

A Project Report on

# ADVANCE ANTI-THEFT WITH SMART SUSPECT RECOGNITION SYSTEM

Submitted in partial fulfillment of award of

**BACHELOR OF TECHNOLOGY**

Degree  
in

**COMPUTER SCIENCE & ENGINEERING**

By

PRAKASH AHUJA-1408210093

PRANJAY GUPTA-1408210095

RITIK RANA-1408210106

SANCHIT VARSHNEY-1408210116

SHIVAM SAXENA-1408210121

(2014-2018)

Mr. Shivanshu Rastogi

Assistant Professor

**SUPERVISOR**



IN PURSUIT OF EXCELLENCE

**Department of Computer Science & Engineering  
Moradabad Institute of Technology  
Moradabad (U.P.)**



A Project Report on

# ADVANCE ANTI-THEFT WITH SMART SUSPECT RECOGNITION SYSTEM

Submitted in partial fulfillment of award of

**BACHELOR OF TECHNOLOGY**

Degree  
in

**COMPUTER SCIENCE & ENGINEERING**

By

PRAKASH AHUJA-1408210093

PRANJAY GUPTA-1408210095

RITIK RANA-1408210106

SANCHIT VARSHNEY-1408210116

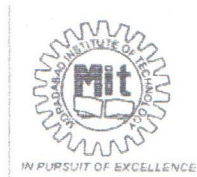
SHIVAM SAXENA-1408210121

(2014-2018)

Mr. Shivanshu Rastogi

Assistant Professor

SUPERVISOR



Head  
Computer Sci & Engg Department  
Moradabad Institute of Technology  
Moradabad-24400

Department of Computer Science & Engineering  
Moradabad Institute of Technology  
Moradabad (U.P.)

## CERTIFICATE

Certified that the Project Report entitled "ADVANCE ANTI THEFT WITH SMART SUSPECT RECOGNITION SYSTEM" submitted by Prakash Ahuja(1408210093), Pranjay Gupta (1408210095), Ritik Rana (1408210106), Sanchit Varshney(1408210116), Shivam Saxena (1408210121) is their own work and has been carried out under my supervision. It is recommended that the candidates may now be evaluated for their project work by the University.

Date: 12/05/2018

Shivam Saxena  
01/06/2018



Shivanshu Rastogi

(PROJECT GUIDE)

Assistant Professor

CSE Department

Head  
Computer Sci. & Engrg. Department  
Moradabad Institute of Technology  
Moradabad-244001




## ABSTRACT

Security has become one of the prominent issue of today's world. It is one of those attribute which is required from a very basic to an extremely high protection measure. We are living in a society where it doesn't take much time to breach an application which needs to be secured. Though, there are various protocols as well as customized products which are coming in trends for providing a standard level of security but somehow these systems are not capable enough to resist the ongoing theft or breachment of security. We do have CCTV surveillance, motion detect ion, biometric systems, etc. but still have some mishappening occurs, we just left with some of the evidence in the form pictures, videos and audios. So this situation needs a smarter system which not only captures the suspect and his activities but also make the legitimate user aware about it.

To overcome this we introduce the Arduino based security which is based on microcontroller and sensor. This technology provides exciting and new opportunities to increase the connectivity of devices within the home or commercial for the purpose of security. In this project, the main focus on sensor

Head  
Computer Sci. & Engg. Department  
Moradabad Institute of Technology  
Moradabad-244001






based security in which there are sensors, camera, motion detectors, and embedded kits are used. A wireless interface are used to detect and identify visitors and send an email or an alert message about the current home environment status via GSM network automatically to the home owner's mobile phone or any communication devices. The device can be placed at any remote location which can be easily accessed by the user and give his/her immediate response according to the respective situation. For this, it uses a microcontroller for the system control, GSM technology for communication and sends SMS containing the emergency message and GPS location of the sender.

  
**Head**  
Computer Sci & Engg Department  
Moradabad Institute of Technology



## ACKNOWLEDGEMENT

It gives us immense pleasure and privilege to acknowledge our deepest sense of gratitude towards all those who helped us in the successful execution of this project. We whole heartedly venerate our guide Mr. Shivanshu Rastogi (Assistant Professor), our project committee members Mr. Rakesh Ahuja (Head of the Department), Mr. Himanshu Agarwal (Assistant Professor), Mr. Manoj kr. Singh (Assistant Professor), Mr. Praveen Saini (Assistant Professor) and Mr. Ranjan Bhaghel (Assistant Professor) for their strenuous guidance. With their cooperation and encouragement helped us to bring this project in an elegant manner. We also express our deep sense of gratitude to our parents and almighty God for their being blessings without which this report was not possible.


 PRAKASH AHUJA  
 PRANJAY GUPTA  
 RITIK RANA  
 SANCHIT VARSHNEY  
 SHIVAM SAXENA

Head


Computer Sci & Engg Department  
 Moradabad Institute of Technology  
 Moradabad-744001

## TABLE OF CONTENT

CHAPTER NO.	CONTENTS	PAGE NO.
	ABSTRACT	iii
	TABLE OF CONTENT	vi
	LIST OF FIGURES	viii
	LIST OF TABLES	x
<b>CHAPTER 1.</b>	<b>LITERATURE SURVEY</b>	<b>11-18</b>
	1.1 Machine to Machine Communication Based Smart Home Security System	11
	1.2 Android Interface Based GCM Home Security System	15
	1.3 Laser Based Security System using Sensor Network	18
<b>CHAPTER 2.</b>	<b>OVERVIEW OF PROJECT</b>	<b>19-38</b>
	2.1 Introduction	19
	2.2 Project Requirement	20
	2.3 Hardware Description	20
	2.3.1 Arduino UNO	20
	2.3.2 SIM 900A Module GSM	22
	2.3.3 IP Camera	24
	2.3.4 Buzzer	28
	2.3.5 Laser	29
	2.3.6 Photoresistor	30
	2.3.7 Smart Phone	31
	2.4 Software Description	33

  
**Head**  
 Computer Sci. & Engrg. Department  
 Moradabad Institute of Technology  
 Moradabad-244001


2.4.1 Embedded C	33
2.4.2 Arduino IDE	34
2.4.3 Android Studio	37
<b>CHAPTER 3. MODULES</b>	<b>39-43</b>
3.1 Laser Mesh (Tripwire)	39
3.2 GPS and Remote Control	40
3.2.1 GSM	41
3.2.2 Working Explanation	42
<b>CHAPTER 4. SNAPSHOT</b>	<b>44-56</b>
4.1 Laser Mesh(Frontend)	44
4.1.1 Laser Mesh is ON	45
4.1.2 Laser Mesh is OFF	46
4.2 Hardware Circuit(Backend)	47
4.3 Integrated System	48
4.4 Android Application	49
<b>CHAPTER 5. ADVANTAGES AND DISADVANTAGES</b>	<b>57-59</b>
5.1 Advantages	57
5.2 Disadvantages	58
<b>CHAPTER 6. CONCLUSION</b>	<b>60</b>
<b>CHAPTER 7. FUTURE ASPECTS</b>	<b>61</b>
<b>REFERENCES</b>	<b>62</b>

  
**Head**  
 Computer Sci & Engg Department  
 Moradabad Institute of Technology  
 Moradabad-744001




## LIST OF FIGURES

Figure No.	Figure Name	Page No.
1.1	NFC	13
1.2	PIR	13
1.3	Arduino Module	14
1.4	GSM Module	15
1.5	Object Motion detection	17
2.1	Arduino UNO	21
2.2	SIM 900A GSM Module	23
2.3	IP Camera	27
2.4	Buzzer	28
2.5	Laser Module	29
2.6	LDR	31
2.7	Smart Phone	33
2.8	Arduino IDE	37
2.9	Android Studio	38
3.1	Laser Mesh (Tripwire)	40
3.2	GPS and Remote Control	41
4.1	Laser Mesh (Front end)	44
4.2	Laser Mesh is ON	45
4.3	Laser Mesh is OFF	46
4.4	Hardware Circuit (Backend)	47
4.5	Integrated System	48
4.6	Home Screen	49

  
**Head**  
 Computer Sci. & Engrg. Department  
 Moradabad Institute of Technology  
 Moradabad-244001

4.7	Camera Surveillance	50
4.8	Emergency Message Sender	51
4.9	Add Emergency Contact	52
4.10	Settings Activity	53
4.11	New Pincode Activity	54
4.12	Lock Screen	55
4.13	Change Number Activity	56



**Head**  
Computer Sci. & Engg. Department  
Moradabad Institute of Technology  
Moradabad-744001.

## LIST OF TABLES

Table No.	Table Name	Page No.
3.1	Activation of Laser and Buzzer	42

Head

Computer & Engg. Department  
Moradabad Institute of Technology  
Moradabad-244001.



# CHAPTER 1

## LITERATURE REVIEW

### 1.1 Machine-to-machine Communication Based Smart Home Security System

Suddenly is a rapid growth of burglary and theft since last few years that has been threatening the vulnerability of traditional home security systems. In this research, the authors develop a machine-to-machine (M2M) communication based smart home security system. Here a six level home security system (HSS) has been develop which control responses against unwanted burglars and intruders. The first security level uses Near Field Communication (NFC) tag, the second level uses a secured password system and the third level uses fingerprint authentication.

After that, a GSM module embedded with the proposed HSS sends the logged password to a remote server via M2M communication. The server encrypts the password and notifies the homeowner via an android based mobile application whether the person is an authenticated person or not. Many security systems has a functionality of door opening but not of door closing.

Here the 6 layer security system has a simple integrated and embedded form design. An electro-mechanical lock designed in this way that it can be opened even when the power is turned off. The design also includes options of password changing and triggering the alarm circuit when the wrong password is provided 4-5 times.

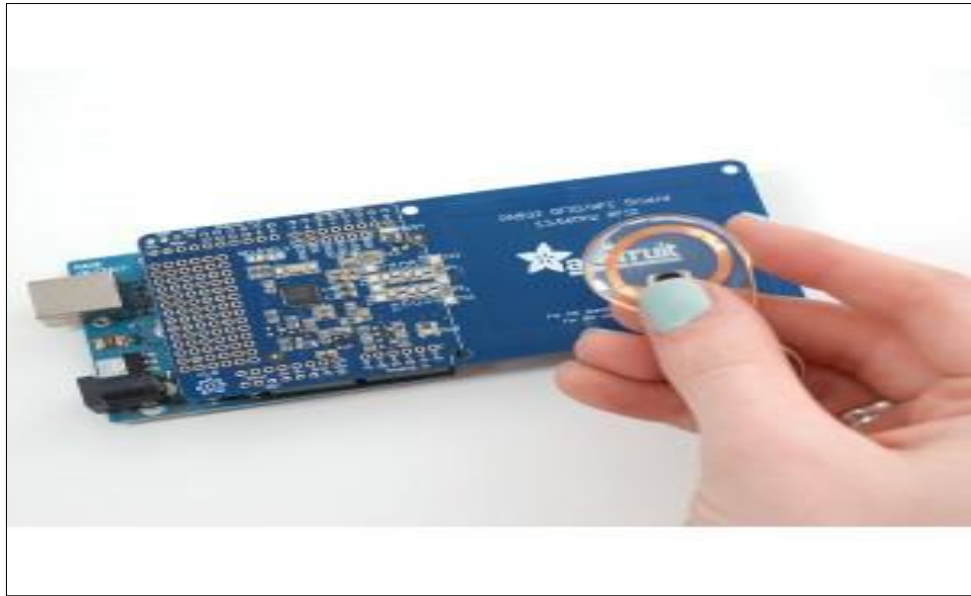
The door will be opened automatically for a valid NFC Tag ,password, and fingerprint by a servomotor coupled with a lock in its shaft. If an unauthorized person wants to access a room he must have an NFC tag, if he has it then system will asks for password and fingerprint. For any invalid user with 4-5 consecutive wrong trials for the

password in the keypad, the system will identify the user as malignant and generates the emergency alarm but if he enters the room without these three protections for example he breaks the password and fingerprint, then the PIR sensor works and sounds the alarm. If tag, password and fingerprint match, then a notification from the GSM module of the HSS is transmitted to a remote server via M2M communication.

After that, the server sends the login alert message to the cellphone of the homeowner via an android application. After receiving the message, the owner can easily identify who is trying to access the home, and whether they are an authenticated user or not. In this way maximum security is ensured with the help of proposed HSS. Due to automation facility no physical labor is required to monitor the home condition.

