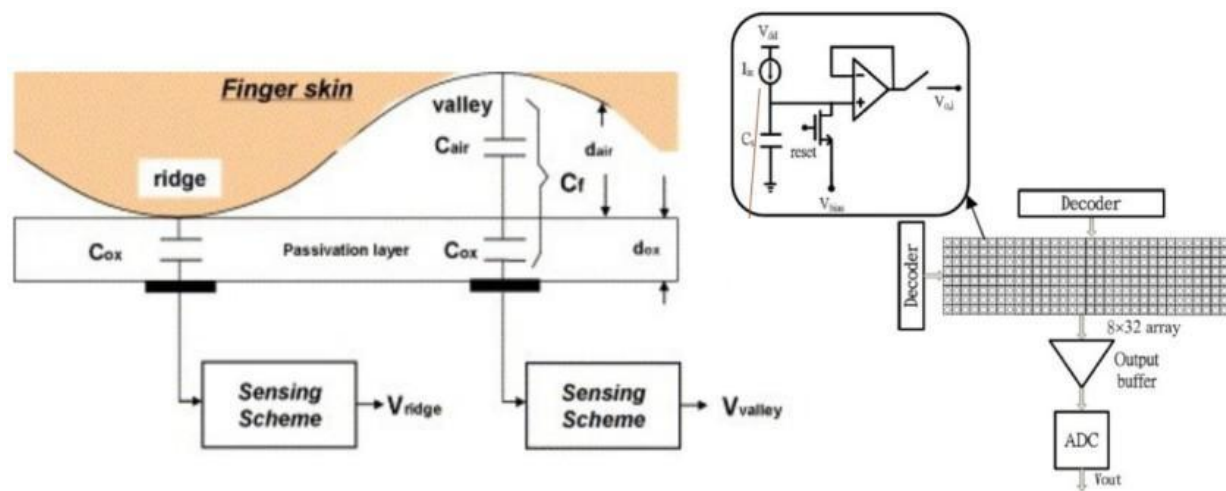


Figure 2.2.1-3: Capacitive scanners

2.2.2: Password Authorization

Password based security door lock system is an access control system that allows only authorized persons to access a restricted area. This system is best for home security system and also for corporate offices and ATMs. The system contains a small electronic unit with a numeric keypad which is fixed outside the entry door. When an authorized person enters a user ID and password with the keypad the door will open and after few times later the door will lock again. If the code entered incorrectly three times in a row, the code lock will switch to block mode and the function

prevent any attempts by the hackers try a large number of codes in a sequence. If the users forget his/her password the code lock can be access by a unique 10 digits of administrator password. The secret code can be changed any time by the master code. A buzzer can be providing on the system for audio acknowledgment of the key impression. A short beep sound can make impression the system acknowledgment when a key pressed on the numeric keypad.

2.2.3: RFID Authorization

A Radio-Frequency Identification system has three parts which are a scanning antenna, a transceiver with a decoder to interpret the data, and a transponder - the RFID tag - that has been programmed with information. The scanning antenna puts out radio-frequency signals in a relatively short range. The RF radiation does two things those are, it provides a means of communicating with the transponder and it delivers the RFID tag with the energy to communicate. This is an absolutely key part of the technology; RFID tags do not need to contain batteries, and can therefore remain usable for very long periods of time.

The scanning antennas can be permanently affixed to a surface; handheld antennas are also available. They can take whatever shape you need; for example, you could build them into a door frame to accept data from persons or objects passing through.

When an RFID tag passes through the field of the scanning antenna, it detects the activation signal from the antenna. That "wakes up" the RFID chip, and it transmits the information on its microchip to be picked up by the scanning antenna. In addition, the RFID tag may be of one of two types. They are Active RFID tags and Passive RFID tags. 1) Active RFID tags have their own power source. The advantage of these tags is that the reader can be much farther away and still get the signal. Even though some of these devices are built to have up to a 10 year life span, they have limited life spans. 2) Passive RFID tags, however, do not require batteries, and can be much smaller and have a virtually unlimited lifespan.

RFID tags can be read in a wide variety of circumstances, where barcodes or other optically read technologies are useless. The tag need not be on the surface of the object and is therefore not

subject to wear. The read time is typically less than 100 milliseconds and large numbers of tags can be read at once rather than item by item.

2.2.4: Face Detection

Face detection technique is used to recognize the face which usually works by capacity to dependably find a face and its landmarks. This is basically a segmentation issue and vast majority of the exertion goes to solving this problem. In fact the genuine acknowledgment in light of components separated from these facial landmarks is just a minor last step. There are two sorts of face identification issues:

- 1) Face detection in pictures and
- 2) Real-time face detection

2.2.4-1 Face detection in pictures

Face detection systems attempt to remove a small amount of the entire face, so eliminating the majority of the background and different areas of an individual's head like hair that are a bit much for the face detection. This is frequently done by running a "window" over the picture and the face location framework judges if a face is available inside the window with static pictures but static images have large space of possible locations of a face in a image so it can be situated anyplace from the upper left to the lower right of the picture and 21 extensive or little. Most face detection systems utilize an example based learning approach to deal with choose whether or not a face is available in the window at that given moment. A neural network enable it to group a picture as a "face" or 'non-face' by pictures for effective training. There is another procedure for figuring out if there is a face inside the face location framework's window - utilizing Template Matching. The contrast between a fixed target pattern and the window is computed. If window contains a pattern which is near the objective pattern then the window is judged as containing a face and uses an entire bank of fixed sized templates to identify facial components in a picture.

By utilizing a few formats of various sizes, appearances of changed scales are distinguished. There is other implementation of layout coordinating is utilizing a deformable format. Rather than utilizing a few settled size formats, we utilize a deformable layout and thereby change the span of the format hoping to identify a face in a picture.

2.2.4-2 Real-time face detection

Real-time face detection involves detection of a face from a series of frames from a video capturing device and the hardware requirements are much more stringent. This process is really a far less complex than detecting a face in a static image. The reason behind this is surrounding our environment, people are continually moving around, blink, fidget, wave our hands about, etc. Since in real-time face detection, the framework is given a progression of edges in which to distinguish a face, by utilizing spatio-temporal filtering the region of the casing that has changed can be recognized and the individual identified. Besides, correct face areas can be effortlessly distinguished by utilizing a couple of straightforward standards, for example, 1) the head is the little blob over a bigger blob - the body 2) head movement must be sensibly moderate and bordering - heads won't bounce around erratically. Real-time face detection has in this way turn into a moderately basic issue and is conceivable even in unstructured and uncontrolled situations utilizing these simple picture handling systems and reasoning rules.

2.2.5 Fire-Detection Systems

Before deciding to replace an antiquated fire alarm we should be aware of the different types of fire alarm systems that are on the market. The two main types of fire alarm systems are conventional and addressable and the various components that make up the system are either automatic or manual.

2.2.5-1 Conventional Fire Alarm

Conventional fire alarm systems and its components are all wired to the same cable that connects them to a fire alarm control panel. When a components is activated a signal is displayed on the control panel. These types of systems are inexpensive and work well in small facilities. The

main problem with conventional fire alarm systems is that when a fire alarm component produces a signal and it appears on the control panel there is no way to know which component it is in the building.

2.2.5-2 Addressable Fire Alarm

Addressable fire alarm systems are the most modern type of system and its components have individual unique identifiers. When one of the system's components is initiated it indicates the component's address on the fire alarm panel. Large facilities are typically equipped with these systems because they can quickly pinpoint where the trouble signal originated. This saves a lot of time because it eliminates the need to search for the component that produced the signal.

2.3 Summary:

There are different kind of security systems which we talked throughout the whole chapter in details and we discussed about their structures, working principles, and pros and cons briefly. We tried to clarify the overview of our proposed security system and the subsystems of this project. For example, we talked about fingerprint scanner, their types and working principle. Furthermore, we also discussed about other subsystem like password authorization, RFID authorization, face detection and their types as well as fire detection and their types in briefly.

Chapter 3

Hardware Components

3.1 Introduction:

In our project we tried to build a smart security system by using the most reliable and efficient components in order to achieve better output of the system. And we tried to minimize the overall cost of the equipment so that we can get a better efficiency with the minimum cost. For the construction of this project we used Arduino Mega 2560 as a microcontroller, RFID module, GSM+GPRS module, Raspberry Pi, Raspberry Pi camera module and other component which are discussed briefly throughout the chapter.

3.2 Component used:

Components we used in this project are:

- 1) Arduino Mega 2560
- 2) Fingerprint Scanner
- 3) 125Khz RFID Module
- 4) RFID Tag
- 5) LCD Display
- 6) 16 Key Capacitive Keypad
- 7) Potentiometer
- 8) Simcom Sim900a GSM+GPRS module
- 9) Electric Solenoid Mini Door Lock DC 12V
- 10) Buzzer
- 11) LED Lights-5mm
- 12) Raspberry Pi 2 Model B

- 13) Raspberry Pi camera module
- 14) Arduino UNO
- 15) Flame Sensor

3.2.1 Arduino Mega 2560

This system uses the Arduino Mega 2560, which is a high-end microcontroller unit in comparison to most other similar boards, and has been chosen so that handling large amounts of data is not an issue, as it has a fairly large RAM. The device driver programs are solely responsible for controlling the hardware devices and executing low-level hardware specific routines. These custom device drivers running on the Arduino Mega 2560 microcontroller are designed specifically to suit the needs of our proposed security system.

The Arduino Mega 2560 is a microcontroller board based on the ATmega2560. There are 54 input/output pins.

- 15 PWM (Pulse width modulation) outputs
- 16 analog inputs
- 4 UARTs (hardware serial ports)
- A 16 MHz crystal oscillator
- USB connection
- A power jack
- An ICSP header
- A reset button

USB connection or external power supply is the main power source of Arduino Mega which is selected automatically and the external power can come through an AC to DC adapter or battery. The adapter can be connected by plugging a 2.1mm center-positive plug into the board's power jack and a battery can be inserted in the Gnd and Vin pin headers of the power connection. The

board can operate on an external supply of 6 to 20 volts and the recommended range is 7 to 12 volts. Also there are some restrictions of the board's power supply. If the power supply is less than 7 volts then the 5V pin may supply less than five volts and the board is unstable but if the supply is more than 12 volts then the voltage regulator may overheat and damage the board.

The Mega2560 differs from all preceding boards in that it does not use the FTDI USB-to serial driver chip. Instead, it features the Atmega8U2 programmed as a USB-to-serial converter it has 256KB of flash memory for storing code (of which 8 KB is used for the bootloader), 8 KB of SRAM and 4 KB of EEPROM (which can be read and written with the EEPROM library).

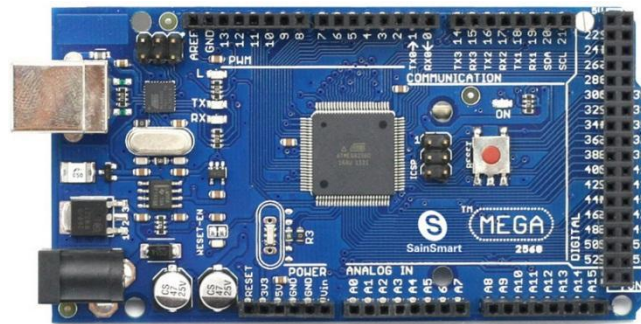


Figure 3.2.1a:Arduino Mega 2560

The Arduino Mega can be programmed with the Arduino software. The ATmega2560 on the Arduino Mega comes pre-burned 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). You can also bypass the bootloader and program the microcontroller through the ICSP (In Circuit Serial Programming) header. One of the hardware flow control lines (DTR) of the ATmega8U2 is connected to the reset line of the ATmega2560 via a 100 Nanofarad capacitor. When this line is asserted, the reset line drops long enough to reset the chip. The Arduino software uses this capability to allow you to upload code by simply pressing the upload button in the Arduino environment. The Arduino Mega2560 has a resettable polyfuse that protects your computer's USB ports from shorts and overcurrent. The Mega2560 is designed to be compatible with most shields designed for the Uno, Diecimila or Duemilanove. Although most computers provide their own internal protection, the fuse provides

an extra layer of protection. If more than 500 mA is applied to the USB port, the fuse will automatically break the connection until the short or overload is removed.