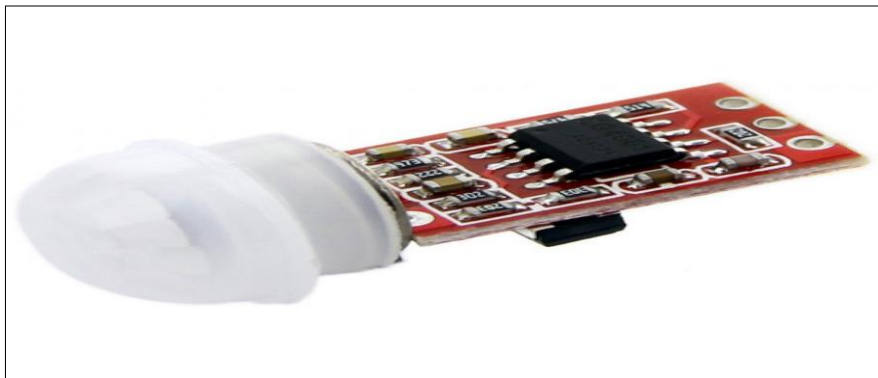
Machine-to-machine (M2M) communication takes place between embedded devices at one side and at another side a network server is present. The M2M for HSS is divided into types. First is tracking for sensing data like password, fingerprint, second is logging for scheduled data communication. Then The final type is Notifications to notify and alert users in real time to take decisions.

- **NFC:** Near Field Communication (NFC) is a wireless non-contact short-distance communication of radio-frequency electromagnetic waves to transfer data automatically for identifying and tracking tags attached near the shield. The tag stores information electronically, in a non-volatile memory. Tags are powered by electromagnetic induction within a small distance or by a local power source such as a battery. In this research, a lock has been designed which is operated both electrically and mechanically. The lock is coupled with the shaft of the servo motor, used for precise angular position. The shaft is connected to a top portion of the lock mechanically. The inner portion of the lock is operated by a compression spring. When the servo's shaft rotates clockwise, the spring is compressed and the door opens. Conversely, when the servo releases power, the spring is decompressed and the door closes. The lock also carries the advantage of opening the door with a mechanical key which can be designed by the manufacturer.



**Fig 1.1 NFC**

- **PIR:** The passive infrared (PIR) sensor can detect levels of infrared radiation as it is made of a pyroelectric sensing coating. It detect a change of motion so the sensor in a motion detector is actually split into two halves and it is not supposed to detect the average IR level. Sensor remain idle when both slots receive the same amount of IR.



**Fig 1.2 PIR**

- **Arduino Module:** The monitoring and controlling of the embedded equipment over the Internet can be mechanized by following certain network architectural design strategies and by applying the hardware implementations. The data capturing and then transmitting of smart camera augmented with Arduino over the network is through



mobile application. The virtual home security System is a software developed in Matlab and Android. All communication and instructions are checked for security and safety, in the virtual environment, before implementation in the real home environment. If any visitors arrive, the system sends an appropriate images to the home owner for further action. The owner can directly login and interact with the embedded device in real time and send his/her response for further actions to be performed. In the development of home security Arduino has been used. The communication between the sink module and control module is performed from side to side in a Arduino module. It takes analog reading of the sensors making the system more versatile. Then it averages the two readings to get a center value. Any reading above this center value is considered high and that below as low. This process helps reduce the environmental effects on the sensors. The transformation of control information between the Arduino and network is executed by a program at the IoT application gateway, as the network does not have the architecture to communicate with internet protocols. This IOT application consists of a program that burns in the Arduino board and then using this accordingly.



**Fig 1.3 Arduino Module**

- **GSM Modem:** A GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone. When a GSM modem is connected to a computer, this allows the computer to use the

GSM modem to communicate over the mobile network. While these GSM modems are most frequently used to provide mobile internet connectivity, many of them can also be used for sending and receiving SMS and MMS messages. A GSM modem can be a dedicated modem device with a serial, USB or Bluetooth connection, or it can be a mobile phone that provides GSM modem capabilities.



**Fig 1.4 GSM Modem**

## **1.2 Android Interface based GCM home security system using object motion detection**

Video surveillance systems are essential for crime investigation and the quantity of cams introduced into wider public space is blowing up. Numerous robotised frameworks have been created which illuminates the holder in a remote area about any brake or attempt to barge in the household. In addition GSM/GPRS facilities of handset are also used. The android applications which interprets the message a cell phone gets a possible interruption and in this manner a message which triggers the alert in the remote house making others mindful of the possible interruption. After the intruder's movement identification system will send GSM ready for the android mobile application.

i. This Step involves user authentication for application basically it is a user validation method for identifying the user and confirming that the user is confirming is permitted to make to some confined administration. This module incorporates with the username and the secret word for the validation to apply the acceptance.

ii. This step involves detecting image using Cauchy distribution model. This model in used to acknowledge the moment in a specified field by utilizing Cauchy appropriation model and absolute differential estimation motion detection can be carried out. Absolute differential estimation is utilized to attend at the foundation age and approaching feature outline if any progressions happen in an approaching video frame. The picture element of the moving object in the distinguished approaching video frame Cauchy distribution model is used to recognize this.

iii. This step incorporates with sending the GSM alert it is a foundation step of our approach. Whenever movement, distinguished that picture is preserved on the server and the waiter will inform the Google server. GCM alert will be send to the android application client with the help of google server. Google Cloud Messaging for Android (GCM) is an administration that allows you to send data from your server to your clients' Android-controlled appliance. This can be a lightweight application which tell with the help of SMS. This is the way by which these segments collaborate:

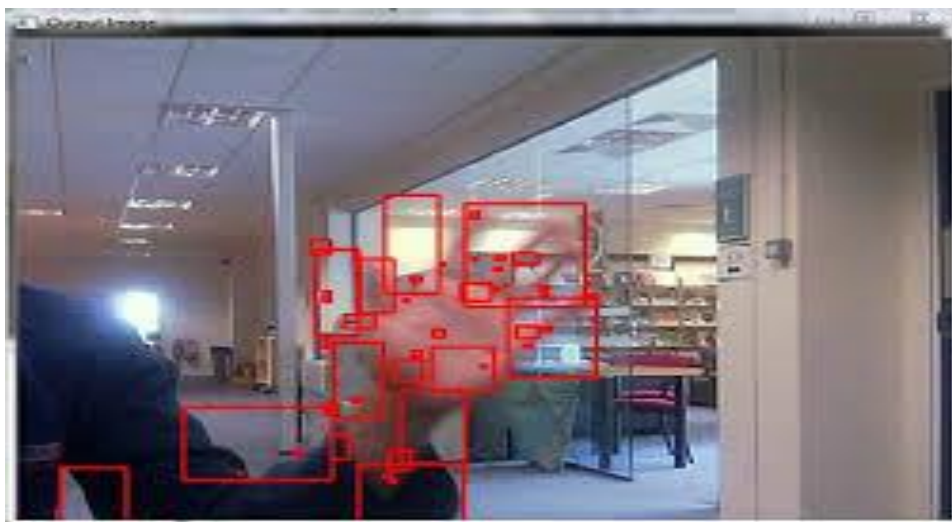
- Google-gave GCM Connection Servers take messages from a third gathering application server and transmit these messages to a GCM-empowered Android application (the "customer application") playing on a gadget. As of now Google gives association servers with HTTP and XMPP.
- The third Party Application Server is a part that you execute to work with your picked GCM association server(s). Application servers send messages to a GCM association server; the association server enqueuers and stores the message, and after that sends it to the gadget when the gadget is on the web. For more data, see Implementing GCM Server.
- The Client App is a GCM-empowered Android application running on a gadget. To get GCM messages, this application must enrol with GCM and get an enrolment ID. In the event that you are utilizing the XMPP (CCS) association server, the customer application can send "upstream" messages over to the association server. For more information on the most proficient method to fulfil the client application, see Implementing GCM Client.



iv. This step will deal with viewing the detected image with the help of the android application the warning i.e. through GCM taking into account venture ID which is enlisted in the google account. After getting the GCM ready from the waiter to the application and the customer needs to validate for the application The picture can be determined utilizing the URL which is drawn from the GCM alert. A moving security cam is situated to screen the range to recognize a development in that specific field. Two picture frames are required to identify any development. The initial form is called the reference frame, that will speak to the reference age values of the examination vision, the second frame experienced as the info age, which will holds back the moving point.

This system has many advantages as it is not just by simply seeing the sight image, also see the whole cut of what happened and what has been caught. The system has a unique feature in which it sends GSM ready on the double there is any kind of verity in the caught pixel. The system will have an high accuracy in the captured image and whenever the object is detected immediately the user will receive an alert sms the captured photo will be stored in the server and they can be retrieve at the time of motion detection which can be seen by the user or we can say owner of the home will help of the android mobiles.

The Cauchy distribution model algorithm is used to compare reference frame with incoming frame ,if there is no change in the incoming frame then the image won't be sent to the server.



**Fig 1.5 Object motion detection**

### **1.3 LASER Based Security System Using Wireless Sensor Network**

The LASER detector circuit is a voltage divider network consisting of a LDR and a series resistor. The junction of the two is fed into an analog pin of the Arduino board. Thus the Arduino takes analog reading of the sensors making the system more versatile. It takes two initial reading of the sensors, one with LASERs on and the other with LASERs turned off. Then it averages the two readings to get a center value. Any reading above this center value is considered high and that below as low. This process helps reduce the environmental effects on the sensors.

As stated above each sensor node consist of an array of six LASERs and LDRs. Generally a poacher intends to use huge fishing nets to steal fishes from the pond. When any object obstructs the path of the LASER from falling on the LDR; the resistance of the LDR increases. This makes the corresponding pin of the Arduino low. Arduino than calculates the number of LASERs obstructed.

The GPRS/GSM gateway consists of an nRF24L01 module which is set to receive mode. It continuously scans for data from the sensor nodes. It scans each sensor serially. When an intrusion occurs a definite character is send from the sensor nodes.

For testing the level of security we have implemented our system on six dummy ponds. The dummy ponds were placed at approximately 30 meters away from the GSM/GPRS gateway in an open field. We used six LASER and LDR units to verify the security conditions as stated above. The LASERs used had a maximum output power of 5 milli-watts and 650 nano-meters wavelength.

When two or less LASERs were obstructed, the alarm was sounded. When the number of LASER obstructed was more than two, a call was given to a desired number saved in the phonebook. The nRF24L01 worked fine within the given range. Successful communications was established between the sensors and GPRS gateway.

## **CHAPTER 2**

### **OVERVIEW OF PROJECT**

#### **2.1 Introduction**

Security has become one of the prominent issue of today's world. It is one of those attribute which is required from a very basic to a extremely high protection measure. We are living in a society where it doesn't take much time to breach an application which needs to be secured. Though there are various predefined protocol as well as customised products which are coming in trends for providing a standard level of security but somehow these systems are not capable enough to resist the ongoing theft or breachment of security. We do have CCTV surveillance, motion detection ,biometric systems etc but still if some mishappening occurs, we just left with some of the evidence in the form of pictures, videos and audios. So this situation needs a smarter system which not only captures the suspect and his activities but it should also make the legitimate user aware about it.

To overcome this we introduce Arduino based security w hich based on microcontroller and sensor. This technology provides exciting and new opportunities to increase the connectivity of devices within the home or commercial for the purpose of security. In this project focused on sensor based security in which there are sensors, camera, motion detectors, and embedded kits are used. A wireless interface are used to detect and identify visitors and send an email and/or an alert message about the current home environment status via GSM network automatically to the home owner's mobile phone or any communication devices. The device can be placed at any remote location which can be easily accessed by the user. It uses a microcontroller for system control,

GSM technology for communication and sends SMS containing the emergency message and the GPS location of the sender.

## **2.2 Project Requirement**

The project can be better described by dividing it into two categories, namely

1. Hardware
2. Software

## **2.3 Hardware Description**

### **2.3.1 Arduino UNO**

The Arduino UNO is a widely used open-source microcontroller board based on the ATmega328P microcontroller and developed by Arduino.cc. The board is equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (shields) and other circuits. The board features 14 Digital pins and 6 Analog pins. It is programmable with the Arduino IDE (Integrated Development Environment) via a type B USB cable. It can be powered by a USB cable or by an external 9 volt battery, though it accepts voltages between 7 and 20 volts. It is also similar to the Arduino Nano and Leonardo.

The hardware reference design is distributed under a Creative Commons Attribution Share-Alike 2.5 license and is available on the Arduino website. Layout and production files for some versions of the hardware are also available. "Uno" means one in Italian and was chosen to mark the release of Arduino Software (IDE) 1.0. The Uno board and version 1.0 of Arduino Software (IDE) 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. The ATmega328 on the Arduino Uno comes preprogrammed with a bootloader that allows to upload new code to it without the use of an external hardware programmer. It communicates using the original STK500 protocol.



The Uno also differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. The Arduino UNO is generally considered the most user-friendly and popular board, with boards being sold worldwide for less than 5\$.



**Fig 2.1 Arduino UNO**

- LED: There is a built-in LED driven by digital pin 13. When the pin is HIGH value, the LED is on, when the pin is LOW, it's off.
- VIN: The input voltage to the Arduino/Genuino board when it's using an external power source (as opposed to 5 volts from the USB connection or other regulated power source). You can supply voltage through this pin, or, if supplying voltage via the power jack, access it through this pin.
- 5V: This pin outputs a regulated 5V from the regulator on the board. The board can be supplied with power either from the DC power jack (7 - 20V), the USB connector (5V), or the VIN pin of the board (7-20V). Supplying voltage via the 5V or 3.3V pins bypasses the regulator, and can damage the board.
- 3V3: A 3.3 volt supply generated by the on-board regulator. Maximum current draw is 50 mA.
- GND: Ground pins.
- Reset: Typically used to add a reset button to shields which block the one on the board.

### 2.3.2 SIM 900A Module GSM GPRS

This is an ultra compact and reliable wireless module. The SIM900A is a complete Dual-band GSM/GPRS solution in a SMT module which can be embedded in the customer applications. Featuring an industry-standard interface, the SIM900A delivers GSM/GPRS 900/1800MHz performance for voice, GSM has been used due to its high availability, coverage and security.

AT commands can be sent through the GSM network and this controls the devices. Messages are sent by the device to the user through SMS as well. This system can however incur additional costs for the SMS. There is no UI that the user can use to control the device. This system has the disadvantage of not being able to program the devices. Also SMS relies on upon the networks and there is a possibility of delayed delivery.

The system doesn't have any state information related to the devices and expects the user to keep track of it. The system is depicted as an M2M system. It utilizes GSM for communication. GSM offers options for M2M which include Dual Tone Multi Frequency (DTMF), SMS and General Packet Radio Service (GPRS). This system chooses to use the SMS along with AT (attention) commands. It has a PC as a centre of commands.

A GSM dial-up and communication system is embedded in the PC. Visual C++ is used for implementation. The PC decodes the received messages via SMS and performs the commands required. It is a system that can be programmed for the required application as per requirements. The PC decodes the received messages via SMS and performs the commands required. It is a system that can be programmed for the required application as per requirements.

SMS, Data, and Fax in a small form factor and with low power consumption. With a tiny configuration of 24mmx24mmx3mm, SIM900A can fit in almost all the space requirements in user applications, especially for slim and compact demand of design.

The SIM900A module has 6pins in which two pins for Vcc and Gnd and the rest are 3VR&3VT(3volt Rx &Tx) and 5VR,5VT(5volt Rx &Tx) and the connections are made as follows:

- Vcc to 5V
- Gnd to Gnd
- 5VR digital pin 7
- 5VT digital pin 8

Before getting into the program part, we need to look into the AT commands which are discussed in the following used by this module. With the help of these AT commands, the user can send or receive messages, make a call and so on.

The SIM900 is a complete Quad-band GSM/GPRS solution in a SMT module which can be embedded in the customer applications. Featuring an industry-standard interface, the SIM900 delivers GSM/GPRS 850/900/1800/1900MHz performance for voice, SMS, Data, and Fax in a small form factor and with low power consumption. SIM900 can fit almost all the space requirements in your M2M application, especially for slim and compact demand of design.



**Fig 2.2 SIM 900A GSM Module**

This is a GSM/GPRS-compatible Quad-band cell phone, which can be used not only to access the Internet, but also for oral communication (provided that it is connected to a microphone and a small loud speaker) and for SMSs. Externally, it looks like a big package (0.94 inches x 0.94 inches x 0.12 inches) with L-shaped contacts on four sides so that they can be soldered both on the side and at the bottom. Internally, the module

is managed by an AMR926EJ-S processor, which controls phone communication, data communication (through an integrated TCP/IP stack), and (through an UART and a TTL serial interface) the communication with the circuit interfaced with the cell phone itself.

### **2.3.3 IP Camera**

An Internet Protocol camera, or IP camera, is a type of digital video camera commonly employed for surveillance, and which, unlike analog closed-circuit television (CCTV) cameras, can send and receive data via a computer network and the Internet. Although most cameras that do this are webcams, the term IP camera or netcam is usually applied only to those used for surveillance that can be directly accessed over a network connection.

An IP camera is typically either centralized (requiring a central network video recorder (NVR) to handle the recording, video and alarm management) or decentralized (no NVR needed, as camera can record to any local or remote storage media). The first centralized IP camera was Axis Neteye 200, released in 1996 by Axis Communications.

IP cameras are typically available at resolutions from 0.3 (VGA resolution) to 29 megapixels. As in the 21st century, there has been a shift in the consumer TV business towards high-definition (HD) resolutions (eg. 1080P (Full-HD), 4K resolution (Ultra-HD) and 16:9widescreen format). Previous generations of analog CCTV cameras use established broadcast television formats (eg. Common Intermediate Format (CIF), NTSC, PAL, and SECAM). IP cameras may differ from one another in features and functions, video encoding (compression) schemes, available network protocols, and the API to be used by video management software.

In order to address issues of standardization of IP video surveillance, two industry groups were formed in 2008: the Open Network Video Interface Forum (ONVIF) and the Physical Security Interoperability Alliance (PSIA). While the PSIA was founded by 20 member companies including Honeywell, GE Security and Cisco, and ONVIF was founded by Axis Communications, Bosch and Sony, each group now has numerous



members. Cameras and recording hardware operating under the same standard will be able to work with each other, as each device will be communicating in the same language.

It's become incredibly easy to check in on your young child and her nanny from your desk at work -- or to monitor your business from your laptop at home, all in real time. Internet cameras allow you to connect to the internet via a broadband network and remotely view live video from any web browser anywhere in the world. Once your system is set up, the only requirement is Internet access. You can even monitor multiple video cameras or DVRs from your tablet or smartphone. Some internet cameras require a physical cable connection, others are wireless and transmit their data via radio frequency (RF) signals or over a local WiFi network. Think of internet cameras as mini computers that happen to have sophisticated optics built in.

They come with their own software and need to be configured to a network in order to function. The network configuration is a relatively simple process for many devices; generally set up is no more complex than configuring a Wi-Fi network. While some models require a good working knowledge of Internet technology to get them up and running, that's becoming more the exception than the rule. Many cameras now come with their own apps, which make recording and viewing video on the web even easier. These versatile devices come in a number of "form factors." Many look like traditional security cameras, but consumers have demanded hidden cameras (also known as nanny cams) with webcam capability -- and the market has responded. Internet cams are now discreetly hidden in a wide variety of form factors, from a Bluetooth speaker, to a smoke detector, to an air freshener. Instead of transmitting video over a video cable to a monitor or DVR, an internet camera transmits digital video over a data connection: ethernet, USB, WiFi, etc.

Everything required to transfer images over the network is built into the unit. It is connected directly to the network, just like any other network device, like a printer or scanner. Depending on what type of camera it is, it may save video to an attached memory source, connect to another device on the network for storage, or stream captured video to the internet. An internet camera captures images the same way any digital camera does. What makes it different is its ability to compress the files and transmit them over a network. If a building is equipped with a network, the necessary infrastructure is already in place to install network cameras.

If adding one or a few cameras, a user may use a decentralized network camera, one that has its own control interface and storage medium built in. When installing multiple network cameras it can be wise to use a centralized network camera, which requires a network video recorder (NVR). An NVR is a program that can store video from network cameras and allow for viewing of multiple cameras at once. It is similar to a DVR, but while a traditional DVR is responsible for encoding and processing video from component cameras, an NVR depends on the cameras to encode their video, simply storing it and allowing for centralized remote viewing. NVR software can be installed on a dedicated device with its own operating system or on an existing computer.

There are hybrid systems available that can accept both IP and analog inputs. These will often allow analog cameras to be viewed remotely along with any network cameras. Digital Image resolution is measured in pixels. The more detailed an image is, the more pixels it is made up of, and therefore the more data it contains. Detailed images require more space on a hard disk and more bandwidth for transmission. To transmit images over a network, data must be compressed to avoid consuming too much bandwidth. If bandwidth is limited, lowering the frame rate or accepting a lower image quality can radically reduce the size of video files.

A number of compression standards exist that deal with the trade off between frame rate and image quality in different ways, but the most common has become h.264/MPEG-4, otherwise known as AVC (Advanced Video Coding). When you have a device on a network, you can access it by entering the IP (Internet Protocol) address into a web browser. Internet service providers (ISPs) supply a dynamic IP address to most customers.

A dynamic IP address is like a phone number that changes every time you hang up your phone, while a static IP address never changes. Only your ISP can provide you with a static IP address and they will usually charge a monthly fee for that service. In order for you to gain consistent access to your network cameras you will need a static IP address. If your ISP is unable to provide you with a static IP, there are third party services that can provide a virtual static IP address. Many are free to use, and a simple web search will provide multiple options. Internet cameras go by a lot of different names. You might hear

them referred to as IP or "internet protocol" cams, "network cameras," or "webcams." Whatever you choose to call it, an internet cam is a camera that sends and receives data over a local area network (LAN) and/or the internet. While it is technically possible, using dial up to host video is virtually impossible. The biggest issue is that the bandwidth provided is insufficient for streaming video.



**Fig 2.3 IP Camera**

Potential benefits of IP cameras differ from previous generation analog cameras which transmitted video signals as a voltage, whereas IP camera images are sent using the transmission and security features of the TCP/IP protocol. Some advantages to this approach include:

- Two-way audio via a single network cable allows users to listen to and speak to the subject of the video (e.g. a clerk assisting a customer through step-by-step instructions).
- The use of a Wi-Fi or wireless network.
- Distributed artificial intelligence (DAI) as video analytics can be placed in the camera itself allowing the camera to analyze images.
- Secure data transmission through encryption and authentication methods such as WPA or WPA2, TKIP or AES.
- Remote accessibility allowing live video to be viewed from any device with sufficient access privileges.

- Power over Ethernet (PoE) to supply power through the ethernet cable and operate without a dedicated power supply.

### 2.3.4 Buzzer

A buzzer or beeper is an audio signaling device, which may be mechanical, electromechanical, or piezoelectric (piezo for short). Typical uses of buzzers and beepers include alarm devices, timers, and confirmation of user input such as a mouse click or keystroke. A buzzer or beeper is an audio signaling device, which may be mechanical, electromechanical, or piezoelectric (piezo for short). Typical uses of buzzers and beepers include alarm devices, timers, and confirmation of user input such as a mouse click or keystroke

A piezoelectric element may be driven by an oscillating circuit or other audio signal source, driven with a piezoelectric audio amplifier. Sounds commonly used to indicate that a button has been pressed are a click, a ring or a beep.

A piezoelectric buzzer/beeper also depends on acoustic cavity resonance to produce an audible beep. An Arduino can be used to switch the buzzer on and off. It could be used in an alarm circuit or as an audible indicator that a keypad key is pressed. Because the buzzer draws more current than the maximum current that an Arduino pin can deliver, it is necessary to connect the buzzer to Arduino.



**Fig 2.4 Buzzer**



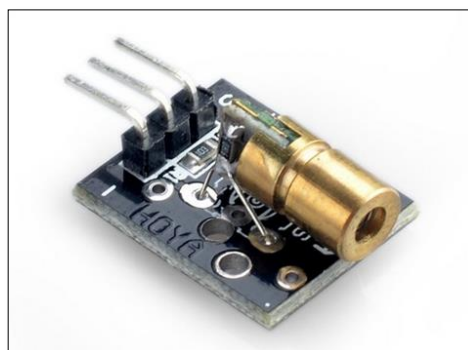
### 2.3.5 Laser

A laser is a device that emits light through a process of optical amplification based on the stimulated emission of electromagnetic radiation. The term "laser" originated as an acronym for "light amplification by stimulated emission of radiation". The first laser was built in 1960 by Theodore H. Maiman at Hughes Research Laboratories, based on theoretical work by Charles Hard Townes and Arthur Leonard Schawlow.

A laser differs from other sources of light in that it emits light *coherently*, spatially and temporally. Spatial coherence allows a laser to be focused to a tight spot, enabling applications such as laser cutting and lithography. Spatial coherence also allows a laser beam to stay narrow over great distances (collimation), enabling applications such as laser pointers.

Lasers can also have high temporal coherence, which allows them to emit light with a very narrow spectrum, i.e., they can emit a single color of light. Temporal coherence can be used to produce pulses of light as short as a femtosecond.

Among their many applications, lasers are used in optical disk drives, laser printers, and barcode scanners; DNA sequencing instruments, fiber-optic and free-space optical communication; laser surgery and skin treatments; cutting and welding materials; military and law enforcement devices for marking targets and measuring range and speed; and laser lighting displays in entertainment.