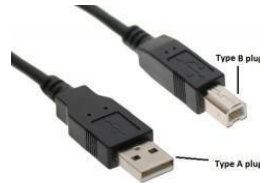


Figure 3.2.1b: USB port of Arduino Mega 2560

3.2.2 Fingerprint Scanner- TTL (GT-511C3)

The fingerprint scanner used for the system is TTL-(GT-511C3). This model has been chosen for reliability and for cost considerations, and its capability of running verification algorithm within itself, eradicating the need of exhausting fingerprint matching algorithm to be implemented and run on the scarce memory of the Android device. This scanner will be attached to the Arduino board using a JST SH Jumper 4 Wire Assembly. They are Vcc, GND, Tx, Rx. The easiest way to demo this would be to connect Pin 1 and Pin 2 to arduino D3 and D4 respectively and run FPS Blink. If the FPS blinks blue that mentions the device is working.

This module is used for both reading and identifying the fingerprints with an optical sensor and 32-bit CPU. The fingerprint scanner can store different fingerprints and the database of prints can even be downloaded from the unit and distributed to other modules. AS well as the fingerprint "pattern", the analyzed version of the print the module take the image of the print and raw image pull by the optical sensor.



Figure 3.2.2: Fingerprint Scanner- TTL (GT-511C3)

This is the updated version of the GT-511 which has an increased memory capacity. The module can store up to 200 different fingerprints and is now capable of 360° recognition.

3.2.3 125KHz RFID Module– UART

Radio frequency identification (RFID) is a wireless device that is basically used in electromagnetic fields to transfer data, for the purpose of automatically identifying and tracking tags attached to objects. There is a signal which is transmitted through the antenna for activate the tags. The signal itself is a form of energy that can be used to power the tag. The radio frequency converts into usable power by the transponder which is the part of RFID tag, Also send and receive messages. RFID 125 KHz card mini-module is designed for reading code from 125KHz card compatible read-only tags and read/write card. It can be applied in office/home/industry security, personal identification, access control and production control systems etc.

A radio frequency identification reader is a device used to gather information from an RFID tag, which is used to track individual objects. Radio waves are used to transfer data from the tag to a reader. Finally RFID is the method for automatic identification and Data Capture.

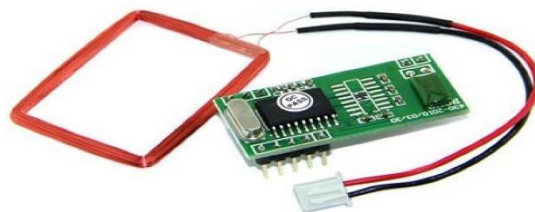


Figure 3.2.3: 125KHz RFID Module– UART

The Radio Frequency Identification (RFID) Reader Module provides a low-cost solution to read passive RFID transponder tags from up to 4 inches away. The module can be used in a wide

variety of commercial applications, including access control, user identification, robotics navigation, inventory tracking, payment systems, car immobilization, and manufacturing automation.

The RFID Reader Module works exclusively with the EM Microelectronic-Marin SA EM4100-family of 125kHz, passive, read-only transponder tags. Each transponder tag contains a unique identifier (one of 2^{40} , or 1,099,511,627,776, possible combinations) that is read by the RFID Reader Module.

3.2.4 RFID Tag

The RFID tags contained electronically stored information. There are two types of tags:

- 1) Active Tags
- 2) Passive Tags

The active tags have a local power source such as a battery and many operate at hundreds of meters from the RFID reader and the passive tags collect energy from a nearby RFID readers interrogating radio waves.



Figure 3.2.4: RFID Tag

The RFID tags are widely used in industries. Library systems, real time location system, toll tracking, access control are some of the industrial application of RFID tags. Since RFID tags can

be attached to cash, clothing and possessions, or implanted in animals and people, the possibility of reading personally linked information without consent has raised serious privacy concerns.

Since RFID tags can be attached to cash, clothing, and possessions, or implanted in animals and people, the possibility of reading personally-linked information without consent has raised serious privacy concerns.

3.2.5 LCD Display - 4x4:

LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 4x4 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.

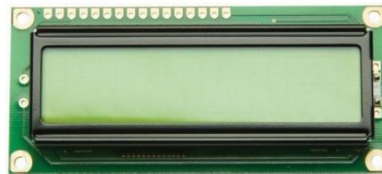


Figure 3.2.5: LCD Display - 4x4

A 4x4 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.

The command register stores the command instructions given to the LCD. A command is an instruction given to LCD to do a predefined task like initializing it, clearing its screen, setting the cursor position, controlling display etc. The data register stores the data to be displayed on the

3.2.7 Potentiometer (10k ohm)

This is a center-tap linear type potentiometer. The outer two pins will always show 10K resistance, the center pin resistance to one of the outer pins will vary from 10K Ohm to about 50 Ohm. The pot is linear meaning the resistance will vary linearly with its position. This is a good choice for general user interfaces. This pot works great in a breadboard but on a few breadboards need to trim off the large metal anchors.



Figure 3.2.7: Potentiometer (10k ohm)

3.2.8 Simcom Sim900a GSM+GPRS module:

SIM900A modules were used for all IO port pin leads which is easy to use and has basic features. It has onboard RS232 serial port which supports hardware flow control, convenient and user friendly with and PC / IPC and other devices. For easy voice communication development, onboard 3.5mm headphone and microphone is given with the module. It leads all the IO ports, and communications section IO port compatibility design made for easy connection 3.3V/5V SCM system. It has efficient synchronous buck circuit board which has conversion efficiency up to 90% and support for wide voltage range (5 ~ 24V), so that it is ideal for industrial applications. The board has onboard power anti-reverse protection, TVS power protection, SIM card ESD protection and the protection function, in addition it has board RTC backup battery (XH414H-IV01E), there is no worry about the power-down problem. Its onboard antenna can effectively improve the signal reception and also can adopt international A-level PCB material by using immersion gold processing technology which is, stable and reliable, processed using the

new components, copper plated pin and durable. The module is designed so perfectly that each interface has a screen annotation by using a glance and also connector location and reasonable arrangements designed to facilitate smoothly. PCB size is 80mm * 58mm and with mounting holes, small and exquisite. ATK-SIM900A module supports RS232 serial port and with hardware flow control it support for 5V ~ 24V that facilitate the wide scope of work, so that the module can be very convenient to connect with the product and giving product, including voice, SMS, GPRS data transmission and other functions with more efficiently.

3.2.9 Electric Solenoid Mini Door Lock DC 12V

The supply voltage of this electric device is 12 V DC which has locking telescopic length of 10mm and power form is interrupted. The unlock time for the door is 1 second. Its red wire connects to positive supply and black wire connects to negative supply. Once supply current is available, the electric lock will retract and unlock the door.



Figure 3.2.9: Electric Solenoid Mini Door Lock DC 12V

3.2.10 Buzzer:

Early devices were based on an electromechanical system identical to an electric bell without the metal gong. Similarly, a relay may be connected to interrupt its own actuating current, causing the contacts to buzz. Often these units were anchored to a wall or ceiling to use it as a sounding board. The word "buzzer" comes from the rasping noise that electromechanical buzzers made.



Figure 3.2.10: Buzzer

While technological advancements have caused buzzers to be impractical and undesirable, there are still instances in which buzzers and similar circuits may be used. In present day, buzzer is usually used for novelty uses, judging Panels, educational purposes, electronic metronomes, microwave ovens and other household appliances, electrical alarms and many other electronic devices.

3.2.11 LED Lights-5mm:

A light-emitting diode (LED) is a two-lead semiconductor light source. LEDs - those blinky things. A must have for power indication, pin status, opto-electronic sensors, and fun blinky displays.

This is a very basic 5mm LED with a red lens. It has a typical forward voltage of 2.0V and a rated forward current of 20mA. LED usually use for Status indicator, backlighting front panels, light pipe sources, lighted switches and other applications. The basic features of LED are high luminous intensity output, low power consumption, versatile mounting on PCB or panel. It has other features like popular T-1 diameter package, reliable and rugged and RoHS compliant.



Figure 3.2.11: LED Lights-5mm

3.2.12 Raspberry Pi 2 Model B:

The Raspberry Pi 2 Model B is the second generation Raspberry Pi which has a 900MHz quad-core ARM Cortex-A7 CPU and 1GB RAM. It has include some other features like 4 USB ports, 40 GPIO pins, full HDMI port, ethernet port, combined 3.5mm audio jack and composite video, camera interface (CSI), cisplay interface (DSI), microSD card slot and videoCore IV 3D graphics core.

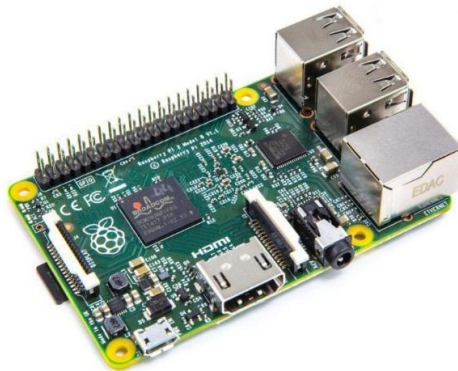


Figure 3.2.12: Raspberry Pi 2 Model B

It has an ARMv7 processor so it can run the full range of ARM GNU/Linux distributions, including Snappy Ubuntu Core, as well as Microsoft Windows 10.

3.2.13 Raspberry Pi camera module:

The Raspberry Pi camera module can be used to take high-definition video, as well as stills photographs.



Figure 3.2.13: Raspberry Pi camera module

The module has a five megapixel fixed-focus camera that supports 1080p30, 720p60 and VGA90 video modes, as well as stills capture. It attaches via a 15 cm ribbon cable to the CSI port on the Raspberry Pi.

The camera works with all models of Raspberry Pi 1 and 2. It can be accessed through the MMAL and V4L APIs, and there are numerous third-party libraries built for it, including the Picamera Python library. The camera module is very popular in home security applications, and in wildlife camera traps.

3.2.14 Arduino UNO:

Arduino is a software company, project, and user community that designs and manufactures computer open-source hardware, open-source software, and microcontroller-based kits for building digital devices and interactive objects that can sense and control physical devices. The Arduino Uno is a microcontroller board based on the ATmega328. It has 14 digital input/output pins, 6 analog inputs, a 16MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. Arduino/Genuino Uno is a microcontroller board based on

the ATmega328P. It has 14 digital input/output pins, 6 analog inputs, a 16MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started. You can tinker with your UNO without worrying too much about doing something wrong, worst case scenario you can replace the chip for a few dollars and start over again.



Figure 3.2.14: Arduino UNO

"Uno" means one in Italian and was chosen to mark the release of Arduino Software 1.0. The Uno board and version 1.0 of Arduino Software were the reference versions of Arduino, now evolved to newer releases. The Uno board is the first in a series of USB Arduino boards, and the reference model for the Arduino platform; for an extensive list of current, past or outdated boards see the Arduino index of boards.

3.2.15 Flame Sensor:

A flame detector is a sensor designed to detect and respond to the presence of a flame or fire. Responses to a detected flame depend on the installation, but can include sounding an alarm, deactivating a fuel line, and activating a fire suppression system. A flame detector can often respond faster and more accurately than a smoke or heat detector due to the mechanisms it uses to detect the flame. Near infrared (IR) array flame detectors, also known as visual flame detectors, employ flame recognition technology to confirm fire by analyzing near IR radiation

using a charge-coupled device (CCD). Infrared (IR) flame detectors monitor the infrared spectral band for specific patterns given off by hot gases.