**Fig 2.5 Laser Module**

### 2.3.6 Photoresistor

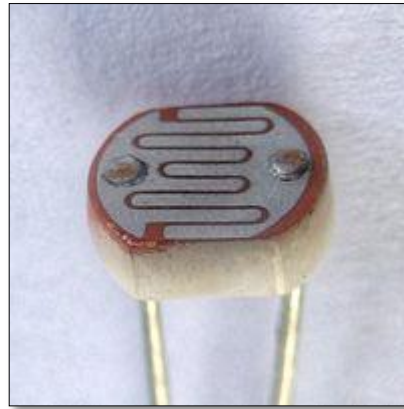
A photoresistor (or light-dependent resistor, LDR, or photo-conductive cell) is a light-controlled variable resistor. The resistance of a photoresistor decreases with increasing incident light intensity; in other words, it exhibits photoconductivity. A photoresistor can be applied in light-sensitive detector circuits, and light-activated and dark-activated switching circuits.

A photoresistor is made of a high resistance semiconductor. In the dark, a photoresistor can have a resistance as high as several megohms ( $M\Omega$ ), while in the light, a photoresistor can have a resistance as low as a few hundred ohms. If incident light on a photoresistor exceeds a certain frequency, photons absorbed by the semiconductor give bound electrons enough energy to jump into the conduction band.

The resulting free electrons (and their hole partners) conduct electricity, thereby lowering resistance. The resistance range and sensitivity of a photoresistor can substantially differ among dissimilar devices. Moreover, unique photoresistors may react substantially differently to photons within certain wavelength bands.

A photoelectric device can be either intrinsic or extrinsic. An intrinsic semiconductor has its own charge carriers and is not an efficient semiconductor, for example, silicon. In intrinsic devices the only available electrons are in the valence band, and hence the photon must have enough energy to excite the electron across the entire bandgap.

Extrinsic devices have impurities, also called dopants, added whose ground state energy is closer to the conduction band; since the electrons do not have as far to jump, lower energy photons (that is, longer wavelengths and lower frequencies) are sufficient to trigger the device. If a sample of silicon has some of its atoms replaced by phosphorus atoms (impurities), there will be extra electrons available for conduction. This is an example of an extrinsic



**Fig 2.6 LDR**

Photoresistors are less light-sensitive devices than photo-diodes or photo-transistors: the two latter components are true semiconductor devices, while a photoresistor is a passive component and does not have a PN-junction. The photoresistivity of any photoresistor may vary widely depending on ambient temperature, making them unsuitable for applications requiring precise measurement of or sensitivity to light photons.

Photoresistors also exhibit a certain degree of latency between exposure to light and the subsequent decrease in resistance, usually around 10 milliseconds. The lag time when going from lit to dark environments is even greater, often as long as one second. This property makes them unsuitable for sensing rapidly flashing lights, but is sometimes used to smooth the response of audio signal compression.

### **2.3.7 Smart Phone**

A smartphone is a handheld personal computer with a mobile operating system and an integrated mobile broadband cellular network connection for voice, SMS, and Internet data communication; most if not all smartphones also support Wi-Fi. Smartphones are typically pocket-sized, as opposed to tablet computers, which are much larger.

They are able to run a variety of software components, known as “apps”. Most basic apps (e.g. event calendar, camera, web browser) come pre-installed with the system,

while others are available for download from official sources like the Google Play Store or Apple App Store.

Apps can receive bug fixes and gain additional functionality through software updates; similarly, operating systems are able to update. Modern smartphones have a touchscreen color display with a graphical user interface that covers the front surface and enables the user to use a virtual keyboard to type and press onscreen icons to activate "app" features. Mobile payment is now a common theme amongst most smartphones.

Today, smartphones largely fulfill their users' needs for a telephone, digital camera and video camera, GPS navigation, a media player, clock, news, calculator, web browser, handheld video game player, flashlight, compass, an address book, note-taking, digital messaging, an event calendar, etc. Typical smartphones will include one or more of the following sensors: magnetometer, proximity sensor, barometer, gyroscope, or accelerometer.

Since 2010, smartphones adopted integrated virtual assistants, such as Apple Siri, Amazon Alexa, Google Assistant, Microsoft Cortana, BlackBerry Assistant and Samsung Bixby. Most smartphones produced from 2012 onward have high-speed mobile broadband 4G LTE capability and touchscreen starting to grow in use more.

Modern smartphones have a touchscreen color display with a graphical user interface that covers the front surface and enables the user to use a virtual keyboard to type and press onscreen icons to activate "app" features. Mobile payment is now a common theme amongst most smartphones. Mobile payment is now a common theme amongst most smartphones.

A telephone, digital camera and video camera, GPS navigation, a media player, clock, news, calculator, web browser, handheld video game player, flashlight, compass, an address book, note-taking, digital messaging, an event calendar, etc. Typical smartphones will include one or more of the following sensors: magnetometer, proximitysensor, barometer, gyroscope or accelerometer



**Fig 2.7 Smart Phone**

## **2.4 Software Description**

### **2.4.1 Embedded C**

Embedded C is a set of language extensions for the C programming language by the C Standards Committee to address commonality issues that exist between C extensions for different embedded systems. Historically, embedded C programming requires nonstandard extensions to the C language in order to support exotic features such as fixed-point arithmetic, multiple distinct memory banks, and basic I/O operations.

In 2008, the C Standards Committee extended the C language to address these issues by providing a common standard for all implementations to adhere to. It includes a number of features not available in normal C, such as, fixed-point arithmetic, named address spaces, and basic I/O hardware addressing.

Embedded C uses most of the syntax and semantics of standard C, e.g., `main()` function, variable definition, datatype declaration, conditional statements (`if`, `switch case`), loops (`while`, `for`), functions, arrays and strings, structures and union, bit operations, macros, etc. A Technical Report was published in 2004 and a second revision in 2006.



## 2.4.2 Arduino IDE

The Arduino integrated development environment (IDE) is a cross-platform application (for Windows, macOS, Linux) that is written in the programming language Java. It originated from the IDE for the languages Processing and Wiring. It includes a code editor with features such as text cutting and pasting, searching and replacing text, automatic indenting, brace matching, and syntax highlighting, and provides simple one-click mechanisms to compile and upload programs to an Arduino board. It also contains a message area, a text console, a toolbar with buttons for common functions and a hierarchy of operation menus. The source code for the IDE is released under the GNU General Public License, version 2.

The Arduino IDE supports the languages C and C++ using special rules of code structuring. The Arduino IDE supplies a software library from the Wiring project, which provides many common input and output procedures. User-written code only requires two basic functions, for starting the sketch and the main program loop, that are compiled and linked with a program stub `main()` into an executable cyclic executive program with the GNU toolchain, also included with the IDE distribution. Programs written using Arduino Software (IDE) are called sketches. These sketches are written in the text editor and are saved with the file extension `.ino`. The editor has features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors.

The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom righthand corner of the window displays the configured board and serial port. The toolbar buttons allow you to verify and upload programs, create, open, and save sketches, and open the serial monitor. The Arduino Software (IDE) uses the concept of a sketchbook: a standard place to store your programs (or sketches). The sketches in your sketchbook can be opened from the File > Sketchbook menu or from the Open button on the toolbar.

The first time you run the Arduino software, it will automatically create a directory for your sketchbook. You can view or change the location of the sketchbook

location from with the Preferences dialog. When you upload a sketch, you're using the Arduino bootloader, a small program that has been loaded on to the microcontroller on your board. It allows you to upload code without using any additional hardware. The bootloader is active for a few seconds when the board resets; then it starts whichever sketch was most recently uploaded to the microcontroller.

The bootloader will blink the on-board (pin 13) LED when it starts (i.e. when the board resets). Libraries provide extra functionality for use in sketches, e.g. working with hardware or manipulating data. To use a library in a sketch, select it from the Sketch > Import Library menu. This will insert one or more `#include` statements at the top of the sketch and compile the library with your sketch. Because libraries are uploaded to the board with your sketch, they increase the amount of space it takes up. If a sketch no longer needs a library, simply delete its `#include` statements from the top of your code. This displays serial sent from the Arduino or Genuino board over USB or serial connector. To send data to the board, enter text and click on the "send" button or press enter.

Choose the baud rate from the drop-down menu that matches the rate passed to `Serial.begin` in your sketch. Note that on Windows, Mac or Linux the board will reset (it will rerun your sketch) when you connect with the serial monitor. Please note that the Serial Monitor does not process control characters; if your sketch needs a complete management of the serial communication with control characters, you can use an external terminal program and connect it to the COM port assigned to your Arduino board.

If you would like to change the language manually, start the Arduino Software (IDE) and open the Preferences window. Next to the Editor Language there is a dropdown menu of currently supported languages. Select your preferred language from the menu, and restart the software to use the selected language. If your operating system language is not supported, the Arduino Software (IDE) will default to English. You can return the software to its default setting of selecting its language based on your operating system by selecting System Default from the Editor Language drop-down.

This setting will take effect when you restart the Arduino Software (IDE). Similarly, after changing your operating system's settings, you must restart the Arduino

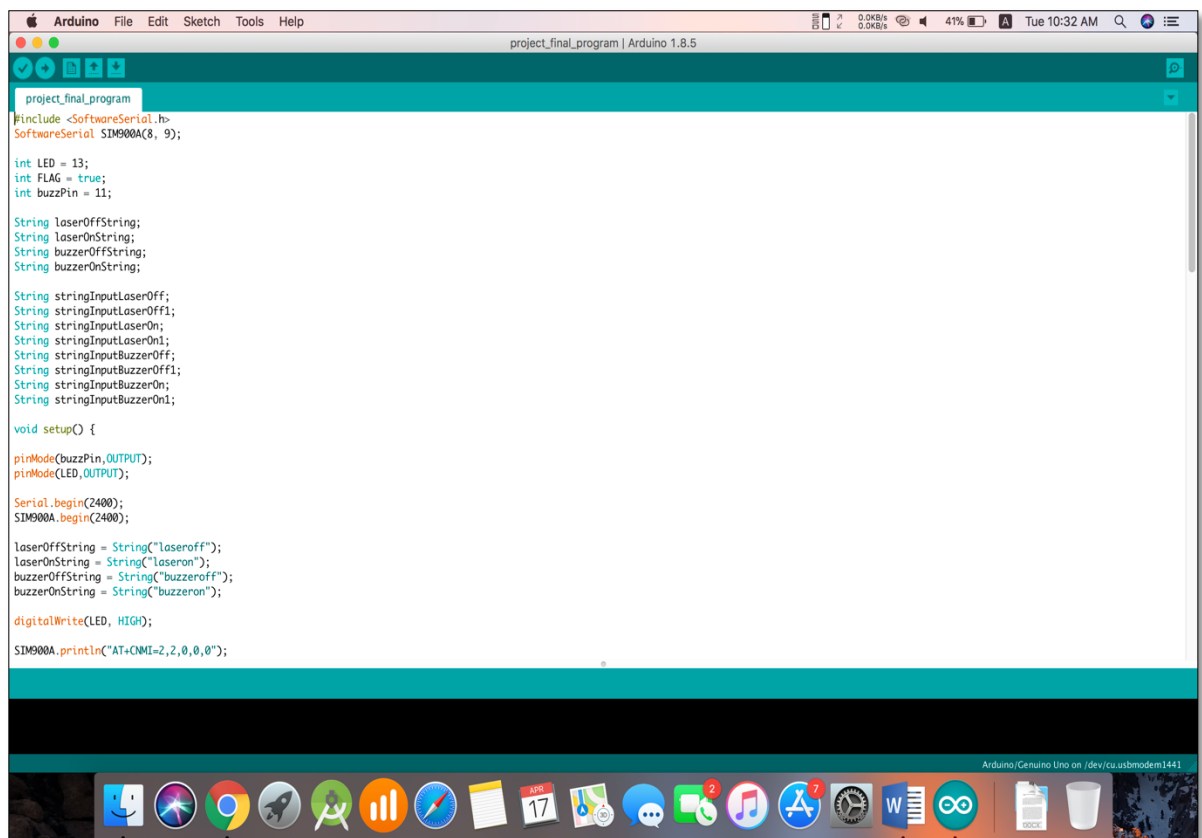
Software (IDE) to update it to the new default language. The board selection has two effects: it sets the parameters (e.g. CPU speed and baud rate) used when compiling and uploading sketches; and sets and the file and fuse settings used by the burn boot loader command.

Some of the board definitions differ only in the latter, so even if you've been uploading successfully with a particular selection you'll want to check it before burning the bootloader. You can find a comparison table between the various boards [here](#).

The Arduino IDE employs the program `avrdude` to convert the executable code into a text file in hexadecimal encoding that is loaded into the Arduino board by a loader program in the board's firmware. Arduino microcontrollers are pre-programmed with a boot loader that simplifies uploading of programs to the on-chip flash memory. The default bootloader of the Arduino UNO is the optiboot bootloader. Boards are loaded with program code via a serial connection to another computer. Some serial Arduino boards contain a level shifter circuit to convert between RS-232 logic levels and transistor-transistor logic (TTL) level signals.

A program written with the Arduino IDE is called a sketch. Sketches are saved on the development computer as text files with the file extension `.ino`. Arduino Software (IDE) pre-1.0 saved sketches with the extension `.pde`. A minimal Arduino C/C++ program consist of only two functions:

- `setup()`: This function is called once when a sketch starts after power-up or reset. It is used to initialize variables, input and output pin modes, and other libraries needed in the sketch.
- `loop()`: After `setup()` has been called, function `loop()` is executed repeatedly in the main program. It controls the board until the board is powered off or is reset.



**Fig 2.8 Arduino IDE**

### 2.4.3 Android Studio

Android Studio is the official integrated development environment (IDE) for Google's Android operating system, built on JetBrains IntelliJ software and designed specifically for Android development.<sup>1</sup> It is available for download on Windows, macOS and Linux based operating systems. It is a replacement for the Eclipse Android Development Tools (ADT) as primary IDE for native Android application development.

Android Studio was announced on May 16, 2013 at the Google I/O conference. It was in early access preview stage starting from version 0.1 in May 2013, then entered beta stage starting from version 0.8 which was released in June 2014. The first stable build was released in December 2014, starting from version 1.0. The current stable version is 3.1 released in March 2018.

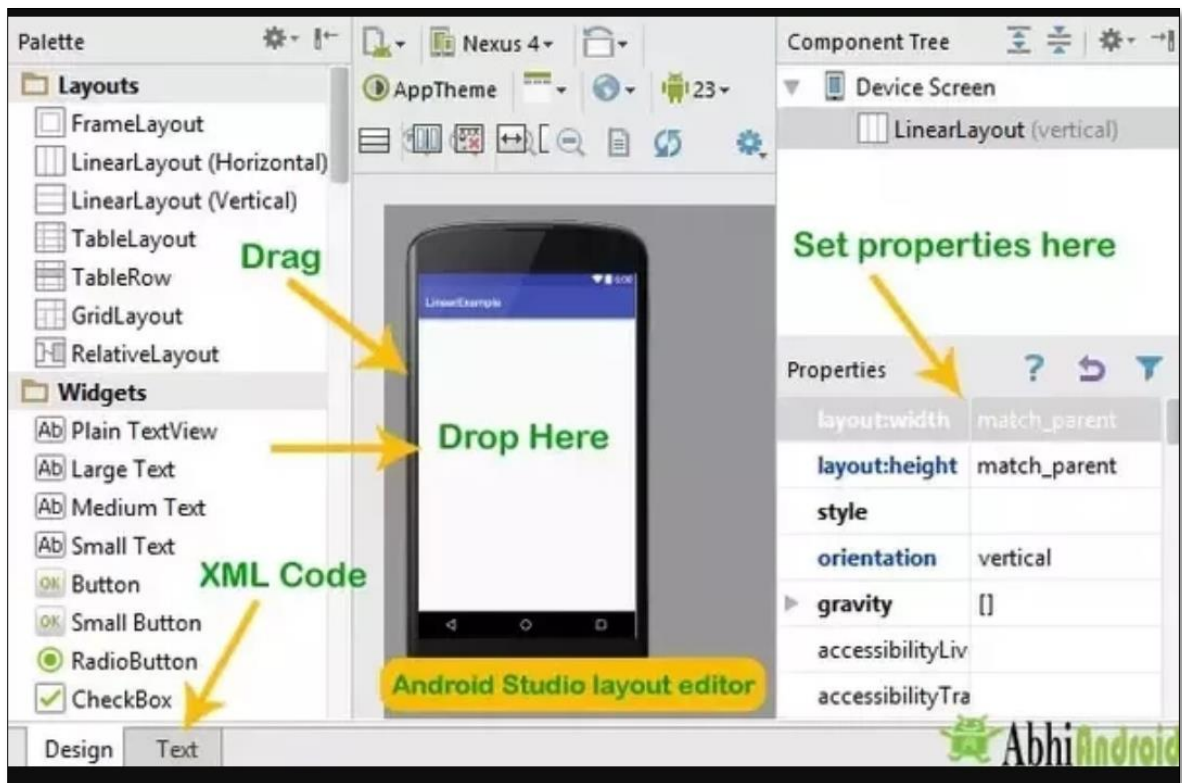


Fig 2.9 Android Studio

## CHAPTER 3

### MODULES

#### 3.1 Laser Mesh ( Tripwire)

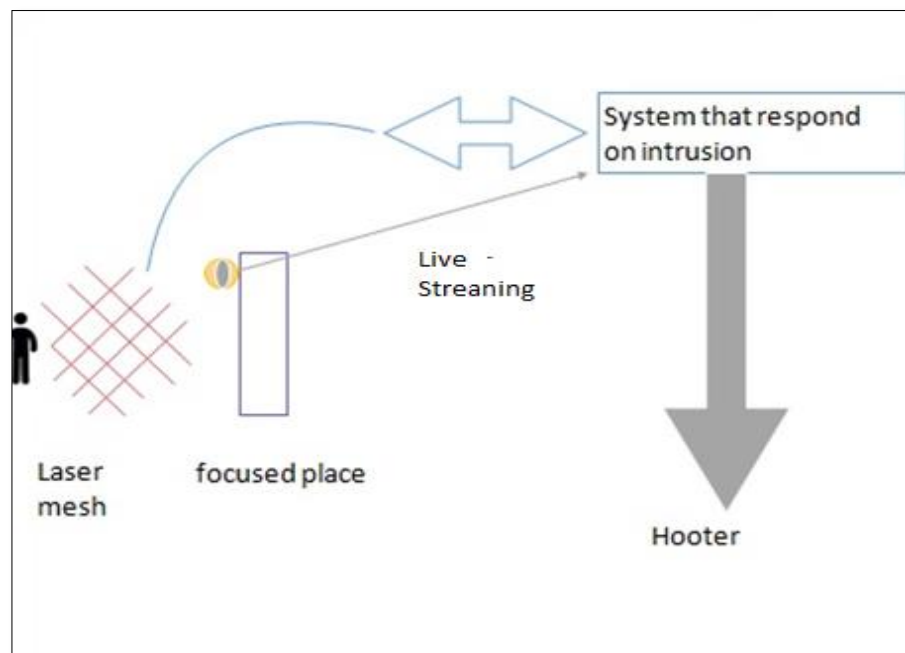
No security system is complete without lasers. Laser Tripwire is a simple implementation of a laser-triggered alarm. So in this project we are going to build a laser tripwire alarm(hooter) from a laser point, a couple of mirrors and LDR With this you can cover an entire house or any area which we want to keep secure with an array of light beams.

If any one of them is crossed it sets off your buzzer Interrupting that laser beam sends the analog input over a threshold, triggering the alarm and sounding a buzzer until a reset button is pressed..

The laser mesh is created by reflecting the laser beam on different mirrors at different angles. A camera is placed in that area which will work like a digital such that legitimate user can see protected area whenever he want from anywhere.

If a intruder trip the laser then the legitimate user can check whether the person is authorized or not and if not then he can turn on the hooter. Photoresistors also exhibit a certain degree of latency between exposure to light and the subsequent decrease in resistance, usually around 10 milliseconds. The lag time when going from lit to dark environments is even greater, often as long as one second. This property makes them unsuitable for sensing rapidly flashing lights, but is sometimes used to smooth the response of audio signal compression So in this project we are going to build a laser tripwire alarm from a laser point, a couple of mirrors and LDR With this you can cover an entire house or any area which we want to keep secure with an array of light beams.





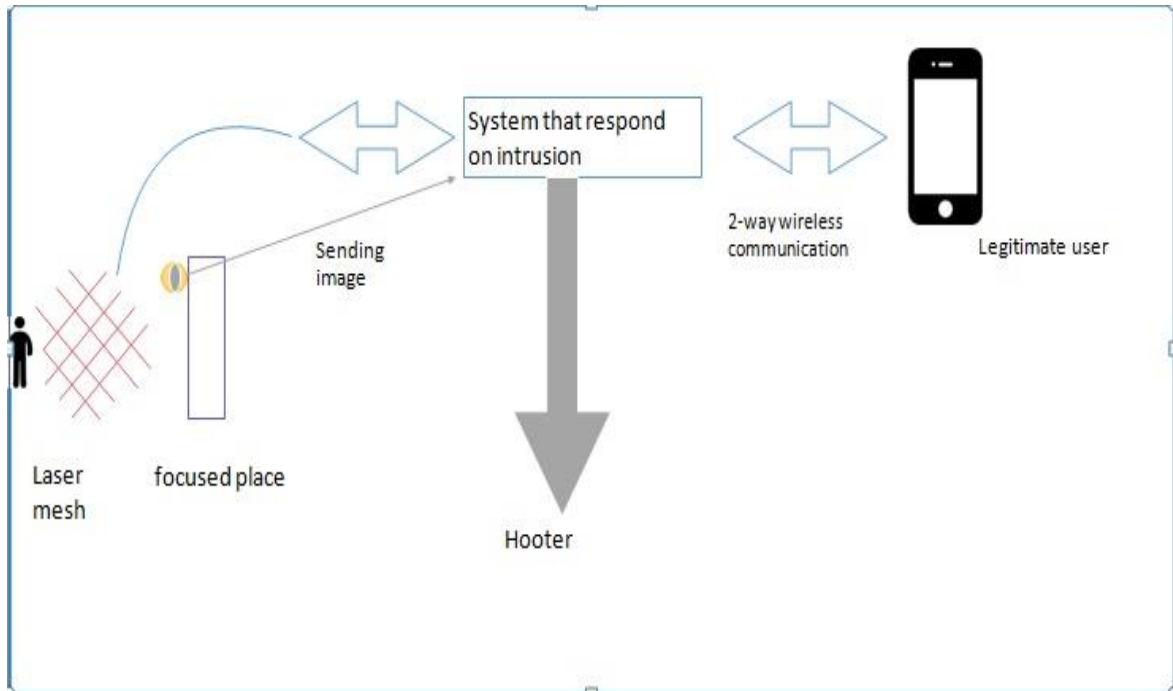
**Fig 3.1 Laser Mesh ( Tripwire)**

### **3.2 GPS and Remote Control**

A wireless interface are used to detect and identify visitors and send an alert message about the current home environment status via GSM network automatically to the home owner's mobile phone or any communication devices. The device can be placed at any remote location which can be easily accessed by the user.

It uses a microcontroller for system control, GSM technology for communication and sends SMS containing the emergency message to the GPS location of the sender. Then the legitimate user see who is the visitor with the help of his camera through his app.

In case of unauthorized entrance in the target area the legitimate user can turn ON the hooter and can also send emergency message to the people which is added in the emergency contact list in the application. Through, GPS he can turn on and off the laser and hooter by sending messages through his app to the target location on SIM900A GPS Module. The target area monitoring camera can be accessed with the help of app remotely from anywhere. In this way we establish a two way communication in our security system which was never seen in any security system before this.



**Fig 3.2 GPS and Remote Control**

### 3.2.1 GSM

GSM has been used due to its high availability, coverage and security. AT commands can be sent through the GSM network and this controls the devices. Messages are sent by the device to the user through SMS as well. This system can however incur additional costs for the SMS. There is no UI that the user can use to control the device. This system has the disadvantage of not being able to program the devices. Also SMS relies on upon the networks and there is a possibility of delayed delivery. The system doesn't have any state information related to the devices and expects the user to keep track of it. The system is depicted as an M2M system.

It utilizes GSM for communication. GSM offers options for M2M which include Dual Tone Multi Frequency (DTMF), SMS and General Packet Radio Service (GPRS). This system chooses to use the SMS along with AT (attention) commands. It has a PC as a centre of commands. A GSM dial-up and communication system is embedded in the PC. Visual C++ is used for implementation.

The PC decodes the received messages via SMS and performs the commands required. It is a system that can be programmed for the required application as per requirements implementation.

The PC decodes the received messages via SMS and performs the commands required. It is a system that can be programmed for the required application as per requirements.

### 3.2.2 Working Explanation

In this project, Arduino is used for controlling the whole process. Here we have used GSM wireless communication for controlling devices. We send some commands and after receiving given commands by arduino through GSM, Arduino send signals to devices, to switch ON or OFF the devices.