Figure 3.2.15: Flame Sensor

These are sensed using a specialized fire-fighting thermal imaging camera (TIC), a type of thermographic camera. False alarms can be caused by other hot surfaces and background thermal radiation in the area. Water on the detector's lens will greatly reduce the accuracy of the detector, as will exposure to direct sunlight. A single-frequency IR flame detector is typically sensitive to wavelengths around 4.4 micrometers, which is a spectral characteristic peak of hot carbon dioxide as is produced in a fire. The usual response time of an IR detector is 3–5 seconds. Dual IR (IR/IR) flame detectors compare the threshold signal in two infrared ranges. Often one sensor looks at the 4.4 micrometer carbon dioxide (CO₂) emission, while the other sensor looks at a reference frequency. Sensing the CO₂ emission is appropriate for hydrocarbon fuels; for non-carbon based fuels, e.g., hydrogen, the broadband water bands are sensed.

3.2.16 Switches

A switch is a component which controls the open-ness or closed-ness of an electric circuit. They allow control over current flow in a circuit (without having to actually get in there and manually cut or splice the wires). Switches are critical components in any circuit which requires user interaction or control. A switch can only exist in one of two states: open or closed. In the off state, a switch looks like an open gap in the circuit. This, in effect, looks like an open

circuit, preventing current from flowing. In the on state, a switch acts just like a piece of perfectly-conducting wire. A short. This closes the circuit, turning the system “on” and allowing current to flow unimpeded through the rest of the system.



Figure 3.2.16: Switches

Chapter 4

Working Process

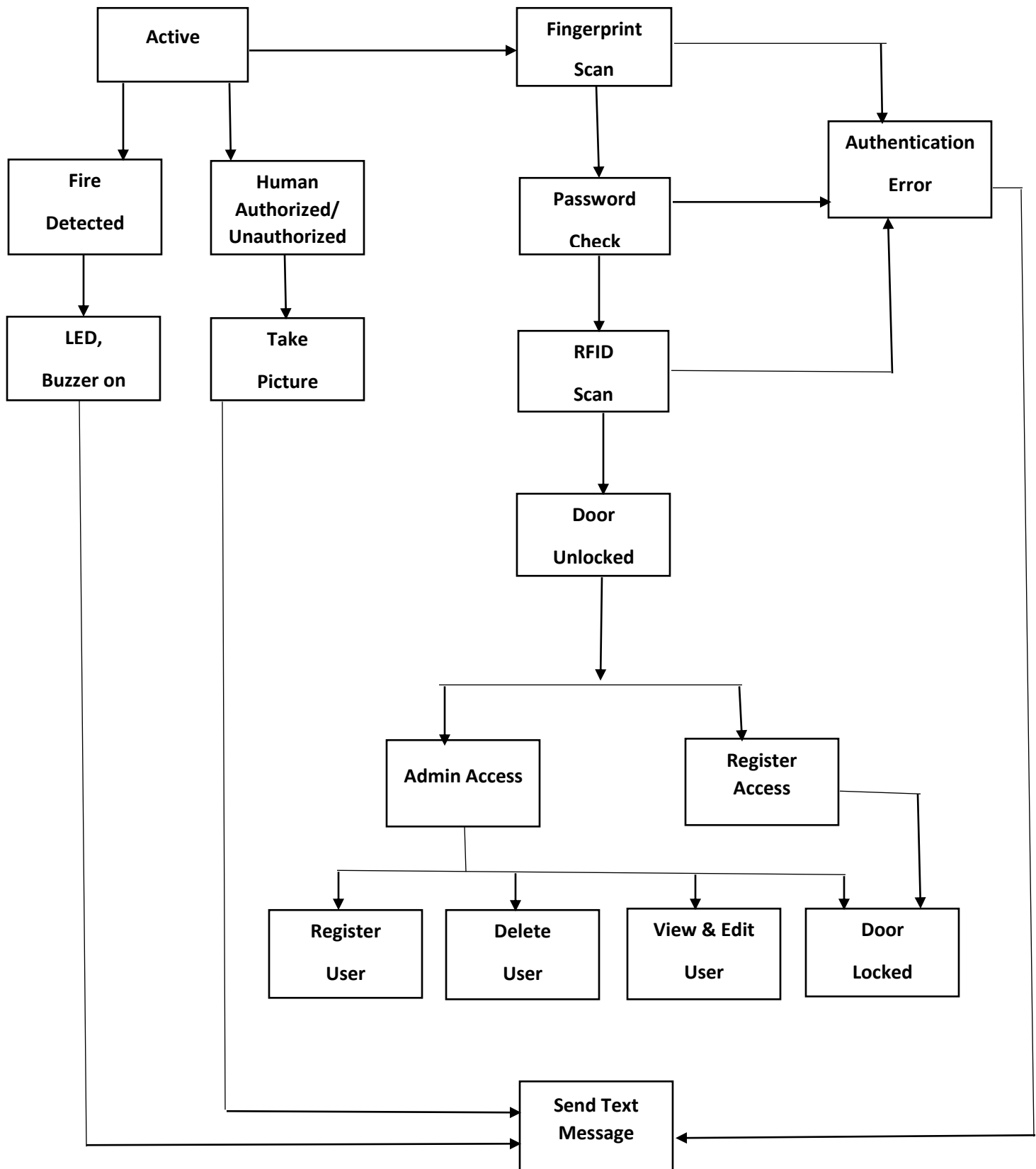
4.0 Introduction:

The prime concern of this project is to hinder any perpetrators, trying to illegitimately break in to an establishment, and alert the admin instantaneously. The authentication devices (i.e. Fingerprint Scanner, RFID, Keypad and display) is positioned on the outside of the door and the security system can be only accessed from outside. However, an unlock switch is placed inside the door in order to open it from the inside at any time. This is because, naturally the person who would be able to access the door from the inside, would not be a perpetrator. Therefore it is futile to place another set of authentication devices on the inside. At real implementation of the system, it is thought that the core devices such as the microcontroller unit, Raspberry Pi, GSM module etc. would be at a secretive place such as inside the wall or on a false ceiling so that they are out of reach of people.

4.2 Overview and Block Diagram of the System:

When the system is activated and user put his/her finger to the fingerprint scanner it generate an image of the ridges and valleys of the finger and detect whether the person is authorized or unauthorized. If ridges and valleys match then the system permit the user to access next process. In the next level the system will ask for the password, so the user need to type his/her password and the system will check whether the password given is correct or wrong and go with the previous way. Correctly accessed user will face RFID scanner and the successful user or admin get the permission to access the door for ten seconds. Every wrong process of this three layers security check user cannot access the next process and admin will get a message by GSM module. Beside these a live video will stream inside the home and also detect human face. If any face detected by the system it will capture and save the image, led in ON and also notify admin by sending a message. Fire detected also added in this security system to detect any flame of fire.

If system sense any fire then LED and buzzer will ON and admin will get a notify message from the system.



4.1 Pin Configuration and Symmetric Diagram:

The keypad are connected to the digital pins 2, 3, 4, 5, 6, 7, 8 and 9 of the Arduino Mega, among which, pins 2, 3, 4, and 5 are connected to the column of the keypad and pins 6, 7, 8 and 9 are connected to the row of the keypad. Pins 50 and 51 of the Arduino board are connected to the RX and TX pins of the fingerprint scanner module, respectively. The module powered by the 5V output pin from the Arduino board. The 125kHz RFID module connected to the Arduino Board on pin no 52 and 53 to the RX and TX pins respectively. The module powered by the 5V output pin from the Arduino board. The GSM module to the Arduino is sent or received through the RX and TX pins which are connected to pins 10 and 11 respectively. The mode of communication used by the GSM module is serial communication. A separate power adapter of 12V, 3A is used to provide the required amount of power to the GSM module to be functional. The electronic solenoid door lock is the main output of the whole system which is linked with the Arduino board by the use of an electronic solenoid door lock driver. The signal pin from the door lock driver is connected to pin number 49 of Arduino. The driver module is powered using a 12V adapter. A 16 X 2 LCD display has 6 data pins which are connected to the pins 33, 35, 37, 39, 41 and 43 of the Arduino board. The power input of the display is 5V which is fed directly from the Arduino board. A 10K analog potentiometer is used adjust the brightness of the LCD. The LED module contains two pins where one is connected to the pin 12 and one of them is the ground. An 89dB buzzer module contains three pins, +5V, ground and a signal pin. The signal pin is connected to the digital pin 13 of Arduino. The Raspberry Pi communicates with the primary control unit of the system using its GPIO pins. Raspberry Pi's GPIO pin number 26 is connected to the Arduino's digital pin 49 in order to send a signal regarding the face detection. The Raspberry Pi camera adapter. A 16 X 2 LCD display has 6 data pins which are connected to the pins 33, 35, 37, 39, 41 and 43 of the Arduino board. The power input of the display is 5V which is fed directly from the Arduino board. A 10K analog potentiometer is used adjust the brightness of the LCD. The LED module contains two pins where one is connected to the pin 12 and one of them is the ground. An 89dB buzzer module contains three pins, +5V, ground and a signal pin. The signal pin is connected to the digital pin 13 of Arduino. The Raspberry Pi communicates with the primary control unit of the system using its GPIO pins. Raspberry Pi's GPIO pin number 26 is connected to the Arduino's digital pin 49 in order to send a signal regarding the face detection. The Raspberry Pi camera module is connected to the dedicated camera port of the

Raspberry Pi development board. The Flame Sensor is connected to Arduino A0 pin which is one of the analog input pins of the microcontroller unit and provides real-time output voltage signal on the thermal resistance, the VCC was connected to a 5V power source and GND.

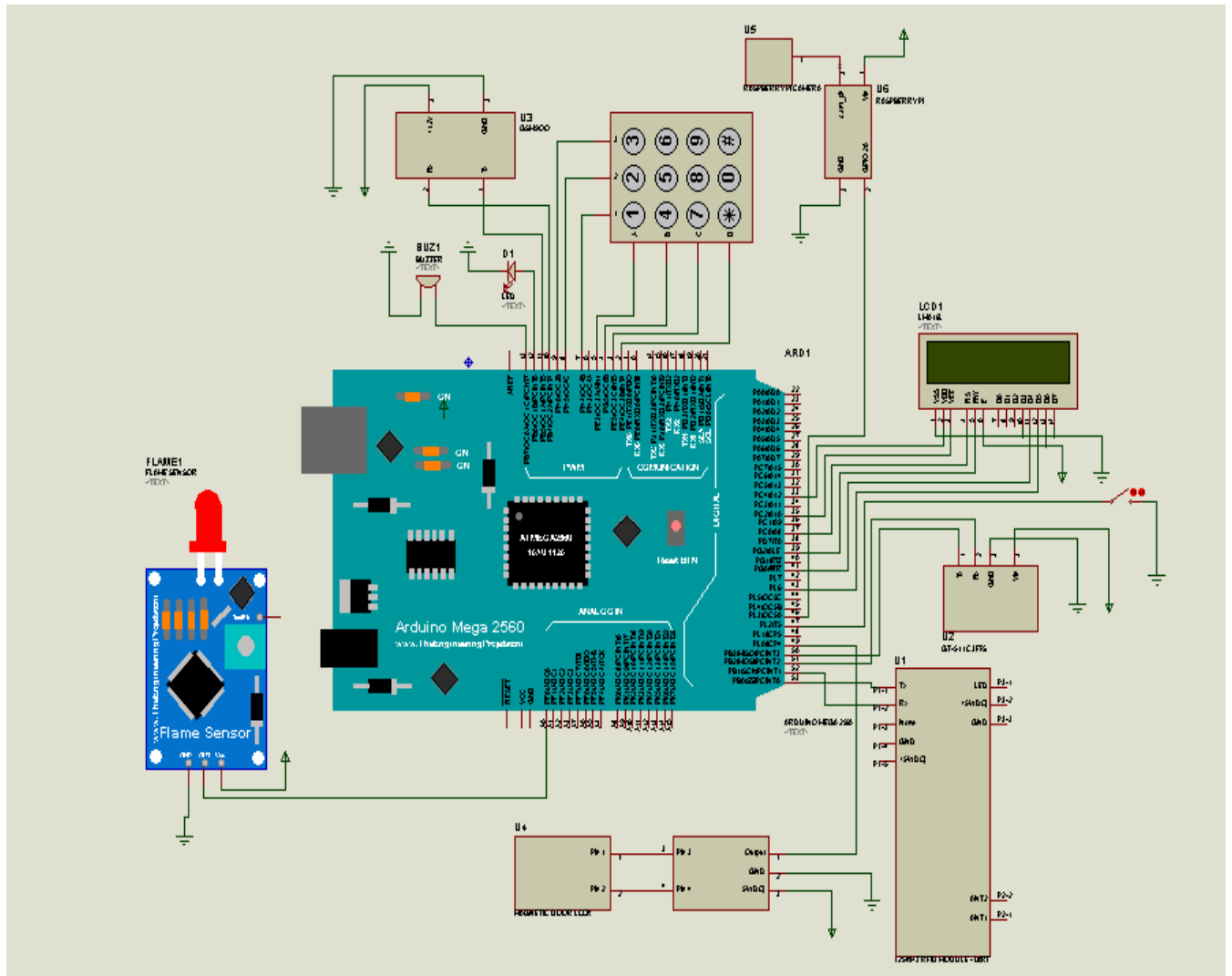


Figure 4.1: Symmetric Diagram

4.3 Digital Door Lock System:

The system is designed to have four different modes once activated. The modes are shown below in a tabular format.

State	Mode	Door Lock Status	LED/Buzzer Status	GSM Status	Fingerprint Status	RFID Status	LCD Status	Comments
1	Setup	Inactive	Inactive	Inactive	Active	Active	Active – Instructions for enrollment is displayed sequentially.	Code for enrollment is burned into the microcontroller. Admin information is obtained and stored in the main code.
2	Admin Access	Unlocked	Green; Off	Inactive	Active	Active	Active – Admin Menu and subsequent messages/instructions are displayed.	Admin Menu is displayed after door is unlocked.
3	User Access	Unlocked	Blue; Off	Active – Send SMS	Active	Active	Active – Displays “Door	Admin Menu will not be

							Unlocked”	accessible by the users
4	Wrong Input	Locked	Red; On	Active – Send SMS	Inactive	Inactiv e	Active – Displays “Wrong ID/Password ” / “Fingerprint not Found” / “RFID Not Found” / “Suspicious Activity Detected” / “Text Sent to Admin”	
5	Sleep	Locked	Yellow ; Off	Inactiv e	Inactive	Inactiv e	Active – Displays “Digital Door Lock”	

Table 4.3 Operating Modes of the System

The system is run at setup mode where a different code is burned into the microcontroller before the main code is uploaded. This is done to enroll the fingerprint of the admin and store necessary information which is required for first boot of the security system. Admin fingerprint enrollment process starts upon requesting to place the finger of the admin three times on the scanner. If the fingerprint is retrieved successfully by the scanner, it is shown on the LCD, otherwise the admin is asked again to place finger until the print is successfully read by the scanner. The RFID card

number and a five digit passcode is entered into the main code which will only be usable by the admin. The fingerprint of the admin is stored at rank 0 by default, therefore the admin's user rank is always 0. Once the RFID, passcode and the fingerprint of the admin is stored inside the database, the final code of the security system is ready to be uploaded and run.

The security system is initiated upon the press of "*" button from the keypad which acts as an input signal to start the system and promptly asks for the fingerprint of the user. When a finger is placed on the fingerprint scanner, it cross-matches the print with the prints previously stored in its database. If the fingerprint matches with the one in the database, the system proceeds to the next step of verification, otherwise it goes to State 4 where it indicates that the fingerprint scanned by the scanner is not recognized, by displaying the message on the LCD while flickering the buzzer and red LED once at the same time before it goes back to sleep mode. If the fingerprint matches with the admin it will be displayed on the LCD.

The next step of verification is a five digit passcode which is entered using the 4 X 4 keypad. Right after the fingerprint authentication the user is prompted to input a five digit user identification number followed by a corresponding five digit user password. Entering incorrect identification number or the password or even if any of the data in this step mismatches the fingerprint provided in the first step, the system displays a message on the LCD saying the password or user identification number is invalid, concurrently flickering the buzzer and the red LED once. Subsequently, if the password or user identification number is invalid for three consecutive times, the system understands that a suspicious activity is taking place and goes to state 4 where it sends a text message via the GSM module to the admin of the system. This also activates an alarm with a combined flickering of the buzzer and red LED fifteen times to grab the attention of any neighboring individual or passerby. The system automatically goes back to sleep mode right after the alarm goes off.

On another scenario, if the user identification number and the password is correctly entered, the system proceeds to the final step which consists of the RFID authentication. The LCD displays to place the RFID card near the designated area to grant the RFID access. If the RFID card number matches with the one which has been pre stored in the database and also matches with the

information provided in the previous steps, only then the access is granted and the solenoid door lock is unlocked. This information is displayed on the LCD and is indicated by glowing the blue LED as long as the door is kept opened. A text message is also sent to the admin informing which user has accessed the system. The system stays in state 3 for five minutes after which the door is locked and the system goes to sleep mode automatically.

In another situation, if the RFID card number is detected invalid i.e. if there is a conflict between the RFID card number with the information previously provided or if the RFID card is not registered, the LCD displays a message saying that the RFID card is invalid again flickering the buzzer and the red LED once. The system goes back to sleep after the buzzer and LED goes off.

On an alternative circumstance, if the person accessing the system is the admin; the system will run in Admin Access Mode which is State 2. Upon carrying out all the steps of authentication correctly; the admin will be able to access a menu, named 'Admin Menu', which will pop up automatically on the LCD with the unlocking of the solenoid door lock. At this stage the system will change its state to unlocked state unless obliged to perform otherwise. The 'Admin Menu' will have four different options which will only be available when the system is accessed by the admin. The options are:

1. Delete – In this process all the information that had been stored inside the system i.e. fingerprints, user identification number and the RFID numbers will be erased and immediately the admin will be prompted to enroll his/ her fingerprint, identification number and password and RFID number to access the system once again. This process is triggered upon the input of the "2" key from the keypad. The system goes back to sleep when the process is complete.
2. Add – This is the process to authorize another user to the system and is initiated when "3" is pressed on the keypad. The user is prompted to enroll his/ her fingerprint then to enter user identification number and password and RFID respectively following the enrollment process which had been explained earlier. The information of the new user is then stored in the database and the user is then authorized to access the security system in future. User ranks are assigned chronologically by the system automatically. The system goes back to sleep mode once the procedure is complete.

3. Show – This process is commenced when the input from the keypad is “1”. This shows the list of all the users who are currently authorized and enrolled to the system. In fact the user identification number and their corresponding password is displayed on the LCD one after another with certain time delays. The menu screen is displayed again on the LCD when the process is complete. At this stage the state of the system remains unchanged.
4. Exit – Exits the menu and resets the system as it goes back to sleep mode.

The system automatically goes to state 5 which is the sleep mode when the door is unlocked and the system is inactive for 5 seconds.

4.4 Face Detection System:

The face detection system works only works when the Raspberry Pi system is switched on by the admin. In a situation when no human is supposed to be present inside the room where the system is present, the Raspberry Pi face detection system starts rolling a live video in search for a human face. If any human face is found during those restricted hours, the Raspberry Pi sends a signal through one of its GPIO pins. That signal is fed through to the Arduino Mega as it is the primary controller for the entire system. The received signal triggers the GSM module which sends a text message to the admin of the system indicating that an intruder is present in the room. This also activates the emergency alarm of the system and with the blinking of a red LED. The Raspberry Pi immediately captures the picture of the person and saves it in its microSD card for later use for the admin. For a better user experience one picture of one type of face is saved despite reading the same type of face multiple times.

4.5 Fire Detection and Alarm System:

The fire detection and alarm system is uses the flame sensor to detect any fire inside the room or nearby. However, unfortunately due to a limited budget a low-priced flame sensor with a range of maximum 50cm was used in this project. Upon detection of fire, the sensor sends a signal directly to the Arduino Mega which triggers the alarm and activates the blinking of red LED. A text message is also sent to the admins mobile phone regarding the fire.

Chapter 5

Software Configuration

5.0 Introduction:

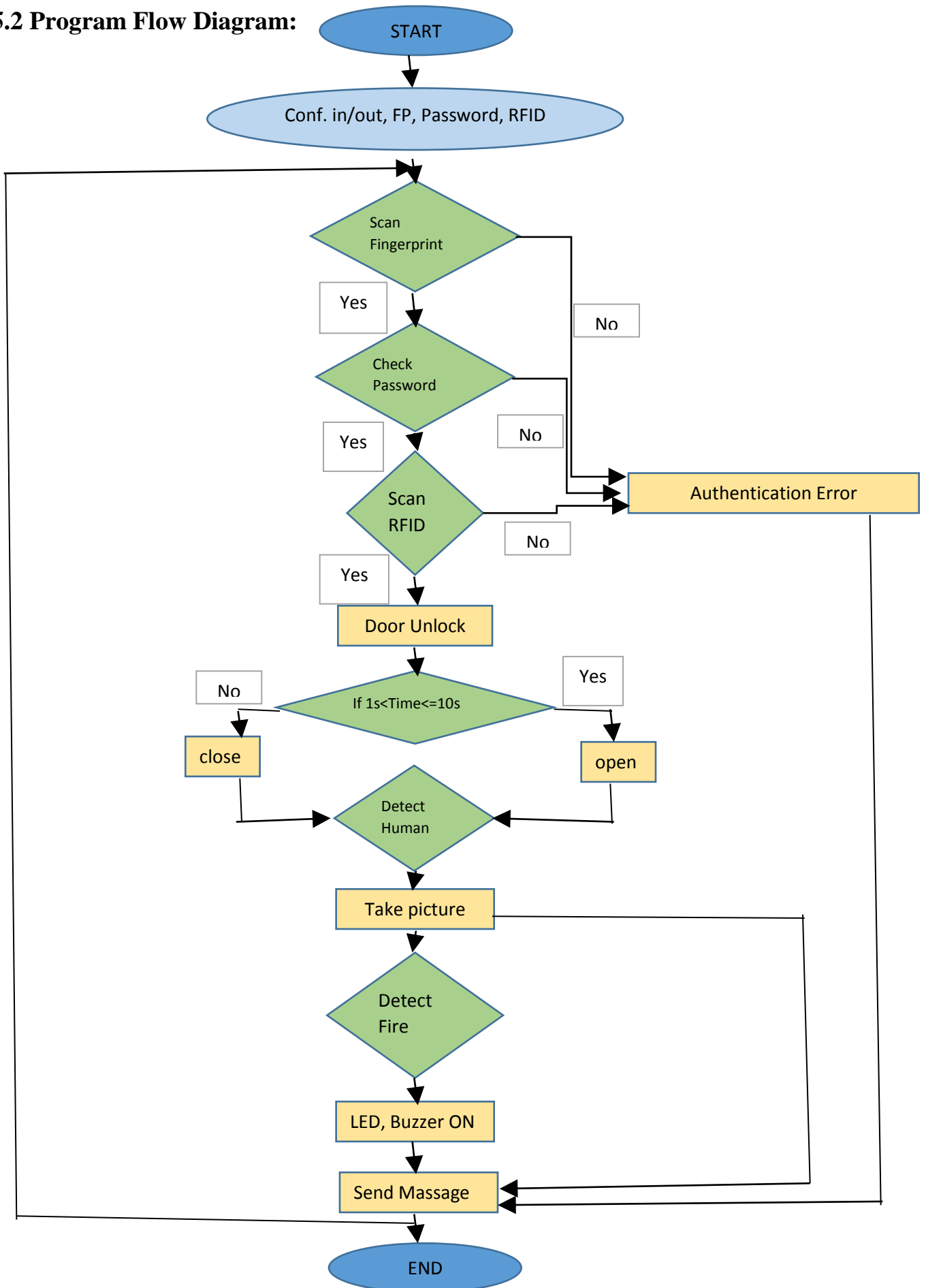
In our project we chose Arduino Mega as our microcontroller which is based on C or C++ language. For effective communications and fast processing between hardware components to microcontroller we are using this programming language. We are also using Raspberry pi and Raspberry pi camera for face detection and flame sensor are using for fire detection.