**Table 3.1 Activation of Laser and Buzzer**

<b>S.no.</b>	<b>Message</b>	<b>Operation</b>
1	laseroff	Laser will turn off
2	laseron	Laser will turn on
3	buzzeroff	Buzzer will turn off
4	buzzeron	Buzzer will turn on

The above table 3.1 shows the functioning of the laser module i.e., when it activates and when it gets off. In addition to that, it also shows the functioning of buzzer, i.e., when it responds according to laser trips and when it gets off.

When we send SMS to GSM module by Mobile, the GSM receives that SMS and sends it to Arduino. Now Arduino Reads this SMS and extract main commands from

received string. If match occurred then Arduino sends signal for turning ON or OFF the devices using appropriate commands.

## CHAPTER 4

### SNAPSHOT

#### 4.1 Laser Mesh(Frontend)

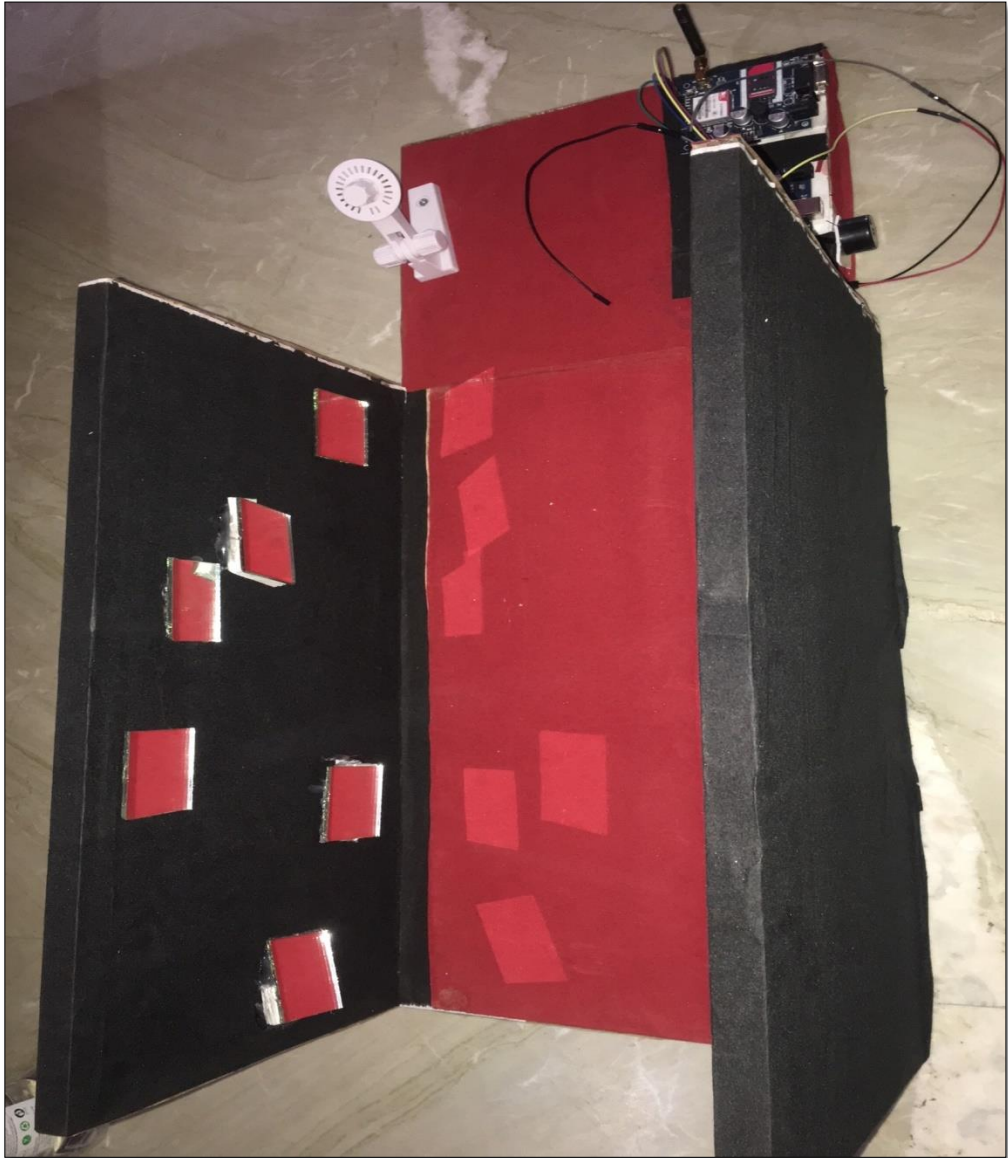
A laser mesh is created with the help of laser module and mirrors . Firstly, the laser beam goes to the walls and then it gets reflected by the mirrors. This process goes on and on until the beam goes to the LDR after reflection through several mirrors.



**Fig 4.1 Laser Mesh ( Frontend)**

### 4.1.1 Laser Mesh is ON

The mesh of reflected beam of lasers through mirrors always remains active until we send a command to the circuit with the help of our android application.



**Fig 4.2 Laser Mesh is ON**



### 4.1.2 Laser Mesh is OFF

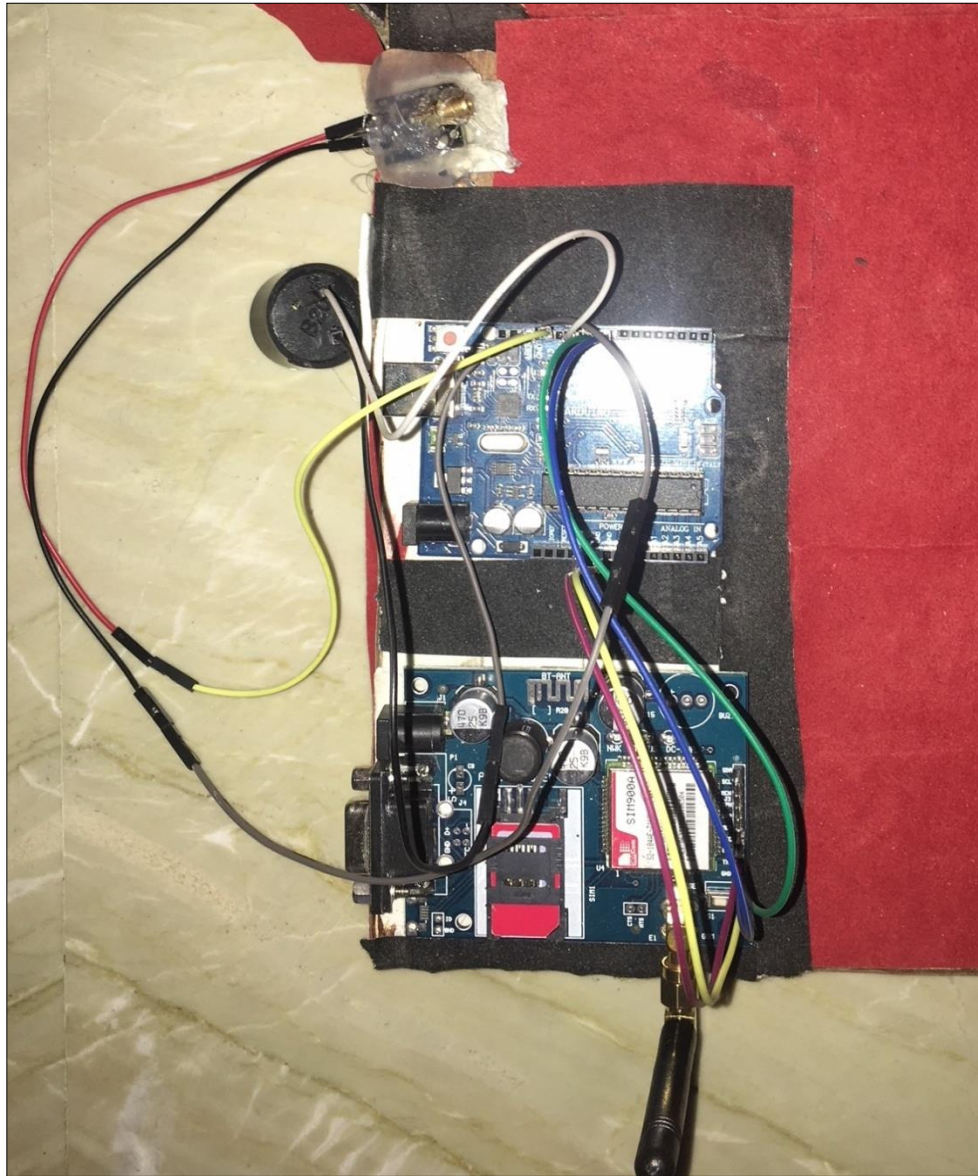
When an intruder trips the laser mesh, the laser mesh gets off . In addition to that the laser mesh gets off with the help of the legitimate user by the android application.



**Fig 4.3 Laser Mesh is OFF**

## 4.2 Hardware Circuit(Backend)

The hardware circuit consists of GSM SIM 900A module, Laser Module, Buzzer and Arduino UNO. These modules are connected to each other and below image shows the respective circuit.



**Fig 4.4 Hardware Circuit(Backend)**

### 4.3 Integrated System

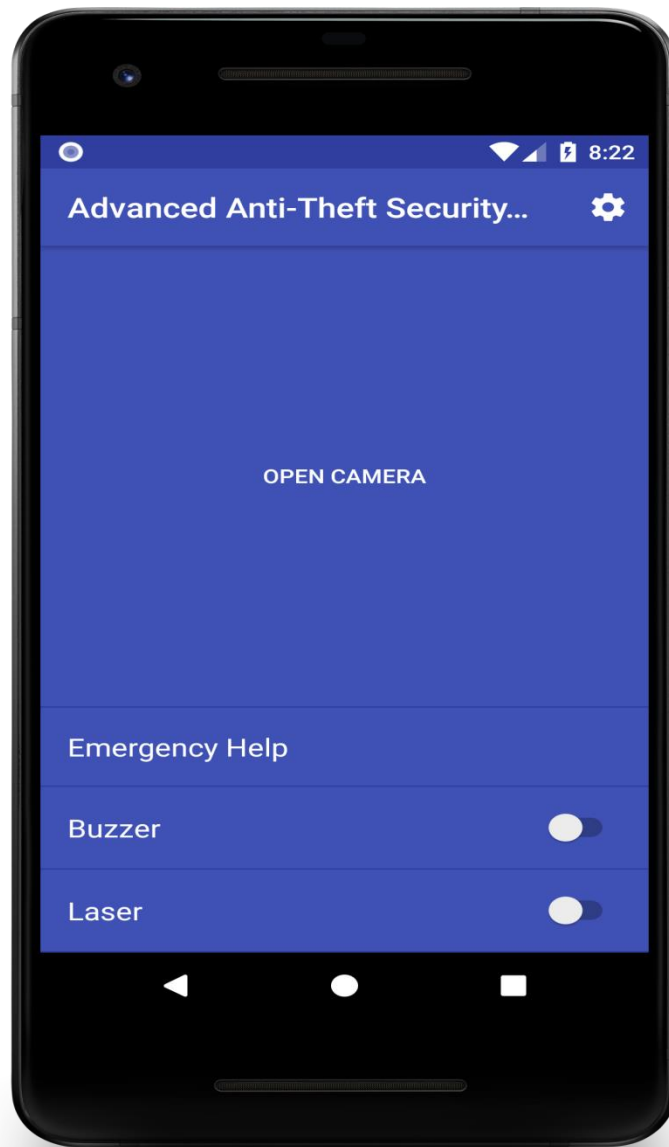
The Laser Mesh, IP Camera ,GSM Module and Arduino UNO integrates together to form the whole integrated system.



**Fig 4.5 Integrated System**

## 4.4 Android Application

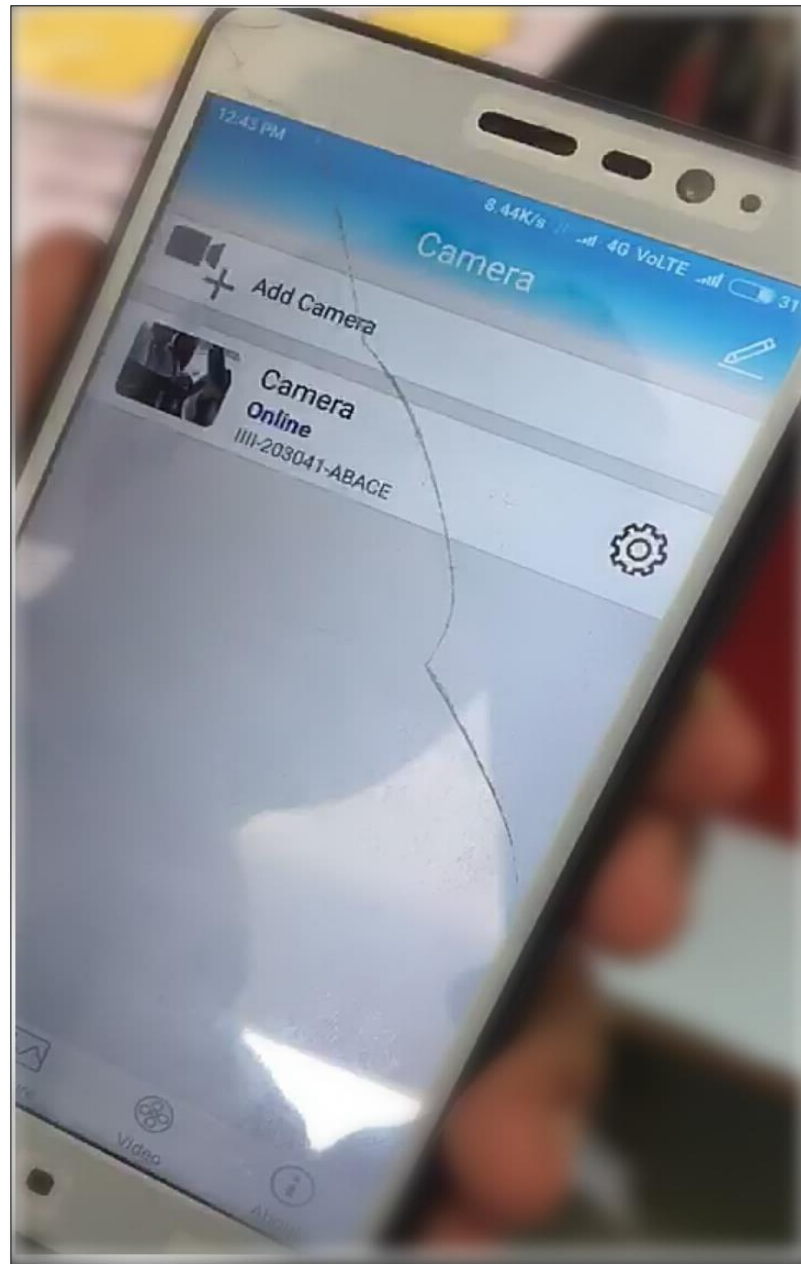
This Android Application plays a crucial role in this project. With the help of this application, the legitimate user can respond at any instant of time, when any mishappening took place. It contains several activities that have different features.



**Fig 4.6 Home Screen**

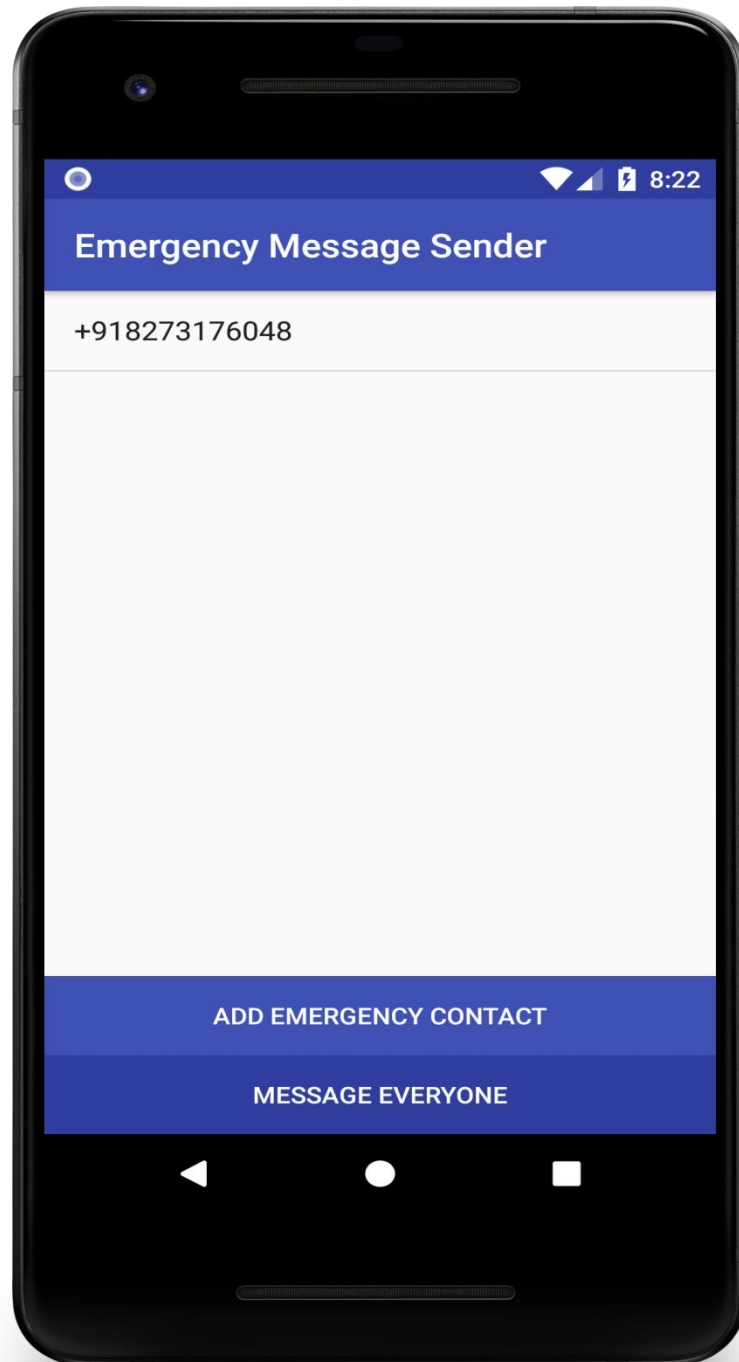
Figure 4.6 shows the home screen of our application which contains open camera button, emergency help , buzzer on/off and laser on/off.





**Fig 4.7 Camera Surveillance**

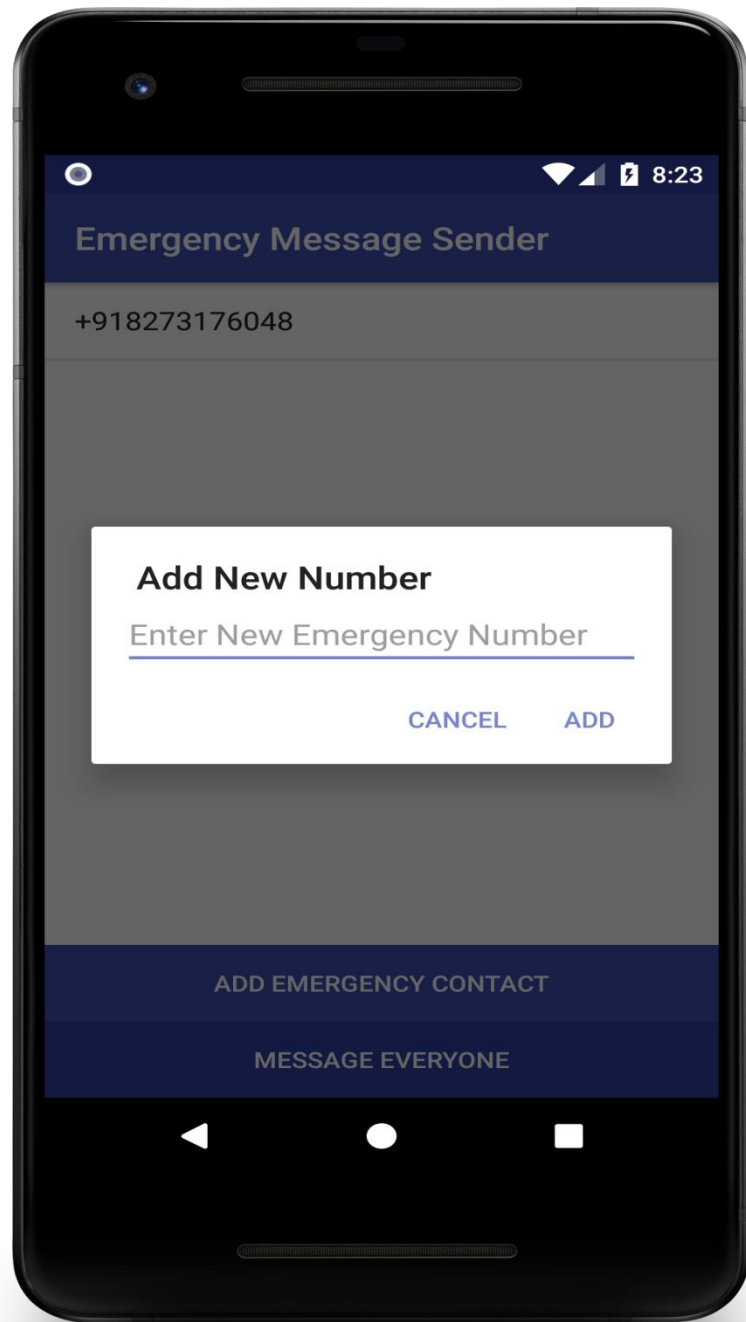
Figure 4.7 shows the live surveillance provided by the camera to the legitimate user on his android application so that he performs the respective actions accordingly



**Fig 4.8 Emergency Message Sender**

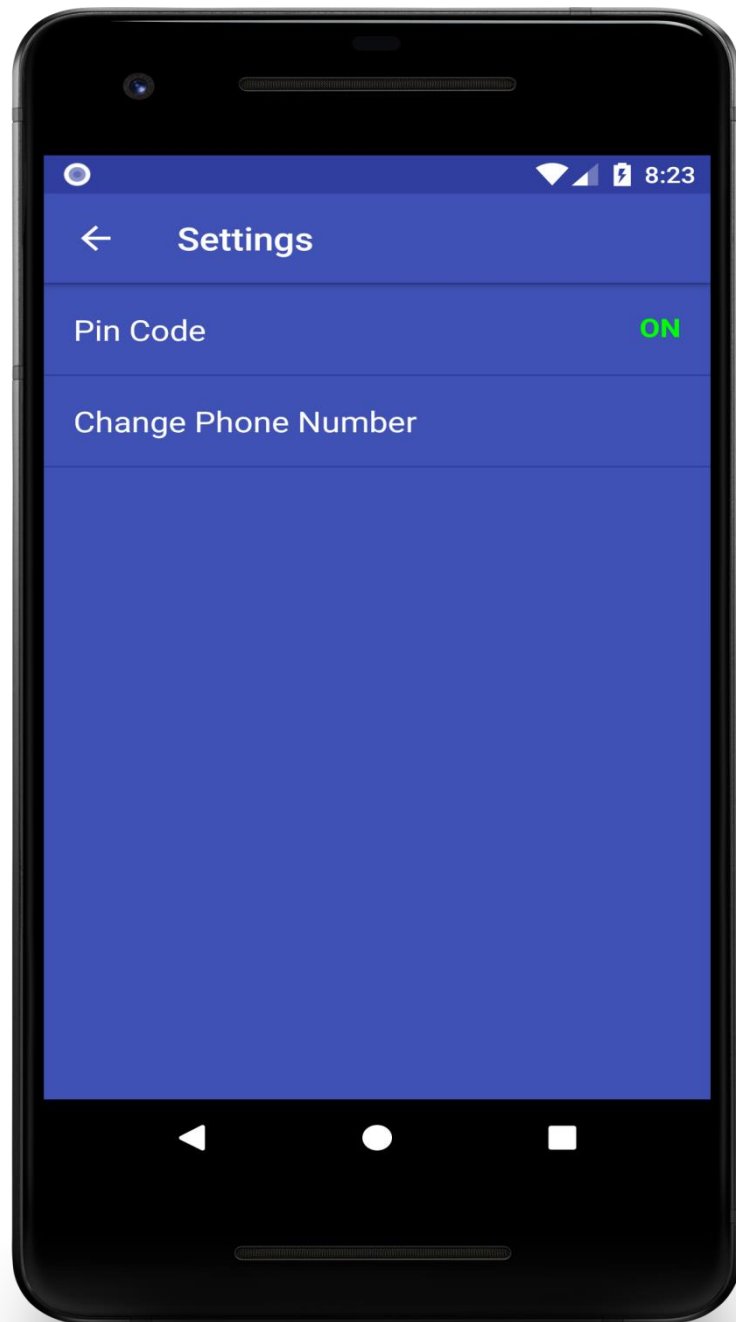
Figure 4.8 shows the lists of contact numbers to which the message is sent to all the contacts in case of emergency. By clicking on Message Everyone button, an emergency message is sent to all the respective numbers.