5.1 Software Algorithm:

1. Start
2. Configure input\output
3. Configure Fingerprint
4. Configure Password
5. Configure RFID Scan
6. Initialize default value and constant
7. Scan Fingerprint
8. If fingerprint matches then go forward
9. Else show authentication error
10. And send message to the admin
11. Check password
12. If password matches then go forward
13. Else show authentication error
14. And send message to the admin
15. Scan RFID

16. If RFID matches then door unlocked
17. Else show authentication error
18. And send message to the admin
19. If time $1s < \text{Time} \leq 10s$ then door open
20. Else door close
21. If detect human then take picture and send message to the admin
22. Else go forward
23. If detect fire then LED and Buzzer on and send message to the admin
24. Else go to step 7
25. End

5.2 Program Flow Diagram:

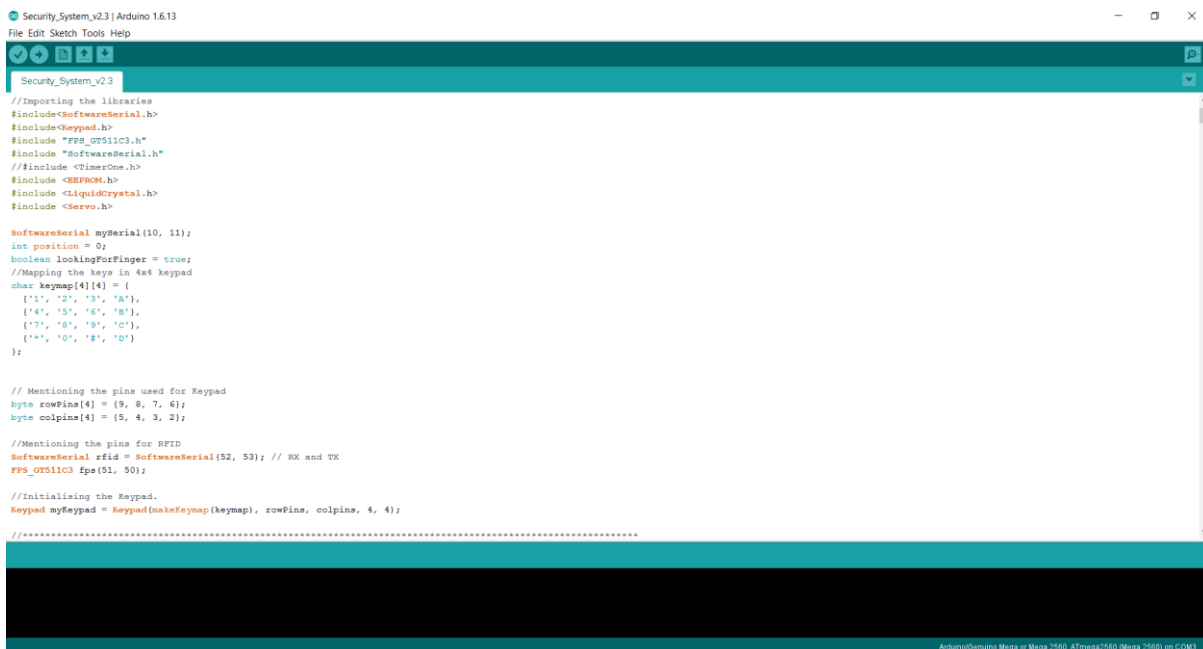


5.3 Software Configuration:

Some basic software what we are using in our project describe in details in next sub-sections.

5.3.1. Arduino IDE:

One of the major components of this security and safety system is the software coding in order to make the system fully functional. The core of the system is the Arduino Mega development board which is programmed using Arduino IDE version 1.6.13. The programming language supported by the board is based on C and C++ languages and is coded using the Arduino development environment. The usage of programming in this project facilitates effective communications and fast processing between hardware components that are connected to the microcontroller.



```

Security_System_v2.3 | Arduino 1.6.13
File Edit Sketch Tools Help
Security_System_v2.3

//Importing the libraries
#include<SoftwareSerial.h>
#include<Keypad.h>
#include "FPS_07511C3.h"
#include "SoftwareSerial.h"
//include <TimerOne.h>
#include <EEPROM.h>
#include <LiquidCrystal.h>
#include <Servo.h>

SoftwareSerial mySerial(10, 11);
int position = 0;
boolean lookingForFinger = true;
//Mapping the keys in 4x4 keypad
char keypad[4][4] = {
  {'1', '2', '3', 'A'},
  {'4', '5', '6', 'B'},
  {'7', '8', '9', 'C'},
  {'*', '0', '#', 'D'}
};

// Mentioning the pins used for Keypad
byte rowPins[4] = {9, 8, 7, 6};
byte colPins[4] = {5, 4, 3, 2};

//Mentioning the pins for RFID
SoftwareSerial rfid = SoftwareSerial(52, 53); // RX and TX
FPS_07511C3 fps(51, 50);

//Initialising the Keypad.
Keypad myKeypad = Keypad(makeKeypad(keymap), rowPins, colPins, 4, 4);

//*****

```

Figure 5.3.1. Arduino IDE Screenshot

Arduino IDE is written in Java and is a cross-platform application. It is designed to help programmers to configure the Arduino microcontrollers to their preference. Arduino programs are written in C or C++ but require two functions, setup() and loop(), to make a runnable cyclic

executive program. The `setup()` function initializes all the settings and runs once at the start of the program. The `loop()` function executes the microcontrollers main job and is called repeatedly until the board powers off.

The ATmega2560 on the Arduino Mega 2560 comes preprogrammed with a bootloader that allows users to upload new code to it without the use of an external hardware programmer. It communicates using the original STK500. It can also be able to bypass the bootloader and program the microcontroller through the ICSP (In-Circuit Serial Programming) header using Arduino ISP or similar. The ATmega16U2/8U2 is loaded with a DFU bootloader, which can be activated by pulling the 8U2/16U2 HWB line to ground, making it easier to put into DFU mode. Then the Atmel's FLIP software (Windows) or the DFU programmer (Mac OS X and Linux) can be used to load a new firmware. Or the ISP header with an external programmer (overwriting the DFU bootloader) can also be used.

An important role that the software plays is the about the security concerns. The software is equipped with a sturdy security that is unbreakable by any ordinary programmer and be able to read the RFID tag numbers or the passcode. These numbers are processed within the module and are severely encoded which is not easy to decode the encryption and read the tag numbers. The system is coded in such a way that it is smart enough to determine the authorized user and can act accordingly.

In order to use the Raspberry Pi module, the Raspberry Pi operating system had to be installed. The operating system that was used is called Raspbian which comes pre-installed with plenty of software for education, programming and general use. It has Python, Scratch, Sonic Pi, Java, Mathematica and more.

5.3.2. Software Libraries:

Programming also enables the microcontroller to learn about different devices that are attached with it. For each of the different modules used for the architecture of the system, different software libraries were used.

A software library is a suite of data and programming code that is used to develop software programs and applications. It is designed to assist both the programmer and the programming language compiler in building and executing software.

A software library generally consists of pre-written code, classes, procedures, scripts, configuration data and more. Typically, a developer might manually add a software library to a program to achieve more functionality or to automate a process without writing code for it. For example, when developing a mathematical program or application, a developer may add a mathematics software library to the program to eliminate the need for writing complex functions. All of the available functions within a software library can just be called/used within the program body without defining them explicitly. Similarly, a compiler might automatically add a related software library to a program on run time.

In other words, libraries are a collection of code that makes it easy to connect to a variety of modules or devices such as a sensor, display etc. For example, the built-in LiquidCrystal library makes it easy to talk to character LCD displays.

In this project a number of libraries were required so as to interface different devices and modules which are included in this process of software implementation to make the system functional. Libraries were used for the Fingerprint Scanner, RFID module, GSM Module, Keypad, EEPROM of Arduino and the Liquid Crystal Display.

For the development of the face detection system, the OpenCV library was installed inside the Raspberry Pi. OpenCV (Open Source Computer Vision) is a library of programming functions mainly aimed at real-time computer vision. Originally developed by Intel's research center in Nizhny Novgorod (Russia), it was later supported by Willow Garage and is now maintained by Itseez. This library is essentially used for real-time image processing, and is used in applications like gesture mapping, motion tracking – and facial recognition.

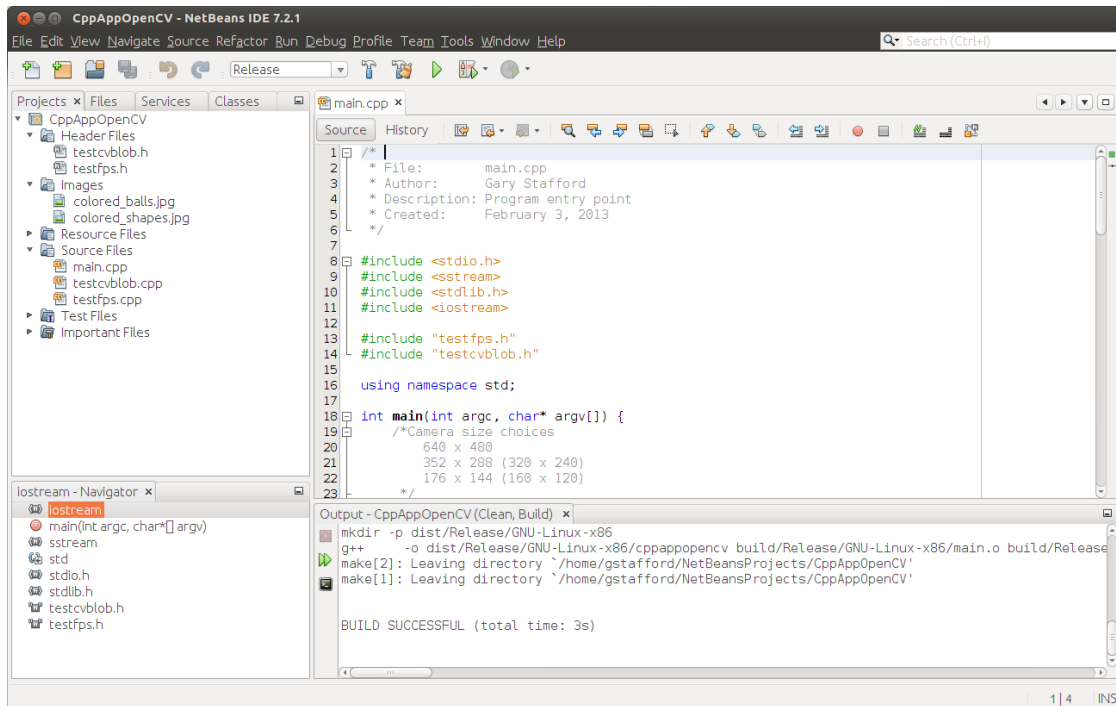


Figure 5.3.2 Raspberry Pi IDE Screenshot

The aforementioned devices or modules and their corresponding library files that were used to program the system are shown in the table below.

Sl.no	Devices/ Modules	Library files
1	Fingerprint Scanner	FPS_GT511C3.h
2	RFID Module	SoftwareSerial.h
3	GSM Module	SIM900 ,SoftwareSerial.h
4	Keypad	Keypad.h
5	Liquid Crystal Display	LiquidCrystal.h
6	Arduino EEPROM	EEPROM.h
7	Raspberry Pi	OpenCV

Table 5.3.2 Devices/ Modules and their corresponding libraries

5.3.3. Functions & Syntax:

Several built-in functions from each of the libraries and default Arduino functions are used to operate different tasks by the devices connected to the Arduino.

The functions and their corresponding tasks are shown in the following table.

Sl. no.	Functions	Tasks
1	<code>#include<SoftwareSerial.h></code>	Imports the Software serial library file
2	<code>#include<Keypad.h></code>	Imports the Keypad library file
3	<code>#include "FPS_GT511C3.h"</code>	Imports the Fingerprint Scanner library file
4	<code>#include <EEPROM.h></code>	Imports the EEPROM library file
5	<code>#include <LiquidCrystal.h></code>	Imports the LCD library file
6	<code>SoftwareSerialmySerial(10, 11);</code>	Creates an object named mySerial for GSM module. Indicates that the RX pin of the module is connected to pin 10 and TX pin is connected to pin 11 of the Arduino.
7	<code>SoftwareSerialrfid = SoftwareSerial(52, 53);</code>	Creates an object named rfid for RFID module. Indicates that the RX pin of the module is connected to pin 52 and TX pin is connected to pin 53 of the Arduino.
9	<code>FPS_GT511C3 fps(51, 50);</code>	Creates an object named fps for Fingerprint Scanner module. Indicates that the RX pin of the module is connected to pin 51 and TX pin is connected to pin 52 of the Arduino.
10	<code>mySerial.begin(9600);</code>	Sets Baud-rate of the GSM Module
11	<code>mySerial.println();</code>	Sends commands to the GSM Module
12	<code>fps.Open();</code>	Starts the Fingerprint Scanner
13	<code>fps.Close();</code>	Stops the fingerprint Scanner
14	<code>fps.SetLED();</code>	Sets the LED status of the Fingerprint Scanner

15	<code>fps.CheckEnrolled();</code>	Checks fingerprint with the previously enrolled in the database
16	<code>fps.EnrollStart();</code>	Enroll new fingerprint
17	<code>fps.IsPressFinger();</code>	Checks if any finger is present on the scanner
18	<code>fps.CaptureFinger();</code>	Captures print of the finger currently placed
19	<code>fps.Identify1_N();</code>	Identifies fingerprint number from the database
20	<code>fps.DeleteAll();</code>	Deletes all fingerprints from the database
21	<code>rfid.begin(9600);</code>	Sets the Baud-rate of the RFID Module
22	<code>Keypad myKeypad = Keypad(makeKeymap(keymap)), rowPins, colpins, 4, 4);</code>	Initializes the Keypad. Makes a map of the keypad using rows and columns
23	<code>myKeypad.waitForKey();</code>	Waits until a key is pressed from the keypad
24	<code>lcd.begin(16, 2);</code>	Initializing LCD. Setting number of rows and columns of the LCD.
25	<code>lcd.setCursor(column, row);</code>	Setting the cursor of the LCD
26	<code>lcd.print(" ");</code>	Displaying message on the LCD
27	<code>lcd.write(" ");</code>	Displaying a single character on the LCD
28	<code>lcd.clear();</code>	Clears the LCD screen
29	<code>EEPROM.read()</code>	Reads the ArduinoEEPROM and send its values to the computer
30	<code>EEPROM.write</code>	Stores values from an analog input to the Arduino EEPROM
31	<code>pinMode(pin number, INPUT/OUTPUT);</code>	Configures the specified pin to behave either as an input or an output.
32	<code>digitalWrite(pin number, HIGH/LOW);</code>	Writes a HIGH (5V) or a LOW (0V) value to a digital pin.
33	<code>digitalRead(pin number)</code>	Reads the value from a specified digital pin, either HIGH (5V) or LOW (0V).
34	<code>analogRead(pin number)</code>	Reads the value from the specified analog pin.
33	<code>delay(ms)</code>	Delays by the value mentioned in microseconds

Table 5.3.3 Functions used in programming and their corresponding tasks

5.3.4. AT Commands:

There are special sets of commands to control the GSM module from the computer or controller. These commands are called AT commands. AT commands are used to control modems. AT is the abbreviation for Attention. Every command line starts with "AT" or "at". That's why modem commands are called AT commands. These commands come from Hayes commands that were used by the Hayes smart modems. The Hayes commands started with AT to indicate the attention from the modem. The dial up and wireless modems (devices that involve machine to machine communication) need AT commands to interact with a computer. These include the Hayes command set as a subset, along with other extended AT commands. For this system, module SIM900a is being used. It has its certain group of commands. As sending SMS between different cells of the system is a prime need, the SMS commands are used.

Point to be noted is that the starting "AT" is the prefix that informs the modem about the start of a command line. It is not part of the AT command name.

Mobile phone manufacturers usually do not implement all AT commands, command parameters and parameter values in their mobile phones. Also, the behaviour of the implemented AT commands may be different from that defined in the standard. In general, GSM/GPRS modems designed for wireless applications have better support of AT commands than ordinary mobile phones.

There are two types of AT commands: basic commands and extended commands.

Basic commands are AT commands that do not start with "+". For example, D (Dial), A (Answer), H (Hook control) and O (Return to online data state) are basic commands.

Extended commands are AT commands that start with "+". All GSM AT commands are extended commands. For example, +CMGS (Send SMS message), +CMSS (Send SMS message from storage), +CMGL (List SMS messages) and +CMGR (Read SMS messages) are extended commands.

The GSM engines are referred to as following term:

- 1) ME (Mobile Equipment);
- 2) MS (Mobile Station);
- 3) TA (Terminal Adapter);

4) DCE (Data Communication Equipment) or facsimile DCE (FAX modem, FAX board);

In application, controlling device controls the GSM engine by sending AT Command via its serial interface. The controlling device at the other end of the serial line is referred to as following term:

- 1) TE (Terminal Equipment);
- 2) DTE (Data Terminal Equipment) or plainly "the application" which is running on an embedded system;

5.3.5. AT Command syntax

The "AT" or "at" prefix must be set at the beginning of each Command line. To terminate a Command line enter <CR>.

Commands are usually followed by a response that includes.
 "<CR><LF><response><CR><LF>"

Throughout this document, only the responses are presented, <CR><LF> are omitted intentionally.

A HEX string such as "00 49 49 49 49 FF FFFFFFFF" will be sent out through serial port at the baud rate of 115200 immediately after SIM900 is powered on. The string shall be ignored since it is used for synchronization with PC tool. Only enter AT Command through serial port after SIM900 is powered on and Unsolicited Result Code "RDY" is received from serial port. If auto-bauding is enabled, the Unsolicited Result Codes "RDY" and so on are not indicated when you start up the ME, and the "AT" prefix, not "at" prefix must be set at the beginning of each command line. All these AT commands can be split into three categories syntactically: "basic", "S parameter", and "extended". These are as follows:

Basic syntax: These AT commands have the format of "AT<x><n>", or "AT&<x><n>", where "<x>" is the Command, and "<n>" is/are the argument(s) for that Command. An example of this is "ATE<n>", which tells the DCE whether received characters should be echoed back to the DTE according to the value of "<n>". "<n>" is optional and a default will be used if missing.

S Parameter syntax: These AT commands have the format of "ATS<n>=<m>", where "<n>" is the index of the S register to set, and "<m>" is the value to assign to it. "<m>" is optional; if it is missing, then a default value is assigned.

Extended Syntax: These commands can operate in several modes, as in the following table:

Test Command	AT+<x>=?	The mobile equipment returns the list of parameters and value ranges set with the corresponding Write Command or by internal processes.
Read Command	AT+<x>?	This command returns the currently set value of the parameter or parameters.
Write Command	AT+<x>=<...>	This command sets the user-definable parameter values.
Execution Command	AT+<x>	The execution command reads non-variable parameters affected by internal processes in the GSM engine.

Table 5.3.5 Types of AT commands and responses

Combining AT commands on the same Command line

You can enter several AT commands on the same line. In this case, you do not need to type the "AT" or "at" prefix before every command. Instead, you only need type "AT" or "at" the beginning of the command line. Please note to use a semicolon as the command delimiter after an extended command; in basic syntax or S parameter syntax, the semicolon need not enter, for example: ATE1Q0S0=1S3=13V1X4+IFC=0,0;+IPR=115200; &W.

The Command line buffer can accept a maximum of 556 characters. If the characters entered exceeded this number then none of the Command will executed and TA will return "**ERROR**".

Entering successive AT commands on separate lines

When you need to enter a series of AT commands on separate lines, please Note that you need to wait the final response (for example OK, CME error, CMS error) of last AT Command you entered before you enter the next AT Command.

Supported character sets

The SIM900 AT Command interface defaults to the **IRA** character set. The SIM900 supports the following character sets:

GSM format

UCS2

HEX

IRA

PCCP

PCDN

8859-1

The character set can be set and interrogated using the "**AT+CSCS**" Command (GSM 07.07).

The character set is defined in GSM specification 07.05.

The character set affects transmission and reception of SMS and SMS Cell Broadcast messages, the entry and display of phonebook entries text field and SIM Application Toolkit alpha strings.

Flow control

Flow control is very important for correct communication between the GSM engine and DTE. For in the case such as a data or fax call, the sending device is transferring data faster than the receiving side is ready to accept. When the receiving buffer reaches its capacity, the receiving device should be capable to cause the sending device to pause until it catches up.

There are basically two approaches to achieve data flow control: software flow control and hardware flow control. SIM900 support both two kinds of flow control. In Multiplex mode, it is recommended to use the hardware flow control.

5.3.6. Set of AT Commands used to program this system:

The AT Command set which is used to program this system is shown in the table below:

Demonstration	Syntax	Expect Result
Check if GSM Module is connected	AT	OK
Set SMS system into text mode, as opposed to PDU mode.	AT+CMGF=1	OK
Send an SMS to Admin.	AT+CMGS="+8801670669566" >This is a test <Ctrl+Z>	OK +CMGS:34 OK
Unsolicited notification of the SMS arriving	+CMTI: "SM",1	
Read SMS message that has just arrived. Note: the number should be the same as that given in the +CMTI notification.	AT+CMGR=1	+CMGR: "REC UNREAD", "+8801670669566", "", "02/01/30,20:40:31+00" This is a test OK
List all SMS messages. Note: "ALL" must be in uppercase.	AT+CMGL="ALL"	+CMGL: 1,"REC UNREAD", "+8801670669566", "", "02/01/30,20:40:31+00" This is a test +CMGL: 2,"REC UNREAD", "", "+8801670669566", "", "02/01/30,20:45:12+00"
Delete an SMS message.	AT+CMGD=1	OK

Table 5.3.6 Set of AT Commands used in the programming of this system and their functions.

5.3.7. AT Command Tester:

AT Command Tester is a serial monitor based software which analyses the AT commands being sent and received from a device as well as providing a look into the underlying process that takes place during those interchanges, which gave us a proper understanding of what is happening inside in response to our input commands. The tool was used to test the GSM module before implementing in the main circuit. The user friendly interface allows developers to:

- Configure and connect to modem ports
- Send single or batch of AT commands
- Perform modem diagnostics
- Establish 3G or GPRS call
- Collect and save modem logs

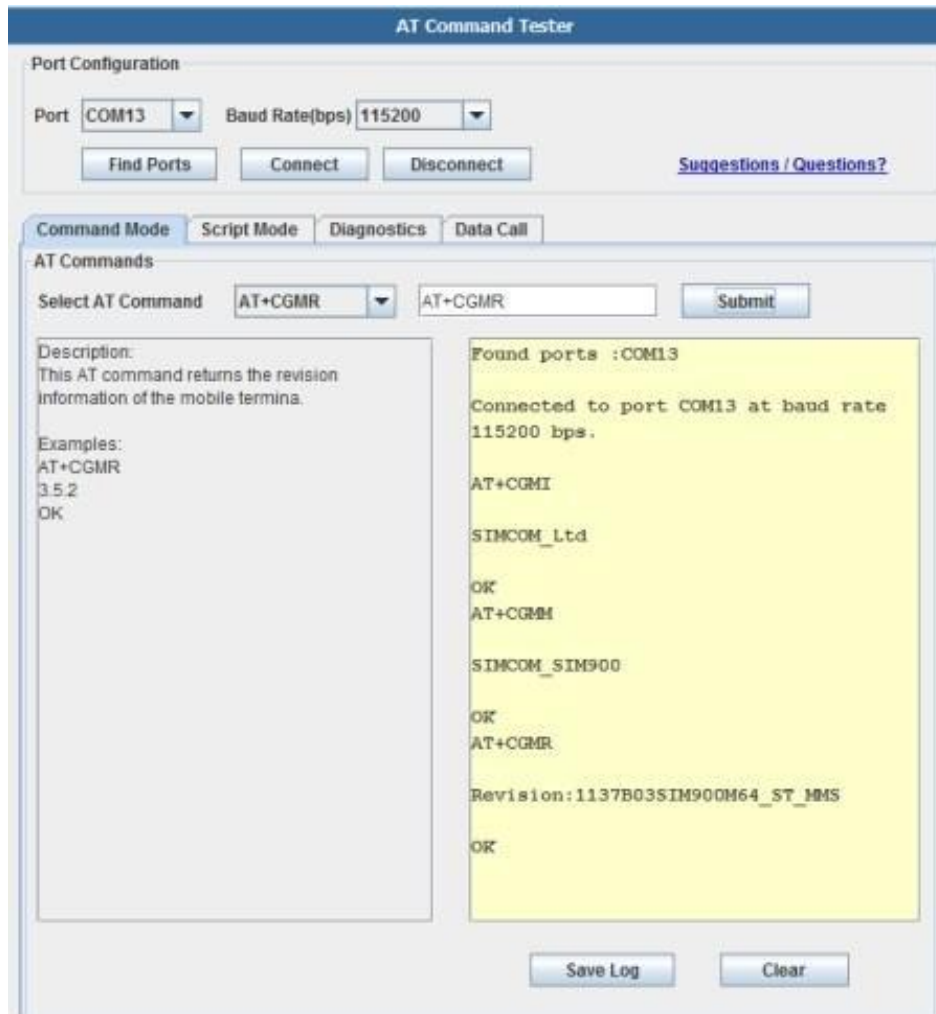


Figure 5.3.7a AT Command Tester User Interface

Port Configuration

AT Command Tester uses Java-based serial drivers to interface to the modem. The 'Find Ports' button will automatically find all ports available in the system. The user can connect the appropriate modem port with the desired port speed.