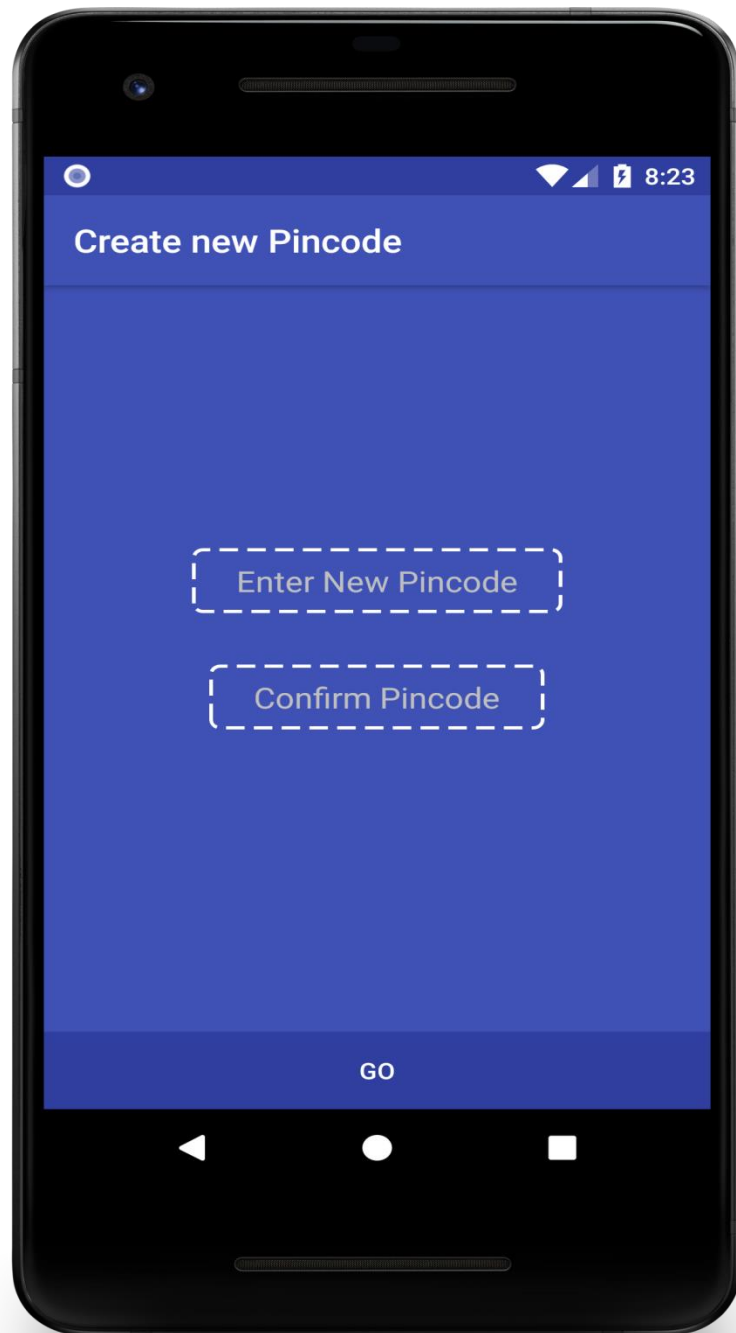
**Fig 4.9 Add Emergency Contact**

Figure 4.9 shows how to add new emergency contacts in the previously defined list of numbers. By clicking on Add Emergency Contact, a dialog box Add New Number appears which ask user to Enter New Emergency Number then by clicking on Add button, the new number is added.



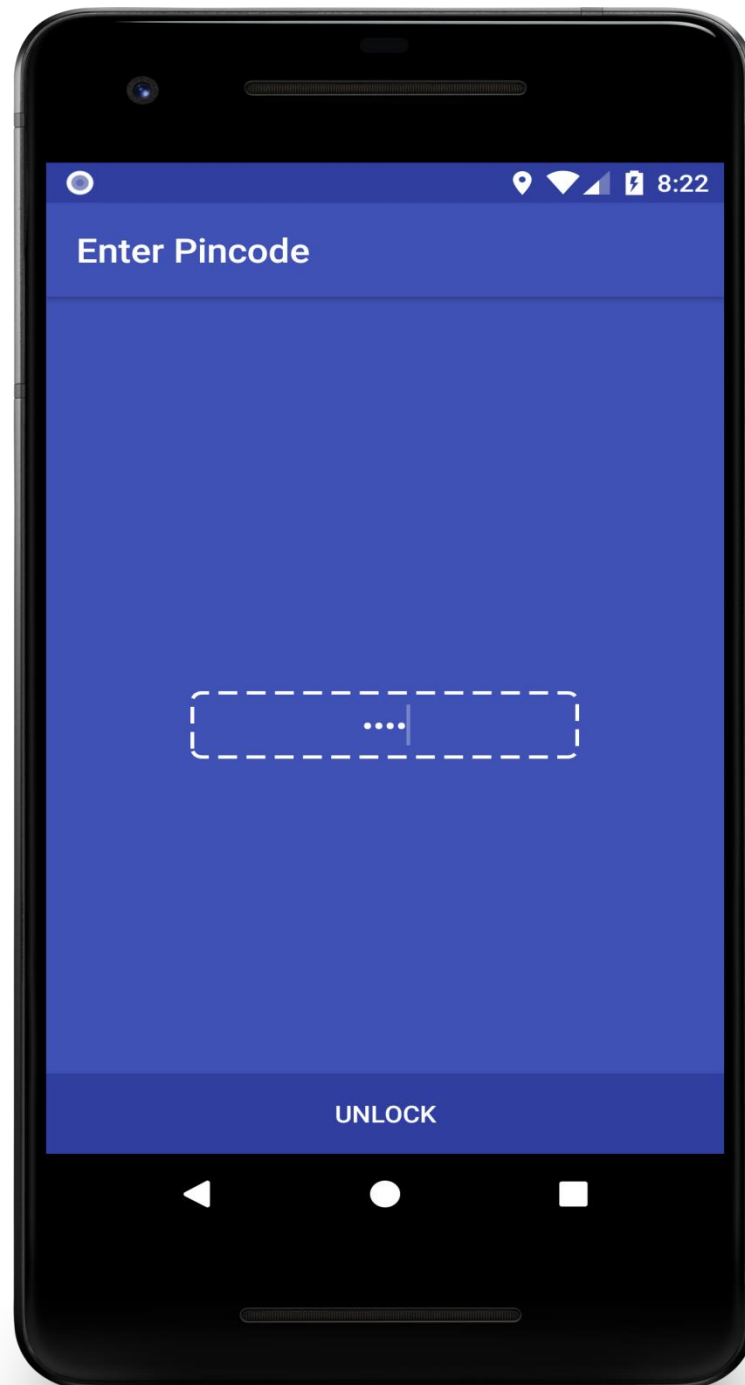
**Fig 4.10 Settings Activity**

Figure 4.10 shows the settings activity which consists of two parameters i.e., Pin Code and Change Phone Number.



**Fig 4.11 New Pincode Activity**

Figure 4.11 shows the activity to create new Pincode. For this, the user have to enter new pincode and then confirm pincode by re-entering same pincode and then click Go, the pincode is added and shows as ON in the settings.



**Fig 4.12 Lock Screen**

Figure 4.12 shows the lock screen and by entering the pincode, the user can unlock the application. This passcode is for validation of authenticated user so that only authenticated legitimate user can open the application.



**Fig 4.13 Change Number Activity**

Figure 4.13 shows the activity to change the number of the legitimate user. For this, the user have to enter the new phone number and then click on Save. In this way his/her Phone Number is changed.

## CHAPTER 5

### ADVANTAGES AND DISADVANTAGES

#### 5.1 Advantages

- Traditional method of using PIR sensor was replaced with LDR and for the sake of proper operation of PIR sensor, it requires a warm up time of 20 to 60 seconds. This is required because, the PIR sensor has a settling time during which it calibrates its sensor according to the environment and stabilizes the infrared detector thus the existing system is not suitable. This limitation was overcome by using the LDR.
  
- Usually the technologies that are developed are single dimensional i.e. they are developed either for the purpose of security or for safety. The various alarms are used individually but are not integrated to work together and make the owner aware about the situation. But we have made the system for both security and safety as we can establish a two-way communication between the legitimate user and the target area.
  
- The existing GSM system communicates to the specific mobile number which may not be sufficient as just having a single mode of communication in case of a security or safety issue. Thus there is a need of integrating the existing system with internet. So we have integrated our system with internet as we can control all the devices and monitor the target area remotely from anywhere.
  
- It is very easy to use. The app interface is so user friendly that in just a click a legitimate user can control the devices and monitor the target area live.

- One of the prominent feature is that it allows two way synchronization between the targeted area and the legitimate user which makes the system different from conventional systems
- It also overcomes the drawback of CCTV surveillance that it do not make the legitimate user aware if something wrong is happening.
- The system can be ideally used in the targeted areas like bank lockers, army/military inventories , international borders, industrial warehouses etc where safety is equally necessary as of security.

## **5.2 Disadvantages**

- The system requires various hardware and their respective installations which makes the working environment somewhat complex.
- As the system responds immediately on any type of intrusion so surely there is a need of fast internet.
- Hardware must be updated and solely tested.
- Laser modules, laser mesh and LDR should be tested and installed with deep concentration because these are the most delicate and variable part of the system.
- User must be having internet connection ,otherwise he/she would not be able to access the targeted area.
- It is not at all cost efficient approach that hardware implementation requires a huge amount to be invested.



- The system is not viable for the places where there is a continuous and repeated roaming of people across the targeted area.
- Communication and coordination is more complicated.

## CHAPTER 6

### CONCLUSION

Our motto was to develop a security system which will provide both high security and be cheaper in cost. Our security system is less bulky as it requires less components and wiring and it has very low power requirements.

Any damaged part in the system can easily be removed and replaced, and all the components are easily available. Moreover, the security system can be used in other sector such as perimeter security with very little modification. So we are hopeful, our security system will provide investors in aquaculture with the required security.

This project presents the design and the implementation of an interactive home security system with the GSM, Arduino. Arduino IDE as a platform and Web-enabled measurement and control systems. The Web based monitor and automatic control of equipment is forming a trend in automation field. Replacing PC with low-cost single chip processor which can make administrators to get parameters of different remote devices and send control information to field equipments at any time through Internet. The GSM is an excellent choice for this due to its extensive coverage.

The design is completely wireless and integrated with the software to form a low cost, robust and easily operable system. The GSM, Arduino and Web based controlled duplex communication system provides a powerful decision making device concept for adaptation to several smart home scenarios.

## **CHAPTER 7**

### **FUTURE ASPECTS**

1. In future, the system can be made advanced with respect to the recognition system of the suspect. Till now, there is no system which recognize the suspect at the entry level of the focused area .
2. On a large scale it can be used to develop robots with military applications. It can be used to target enemy without any human being crossing the territory.
3. It is robust sensitive and fast moving, hence it can be applied in risky operations.
4. With the help of machine learning, database can be created according to the frequent capturing of same faces so that suspect can be easily targeted.
5. Here , there is a wide chance of provisioning the whole system with face recognition which will turn the project in a new face via automations.

## REFERENCES

- [1]. Aylward, R., and Paradiso, J.A.,(2014) "A Compact, High-Speed, Wearable Sensor Network for Biomotion Capture and Interactive Media,"
- [2]. Bishwajit Ghose, (2014) "Fisheries and Aquaculture in Bangladesh: Challenges and Opportunities," in JSciMed Central..
- [3]. Dipankor Paul, Md. Sohel Rana, and Md. Mokraram Hossain, (2002) "A preview on experimentation on Laser security system," in Engineering Science and Technology: An International Journal, vol. 2, no. 2.
- [4]. G. Demiris, B. K. Hensel et al., (2008) "Technologies for an Aging Society: A Systematic Review of Smart Home Applications," Yearb Med Inform, vol. 3, pp. 33–40.
- [5]. L.R.Tabrizi and A.Madanipour, (2006) "Crime and the city: Domestic burglary and the built environment in Tehran," Habitat International, vol. 30, no. 4, pp. 932–944.
- [6]. R. J. Robles, T.-h. Kim, D. Cook, and S. Das, (2010) "A review on security in smart home development," International Journal of Advanced Science and Technology, vol. 15.
- [7]. S. Harrendorf, M. Heiskanen, and S. Malby,(2010) "International statistics on crime and justice". European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI).
- [8]. T. Hope, (2007) "Conceptualising the Trend in Burglary in England and Wales".
- [9]. UNODC, (2015) "International Burglary, Car Theft and Housebreaking Statistics," United Nations Office on Drugs and Crime (UNODC), Tech. Rep.