Command mode

After connecting successfully to the modem, users can send single AT commands under ‘Command Mode’ tab. The drop down provides a list of AT commands with description and examples. The users can modify or enter their own AT command in the text box.

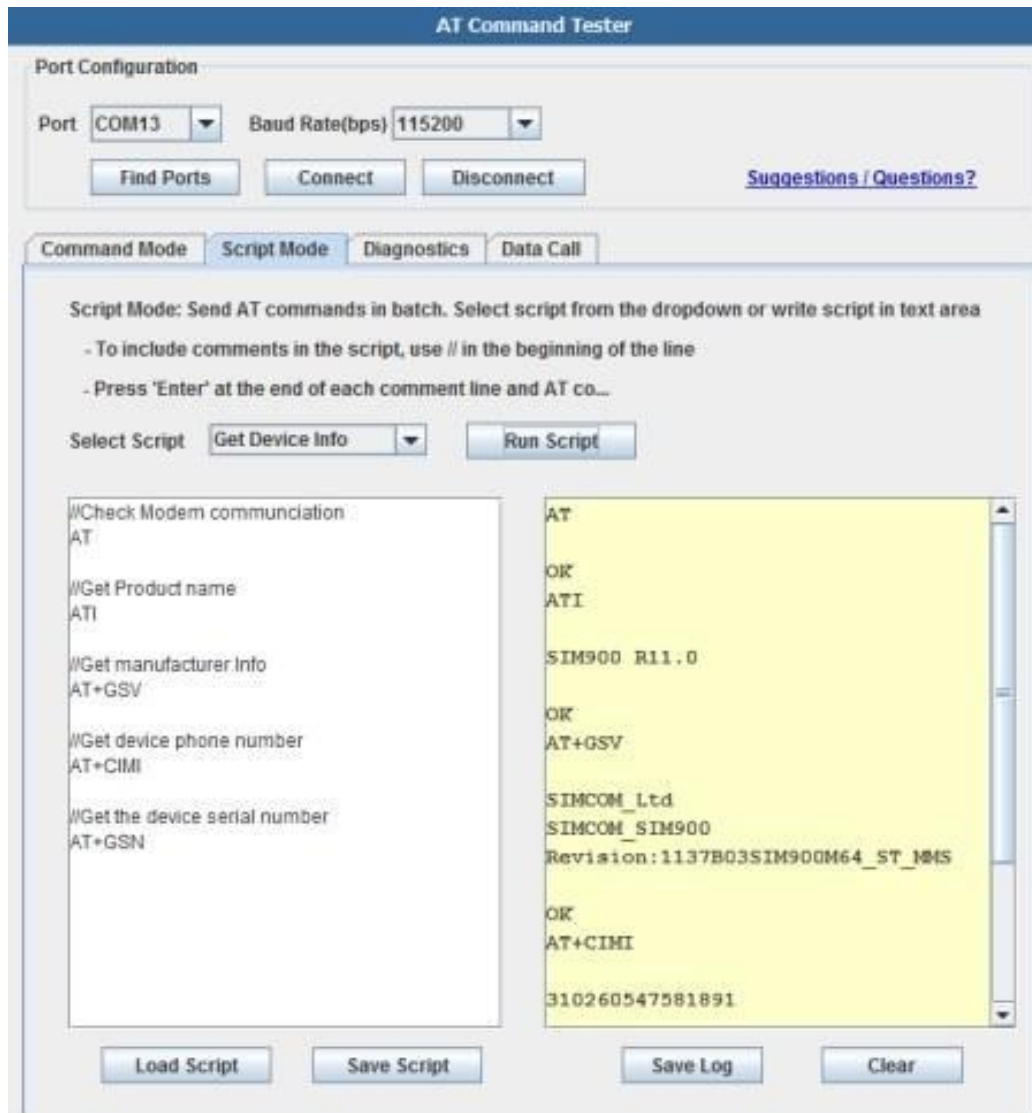


Figure 5.3.7b AT Command Tester Command Mode

Script Mode

Users can send batch of AT commands under the ‘Script Mode’ tab. They can also save and load the script from the local machine. Users can develop their own scripts for specific set of tasks such as call setup, send SMS, HTTP access etc. Users can also include descriptive comments in their script.

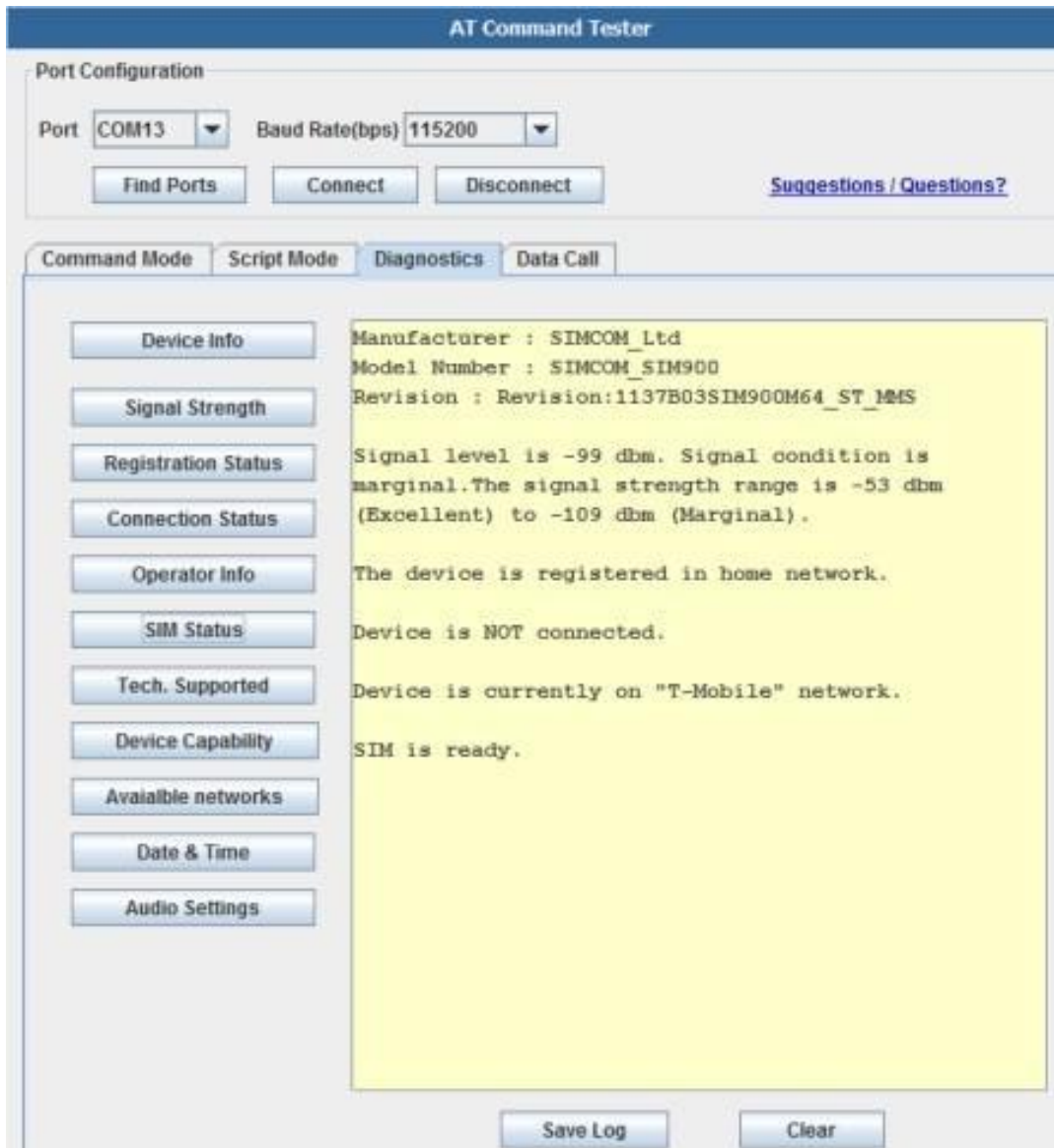


Figure 5.3.7c AT Command Tester Script Mode

Diagnostics

Users can perform basic troubleshooting of the modem under the 'Diagnostics' tab. Here the AT Command Tester tool sends the required AT commands and provides descriptive output about the state of the modem.

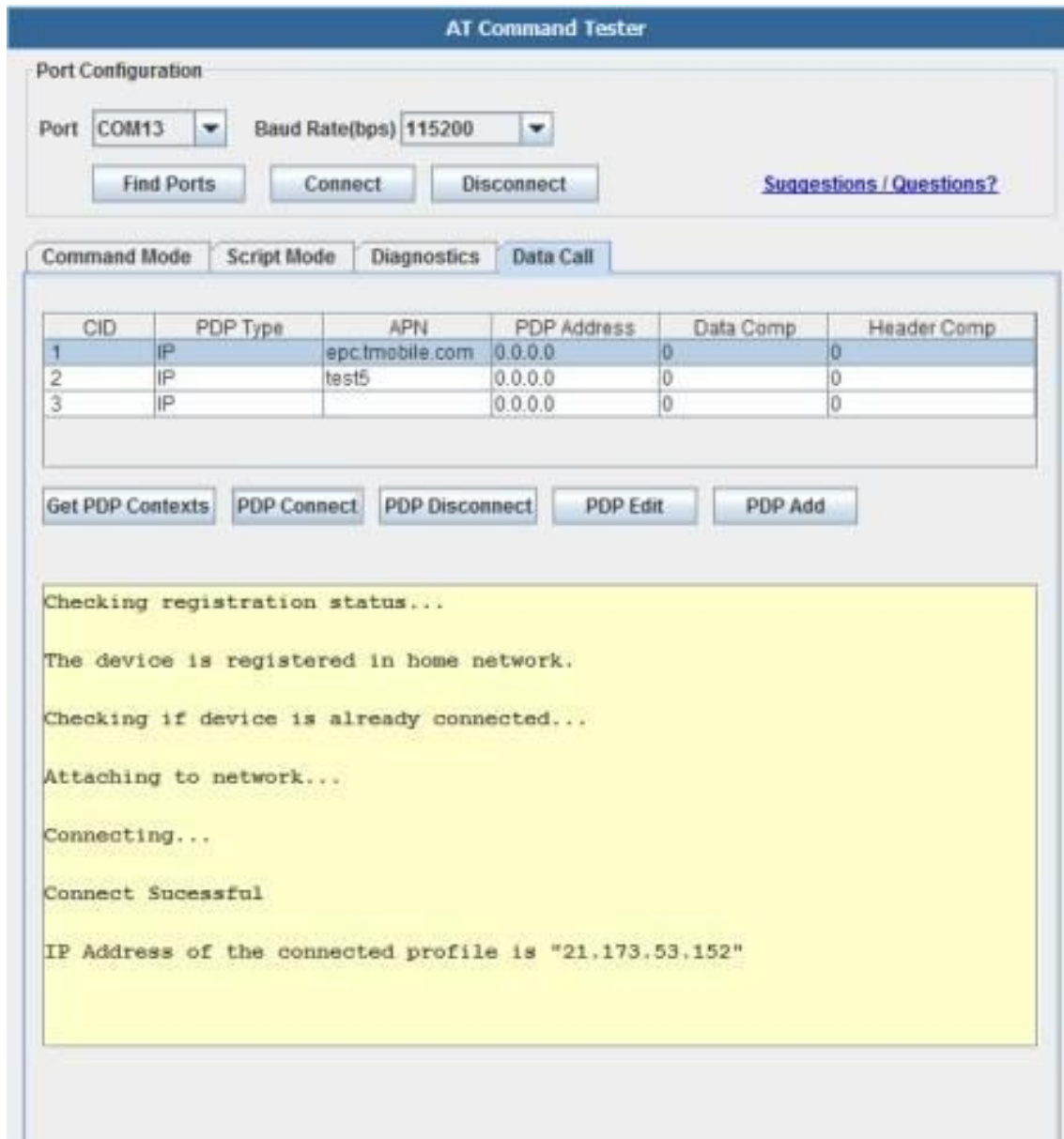


Figure 5.3.7d AT Command Tester Diagnostics Tab

Data Call

The 'Data Call' tab provides the interfaces to setup data call with the GSM network. 'Get PDP Contexts' button will list all the PDP context profiles stored on the SIM. Users can also add or update new PDP context profile. Users can then connect to the selected profile. AT Command Tester will first check whether the device is registered on the network. If so, it will attach and connect to the network with the selected PDP context credentials. More feature additions such as

voice call, SMS, Phonebook functions, HTTP, FTP, TCP/IP are planned for AT Command Tester tool.

Chapter 6

Conclusion

6.1 Conclusion:

We tried to build a smart security system by using the most reliable and efficient components as well as minimize the overall cost of the equipment in order to achieve better output of the system. Beside that we faced many problems to do this project which we tried to overcome. We also have some future plan to add more features in this project.

6.1.1 Limitations

1. By using Solenoid door lock someone can only unlock the door but have to open the door manually.
2. The total system is powered by electricity. When a country wide power failure happens, the system will work on the backup batteries dedicated only to the system, but in case the backup power fails it will restrict entry to the building as door lock system and other components of the system will not work.
3. The face detection system implemented using the raspberry pi saves several images of the same person each time a face is detected even of the admin himself or herself as the system is unable to recognise a specific face.
4. The image and video resolution of the raspberry pi camera is low compared to the digital camera as a result, sometimes, the system is unable to recognize the side faces and sometimes front faces as well. For the system to work at its maximum efficiency, the room has to be well lit, because, in a dimly lit place, the camera is unable to recognize a face properly.
5. Raspberry Pi face detection library available is not that much effective in detecting faces properly.

6. The flame detection system works within 50cm of its radius. Thus, several flame sensors has to be installed depending on the space or area to be covered for efficient use of the system.

6.1.2 Future Implementation

In current system, the door is to be manually pushed open and close after the solenoid magnetic lock is unlocked by authentication. In future, the door will be opened and closed automatically by use of mechanical servos after an authentication is made.

In the face detection system, the video can be improved by using a camera of higher resolution and the detection system can be improved by using a more upgraded face library. By using the upgraded library, a specific face can be detected and stored in the system which will enable us to avoid the recognition of a known face over and over again, and only store image and alert for unknown or unexpected faces. The library will also enable the system to detect the side faces which will be more efficient in terms of security.

The flame sensing system can be implemented using better sensors with a wider range and precision, so that the sensing is more effective and precise and also ensure less number of sensor to be used while implementing it on large area or room.

In future, the face recognition system can be used to restrict the door open switch to be used by any unregistered person and the password will be automatically reseted and the admin will be notified immediately.

A mobile application can also be developed for the system. The system will be connected to the internet. This way, the admin will receive notifications through the mobile application.

References

1. <http://www.robotshop.com/media/files/PDF/ArduinoMega2560Datasheet.pdf>
2. <http://www.asecurelife.com/reasons-to-install-home-security-system>
3. <http://www.inventionhardware.com/diy-projects/use-the-raspberry-pi-camera-to-detect-faces-and-read-emotions-in-pictures>
4. <http://www.impactsecuritysolutions.co.uk/our-services/electronic-security>
5. <https://www.abus.com/eng/Home-Security>
6. <http://www.mediafire.com/file/v1agkrx2q1ocxcw/Proteus+Arduino+Library.rar>
7. <http://www.doityourself.com/stry/install-the-perfect-wireless-home-security-camera-system>
8. <http://www.instructables.com/id/Secret-Knock-Detecting-Door-Lock>
9. <http://www.safewise.com/blog/finding-the-perfect-electronic-door-lock-for-your-home>
10. https://en.wikipedia.org/wiki/Raspberry_Pi
11. <https://www.raspberrypi.org/help/faqs>
12. <https://www.raspberrypi.org/products/camera-module>
13. <http://www.instructables.com/id/Arduino-Modules-Flame-Sensor>

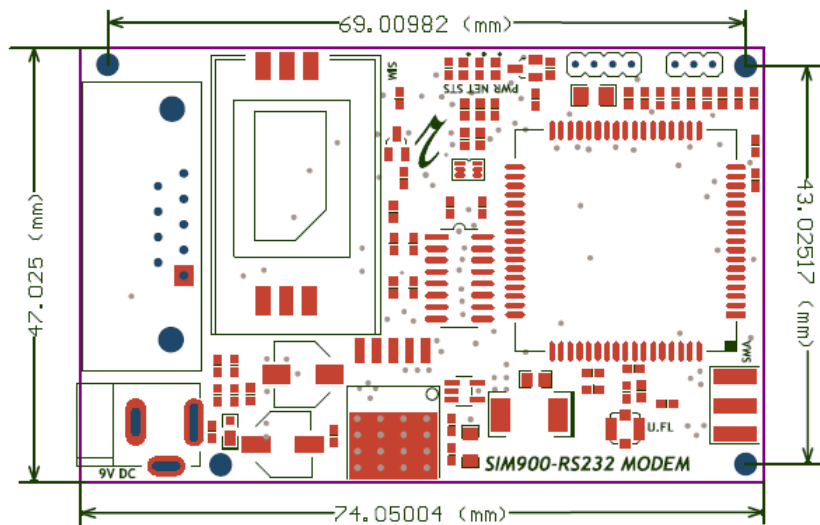
APPENDICES

GSM module:

OPERATING CONDITIONS

Parameter	IN/OUT	Minimum	Maximum	Unit
Supply Voltage - VIN	Input	4.2	13	V
Current Consumption	---	40	590	mA

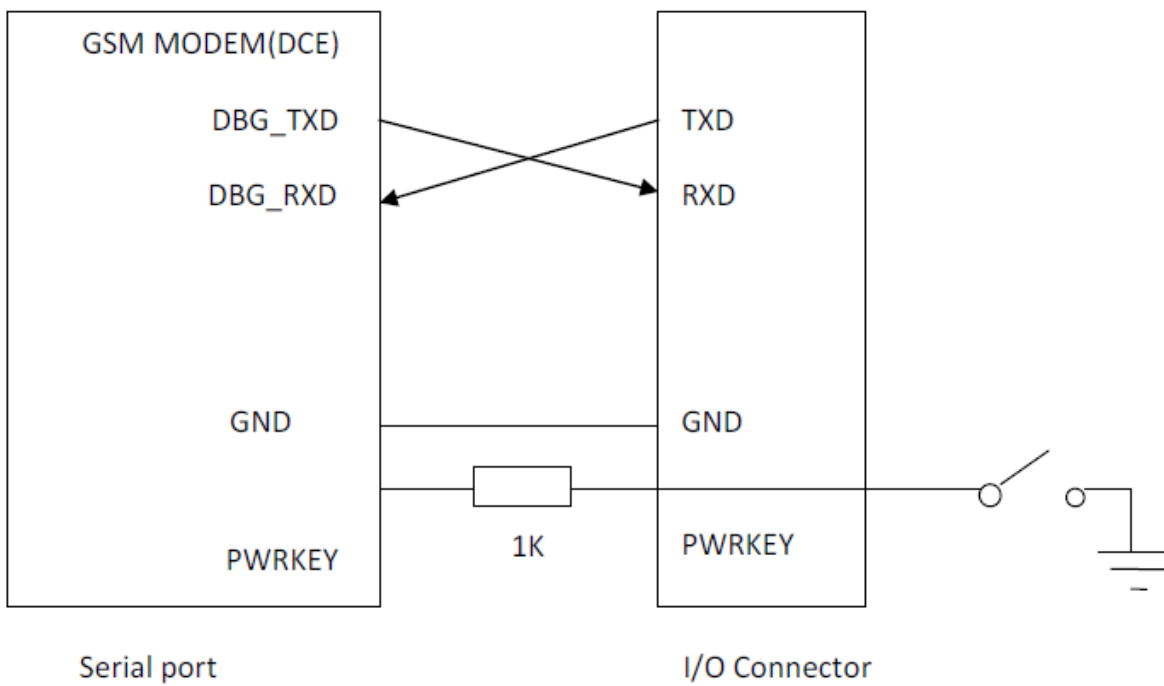
DIMENSIONS



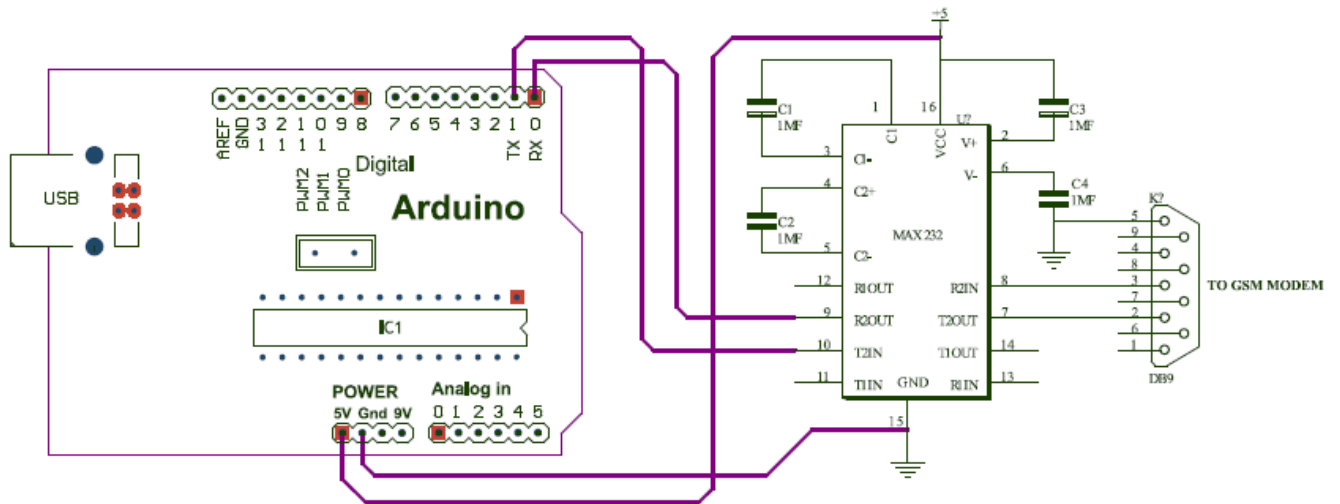
Serial Interface:

	Name	Pin	Function
Serial Port DB9	GND	5	Ground
	CTS	8	Clear to send
	RTS	7	Request to send
	TXD	2	Transmit data
	RXD	3	Receive data

GSM modem upgrading software:



Interfacing Modem to Arduino:



Audio Interfacing:

	Pin Name	Pin Number	Function
AIN/AOUT	MIC	1	Microphone1 input +
	GND	2	Common Ground
	SPK	3	Audio output+

Arduino Mega:

