CHAPTER 1
INTRODUCTION

1.1 Introduction

The Internet of Things is a network of interconnected physical things that may exchange data among themselves without the aid of people. It enables data collection from all types of sources, including household appliances, people, pets, and any physical objects whose IP addresses might permit data transmission over a network. IOT is embedded with electronics devices, including software, sensors, and networks in gear. In 1985, Peter T. Lewis discussed the idea of the Internet of Things in his testimony to the Federal Communications Commission, which is when the name "IOT" first appeared (FCC). When compared to other technologies, the IOT's application space has expanded rapidly. With the use of IOT, we may gather real-time data, information, and analysis while using precise sensors and internet connectivity to aid in taking decisions that would be helpful.

Home security has elevated to one of the top concerns in society in recent years. Making your house secure from intruders is vital. We can easily detect infiltration and generate an alert with the use of sensors (like PIR sensors) for intrusion detection and surveillance. Smart home security systems with the ability to quickly identify intrusions and strong connections to protected environments typically include PIR sensors, buzzers to notify, cameras for taking pictures.

The term "Internet of Things" (IoT) refers to a variety of items connected to electronics, software, devices, and communication networks that exchange information, according to Kevin Ashton of Procter & Gamble in 1999 [1]. The goal is to connect every object in the environment so that they can all communicate with one another and form a self-configuring network. The created network enables autonomous object coordination and communication, such as that between home appliances functioning via a network at home [4].

An IoT-based system receives remote commands and signals through its infrastructure, increasing the system's physical integration and enhancing consumer and economic benefits. Additionally, IoT devices facilitate the fusion of diverse technologies, which hastens the geographic distribution of data generated by everything connected to the Internet and the rapid spread of such technologies.[5] For various consumer applications, including entertainment, smart homes, health-related devices, and washer/dryer machines, vacuum cleaners, ovens, refrigerators, and freezers that use Wi-Fi for remote monitoring, a growing segment of such devices with Internet connectivity or local connectivity are being developed.[6]

Based on the IoT idea, home automation comprises the monitoring and management of distant technological equipment. Additionally, it provides the capability of monitoring and managing isolated programmable devices, such as temperature sensors and gas leak detectors, as well as actuators like relays. Home automation systems frequently connect to appliances and devices like lights and heating/cooling systems. Home automation is becoming increasingly important in today's busy world to make daily duties easier. The ability to monitor and manage one's entire home from a smartphone or website, control power use, lock and unlock doors, and other modern conveniences is provided by home automation. However, purchasing and installing such systems can be expensive, which is why consumer interest in and demand for automation homes have not been very high up until this point. Furthermore, installing and configuring such systems might be difficult. Therefore, it is imperative that new solutions offer simple to configure, cost-effective methods.

1.2 Problem and Motivation

Most older models of home security systems are vulnerable to power outages and security breakdowns, so security monitoring systems need data transmission systems that are quick to receive data and have a good range so that the client can freely install the devices in strategic locations for intrusion detection. The internal setup of the security system must be safe and secure to prevent hacking by anyone, regardless of the means used to power the system, receive data, or transmit data. Since the atmospheric conditions are not constant, the security system must be strong, temperature-resistant, and water-resistant to ensure that neither the data transmission nor the data reception processes are hampered. Security systems need to use a lot of sensors in order to cover every area of the house because some security systems have restrictions on how sensor devices can be used, which prevents them from covering the entire area of an entry.

1.3 Objectives

We have some specific objectives for this project and they are pointed below:

- To design and implement of Automated Home Surveillance System.
- To design and implement Automated Home Surveillance System.
- To detect flame and smoke automatically, laser light protection, buzzer ring and IoT notification.
- IoT web camera monitoring system.
- To implement a system for easy to our daily life.

1.4 Structure of the Project

This Project is organized as follows:

Chapter 1 Introduction**:**The first chapter contains the statement of the introduction, our background study for the project, problem statement, objectives of the study and the project outline.

Chapter 2 Literature Review**:** The chapter two contains our introduction, literature review part.

Chapter 3 Hardware and Software Analysis**:**Chapter three describes the theoretical model. Here we mainly discuss about proposed system Hardware and software development of our project etc.

Chapter 3 Methodology**:**Chapter three describes the theoretical model. Here we mainly discuss about proposed system architecture in details with having block diagram, circuit diagram, structural diagram, project working principle, complete project image etc.

Chapter 4 Result and Discussion**:**Chapter four deals with the result and discussion and discuss about our project advantages and application.

Chapter 5 Conclusion**:**Chapter five all about our project conclusion and future scope.

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

This chapter is arranged on Literature Review. Here's a look at some of last year's literature, like our project. By reading them, we can overcome the mistakes of the previous project and make a more effective project.

2.2 Related Research/ Works

Cameras need to be of good Design and Implementation of Security for Smart Home based on GSM technology was discussed by Govinda et al. (2014) that provides two methods to implement home security using IOT [1]. One is using web cameras such that whenever there is any motion detected by the camera, it sounds an alarm and sends a mail to the owner. This method of detecting intrusion is quite good, albeit somewhat expensive due to the cost of the cameras involved in the process. The quality which means it should have a wide range and the picture quality should be high enough to detect movement. Also if you go for movable cameras such as dome cameras, they will cost even more than the fixed ones.

SMS based system using GSM was proposed by Karri and Daniel (2005) propose to use internet services to send messages or alert to the house owner instead of the conventional SMS.[2] Jayashri and Arvind (2013) have implemented a fingerprint-based authentication system to unlock a door [3]. This system helps users by only allowing the users whose fingerprint are authorized by the owner of the house. This system can also be used to monitor who all have used the sensor to gained entry into the house. The system is coupled with a few more home protection features such as gas leakage and fire accidents. Although a good system, fingerprint sensors are expensive and complex (as they need increased sensor resolution) to integrate into an IoT setup. Some experts also argue that only relying on a fingerprint sensor is not wise as it is relatively easy to lift someone’s fingerprints and replicate them, which is why it is always advised to use fingerprint scanners in two factor authentication systems where an additional layer of security is available in the form of PIN,passcode, voice recognition, etc.

Some researchers proposed an idea of robust IOT home security system where a fault in of one component in the system does not lead to the failure of the whole system [4]. The idea of using multiple devices which may or may not be directly compatible with each other but can be made to work in such a way that they can replace an existing component of the system in case of a fault. In tandem to this, the model has the ability to use overlap between various devices which would result in preserving energy thus making the model more efficient. An example provided of the said model would use temperature sensor, Wi- Fi module and a door sensor to replace a faulty camera. The authors are successful in an effort to demonstrate the given example. However such systems are useful for people with energy efficiency in mind and for those who need a high degree of robustness with their security systems and are willing to expend more money than usual. Laser rays and LDR sensor are used to detect intrusion using their movement was proposedin 2016 [5].

The way the system works is that a laser is focused towards a LDR sensor and the moment that the contact of laser to LDR sensor breaks, the alarm connected to the sensor goes off alerting the neighbours and sends a SMS to the owner. This system solve the problem of covering the places which are out of range from the fixed cameras but faces the same difficulties which are faced with systems consisting of GSM modules to send text messages, which is that the delivery of message is dependent on network coverage. Also due to the nature of lasers being a straight beam, it can be avoided by intruders who know about the system and are capable of dodging the lasers, rendering the whole system useless.

A novel way to design an electronic lock using Morse code and IOT technology [6]. The authors claim that this as an original idea which have not been tried before and is the firstof its kind “optical Morse codebased electronic locking system”. This system uses LED’s (Light emitting diodes) as an encrypting medium to send signals. To make it more accessible to general public, the LED in smart phones has been used. On the receiver’s side is a photosensitive resistor as well as a microcontroller such as Arduino processor which has the ability to decrypt the optical signal after receiving them from the LED. Upon decoding the signal it can than upload the current condition of the lock to a cloud from where the owner can monitor the system. The authors have experimented the system in realtime and it has proved to work under different illumination environments with all the functions working as they were intended to. The authors also claim to have an easy and user friendly interface. The IOT system developed here works very well and can be used by anyone and is very convenient due to the use of mobile phones as LED, which also makesit a cost expensive alternative [7]. Anitha et al (2016) proposed a home automation system using artificial intelligence and also proposed a model for cyber security systems [8,9].

Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana explained the model for IOT project which focuses on building a smart wireless home security system which sends alerts to the owner by using Internet in case of any trespass and raises an alarm optionally. The microcontroller used in the current prototype is the TICC3200 Launchpad board. This system can send alerts and the status sent by the Wi-Fi connected micro-controller managed system can be received by the user on his phone from any distance irrespective of whether his mobile phone is connected to the internet [10]. Vamsikrishna Patchava, Hari Babu Kandala, P Ravi Babu proposed the system for Smart Home Automation technique with Raspberry Pi using IOT and it is done by integrating cameras and motion sensors into a web application. Raspberry Pi operates and controls motion sensors and video cameras for sensing and surveillance. For instance, it captures intruder's identity and detects its presence using simple Computer Vision Technique (CVT) [11].

The main advantage of IOT based Home Automation is user can remotely control or integrated with the electric appliance and devices. Most of the Home Automation Systems are relatively high cost comparing to Bangladesh. Most of the home automation is android or IOS based, not platform independent. The security is a great concern for IOT based home automation system. The paper -"Internet of Things Business Models, Users, and Networks" describes various wireless IOT protocols used in smart home. It also describes the application protocols used for IoT. It is useful to recommend the best security features of different protocols and helps choose which protocol to use [12]

2.3 Summary

The above has been discussed in detail in the past few literature's which has given us a lot of motivation to do this project.

CHAPTER 3

HARDWARE AND SOFTWARE ANALYSIS

3.1 Required Instrument

- Node MCU
- SMPS
- PIR Motion Sensor
- ESP 32 Camera
- Gas Sensor
- Flame Sensor

3.2 Node MCU

Node MCU is an open source firmware for which open source prototyping board designs are available. The name "Node MCU" combines "node" and "MCU" (micro-controller unit). The term "Node MCU" strictly speaking refers to the firmware rather than the associated development kits. Both the firmware and prototyping board designs are open source. The firmware uses the Lua scripting language. The firmware is based on the eLua project, and built on the Espressif Non-OS SDK for ESP8266. It uses many open source projects, such as lua-cjson and SPIFFS. Due to resource constraints, users need to select the modules relevant for their project and build a firmware tailored to their needs. Support for the 32-bit ESP32 has also been implemented.

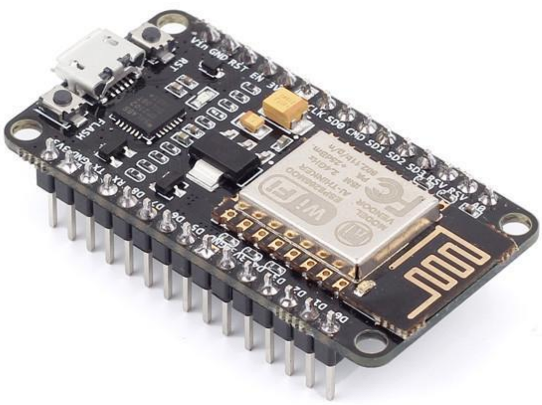

Figure 3.1: Node MCU

The prototyping hardware typically used is a circuit board functioning as a dual in-line package (DIP) which integrates a USB controller with a smaller surface-mounted board containing the MCU and antenna. The choice of the DIP format allows for easy prototyping on breadboards. The design was initially was based on the ESP-12 module of the ESP8266, which is a Wi-Fi SoC integrated with a Tensilica Xtensa LX106 core, widely used in IoT applications.

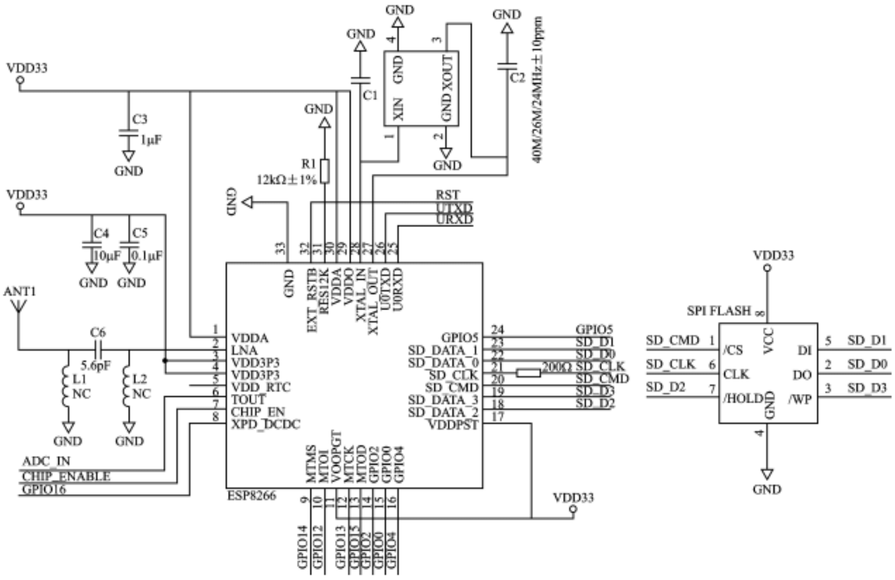

Figure 3.2: Node MCU Schematic Diagram

This an open source IoT platform. It includes firmware which runs on the ESP8266 Wi-Fi SoC from Express if Systems, and hardware which is based on the ESP-12 module. The term "Node MCU" by default refers to the firmware rather than the development kits. The firmware uses the Luascripting language. It is based on the eLua project, and built on the Espress if Non-OS SDK for ESP8266. Node MCU was created shortly after the ESP8266 came out. On December 30, 2013, Espressif Systems began production of the ESP8266. The ESP8266 is a Wi-Fi SoC integrated with a Tensilica Xtensa LX106 core, widely used in IoT applications (see related projects). Node MCU started on 13 Oct 2014, when Hong committed the first file of node mcu-firmware to GitHub. Two months later, the project expanded to include an open-hardware platform when developer Huang R committed the gerber file of an ESP8266 board, named devkit v0.9. Later that month, Tuan PM ported MQTT client library from Contiki to the ESP8266 SoC platform, and committed to Node MCU project, then Node MCU was able to support the MQTT IoT protocol, using Lua to access the MQTT broker. Another important update was made on 30 Jan 2015, when Devsaurus ported the u8glibto Node MCU project, enabling Node MCU to easily drive LCD, Screen, OLED, even VGA displays. In summer 2015 the creators abandoned the firmware project and a group of independent contributors took over. By summer 2016 the Node MCU included more than 40 different modules. Due to resource constraints users need to select the modules relevant for their project and build a firmware tailored to their needs.

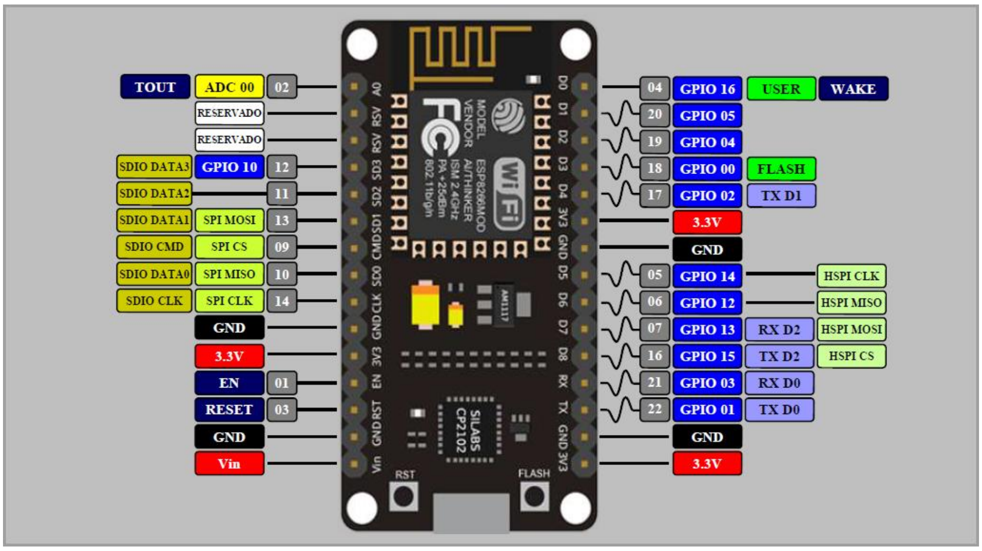

Figure 3.3: Node MCU Pin Out

Node MCU V3 ESP8266 ESP-12E is WiFi development board that helps you to prototype your IoT product with few Lua script lines, or through Arduino IDE. The board is based on ESP8266 ESP-12E variant, unlike other ESP-12E, you won’t need to buy a separate breakout board, usb to serial adapter, or even solder it to a PCB to get started, you will only need a usb cable (Micro USB).

Features

1. Communication interface voltage: 3.3V.
2. Antenna type: Built-in PCB antenna is available.
3. Wireless 802.11 b/g/n standard
4. WiFi at 2.4GHz, support WPA / WPA2 security mode
5. Support STA/AP/STA + AP three operating modes
6. Built-in TCP/IP protocol stack to support multiple TCP Client connections (5 MAX)
7. D0 ~ D8, SD1 ~ SD3: used as GPIO, PWM, IIC, etc., port driver capability 15mA
8. AD0: 1 channel ADC
9. Power input: 4.5V ~ 9V (10VMAX), USB-powered
10. Current: continuous transmission: ≈70mA (200mA MAX), Standby: <200uA
11. Transfer rate: 110-460800bps
12. Support UART / GPIO data communication interface
13. Remote firmware upgrade (OTA)
14. Flash size: 4MByte.

3.3 Switch Mode Power Supply (SMPS)

A switched-mode power supply (switching-mode power supply, switch-mode power supply, switched power supply, SMPS, or switcher) is an electronic power supply that incorporates a switching regulator to convert electrical power efficiently. Like other power supplies, an SMPS transfers power from a DC or AC source (often mains power) to DC loads, such as a personal computer, while converting voltage and current characteristics.

Unlike a linear power supply, the pass transistor of a switching-mode supply continually switches between low-dissipation, full-on and full-off states, and spends very little time in the high dissipation transitions, which minimizes wasted energy. A hypothetical ideal switched-mode power supply dissipates no power. Voltage regulation is achieved by varying the ratio of on-to-off time (also known as duty cycles). In contrast, a linear power supply regulates the output voltage by continually dissipating power in the pass transistor. This higher power conversion efficiency is an important advantage of a switched-mode power supply. Switched-mode power supplies may also be substantially smaller and lighter than a linear supply due to the smaller transformer size and weight.

Figure 3.4: SMPS

Switching regulators are used as replacements for linear regulators when higher efficiency, smaller size or lighter weight are required. They are, however, more complicated; their switching currents can cause electrical noise problems if not carefully suppressed, and simple designs may have a poor power factor.

12V 5A Industrial SMPS Power Supply – 60W – DC Metal Power Supply – Good Quality – Non Waterproof with Aluminum casing.

- Input Voltage: AC 100 – 264V 50 / 60Hz
- Output Voltage: 12V DC, 0-5A
- Output voltage: Adjustment Range: ±20%
- Protections: Overload / Over Voltage / Short Circuit
- Auto-Recovery After Protection
- Universal AC input / Full range
- 100% Full Load Burn-in Test
- Cooling by Free Air Convection
- High Quality and High Performance

- LED power supply with a metal body for hidden installation for LED lighting
- Design with Built-in EMI Filter, improve signal precision.
- Certifications: CE & RoHs

Switched-mode power supplies are classified according to the type of input and output voltages. The four major categories are:

- AC to DC
- DC to DC
- DC to AC
- AC to AC

A basic isolated AC to DC switched-mode power supply consists of:

- Input rectifier and filter
- Inverter consisting of switching devices such as MOSFETs
- Transformer
- Output rectifier and filter
- Feedback and control circuit

The input DC supply from a rectifier or battery is fed to the inverter where it is turned on and off at high frequencies of between 20 KHz and 200 KHz by the switching MOSFET or power transistors. The high-frequency voltage pulses from the inverter are fed to the transformer primary winding, and the secondary AC output is rectified and smoothed to produce the required DC voltages. A feedback circuit monitors the output voltage and instructs the control circuit to adjust the duty cycle to maintain the output at the desired level.

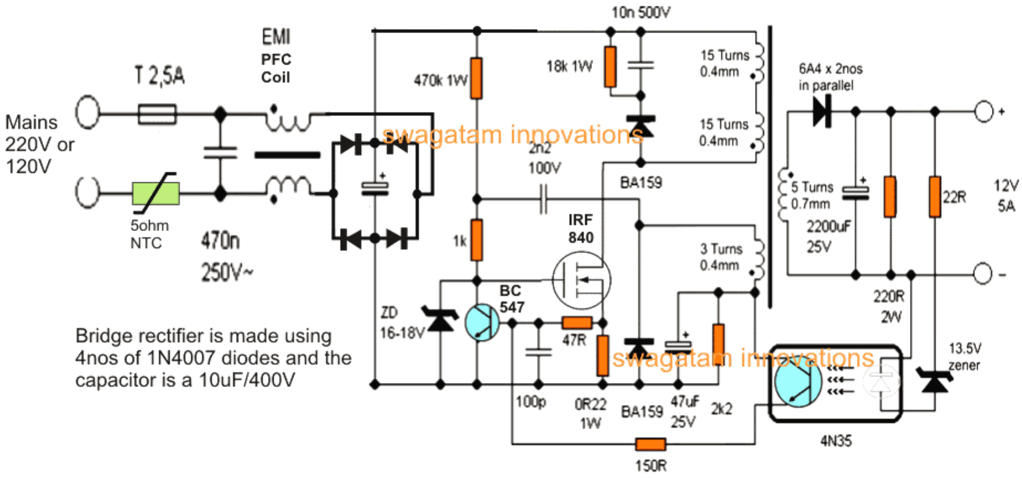

Figure 3.5: SMPS Circuit Design

Basic working concept of an SMPS

A switching regulator does the regulation in the SMPS. A series switching element turns the current supply to a smoothing capacitor on and off. The voltage on the capacitor controls the time the series element is turned. The continuous switching of the capacitor maintains the voltage at the required level.

Design basics

AC power first passes through fuses and a line filter. Then it is rectified by a full-wave bridge rectifier. The rectified voltage is next applied to the power factor correction (PFC) pre-regulator followed by the downstream DC-DC converter(s). Most computers and small appliances use the International Electro technical Commission (IEC) style input connector. As for output connectors and pin outs, except for some industries, such as PC and compact PCI, in general, they are not standardized and are left up to the manufacturer.

There are different circuit configurations known as topologies, each having unique characteristics, advantages and modes of operation, which determines how the input power is transferred to the output. Most of the commonly used topologies such as fly back, push-pull, half bridge and full bridge, consist of a transformer to provide isolation, voltage scaling, and multiple output voltages. The non-isolated configurations do not have a transformer and the power conversion is provided by the inductive energy transfer.

Advantages of switched-mode power supplies:

- Higher efficiency of 68% to 90%
- Regulated and reliable outputs regardless of variations in input supply voltage
- Small size and lighter
- Flexible technology
- High power density

Disadvantages:

- Generates electromagnetic interference
- Complex circuit design
- Expensive compared to linear supplies

Switched-mode power supplies are used to power a wide variety of equipment such as computers, sensitive electronics, battery-operated devices and other equipment requiring high efficiency

Switch Mode Power Supply

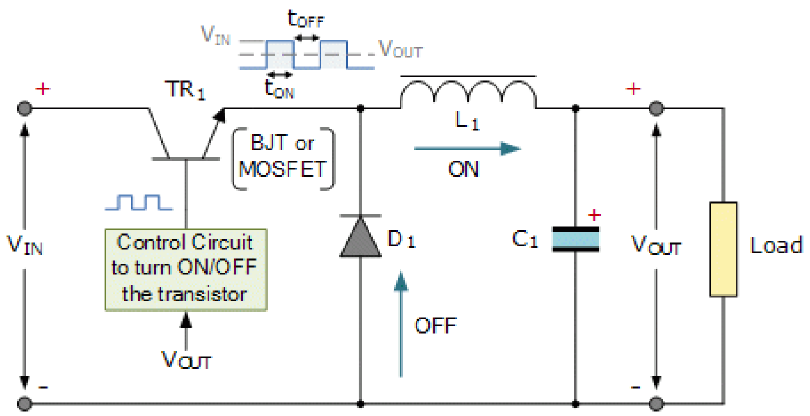

Figure 3.6: Power Supply Connection

Linear voltage IC regulators have been the basis of power supply designs for many years as they are very good at supplying a continuous fixed voltage output. Linear voltage regulators are generally much more efficient and easier to use than equivalent voltage regulator circuits made from discrete components such a zener diode and a resistor, or transistors and even op-amps. The most popular linear and fixed output voltage regulator types are by far the positive output voltage series, and the 79 negative output voltage series. These two types of complementary voltage regulators produce a precise and stable voltage output ranging from about 5 volts up to about 24 volts for use in many electronic circuits.

There is a wide range of these three-terminal fixed voltage regulators available each with its own built-in voltage regulation and current limiting circuits. This allows us to create a whole host of different power supply rails and outputs, either single or dual supply, suitable for most electronic circuits and applications. There are even variable voltage linear regulators available as well providing an output voltage which is continually variable from just above zero to a few volts below its maximum voltage output.

Most D.C. power supplies comprise of a large and heavy step-down mains transformer, diode rectification, either full-wave or half-wave, a filter circuit to remove any ripple content from the rectified D.C. producing a suitably smooth D.C. voltage, and some form of voltage regulator or stabilizer circuit, either linear or switching to ensure the correct regulation of the power supplies output voltage under varying load conditions. Then a typical D.C. power supply would look something like this:

Typical DC Power Supply

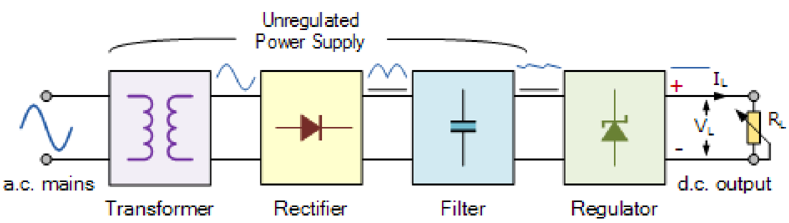

Figure 3.7: DC Power Supply Step

These typical power supply designs contain a large mains transformer (which also provides isolation between the input and output) and a dissipative series regulator circuit. The regulator circuit could consist of a single zener diode or a three-terminal linear series regulator to produce the required output voltage. The advantage of a linear regulator is that the power supply circuit only needs an input capacitor, output capacitor and some feedback resistors to set the output voltage.

3.4 Laser Light

A laser is a device that emits light through a process of optical amplification based on the stimulated emission of electromagnetic radiation. The word "laser" is 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 which is *coherent*. 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 and lidar (light detection and ranging). Lasers can also have high temporal coherence, which allows them to emit light with a very narrow spectrum. Alternatively, temporal coherence can be used to produce ultrashort pulses of light with a broad spectrum but durations as short as a femtosecond.

Figure 3.8: Laser Light

3.5 Flame Sensor

The flame sensor can detect flame and infrared light sources with wavelengths ranging from 760 nm to 1100 nm. It uses the LM393 comparator chip, which gives a clean, stable digital output signal and driving ability of 15 mA. This flame detector that can be used in fire alarms and other fire detecting devices.

Specifications

- LM393 comparator chip
- Detection Range: 760 nm to 1100 nm
- Operating Voltage: 3.3 V to 5 V
- Maximum Output Current: 15 mA
- Digital Outputs: 0 and 1
- Detection Angle: about 60 degrees
- Adjustable sensitivity via potentiometer

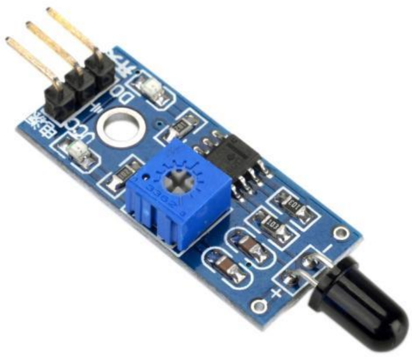

Figure 3.9: Flame Sensor

3.6 MQ 2 Gas Sensor

The utility model can be used for gas leakage monitoring devices in families and factories, and is suitable for the detection of liquefied petroleum gas, butane, propane, methane, Hydrogen, smoke, etc. This is a very easy to use low cost semiconductor Gas sensor Module with analog and digital output.

Figure 3.10: MQ 2 Gas Sensor

Features:

- Adopt high quality double panel design, with power indication and TTL signal output indication.
- It has DO switch signal (TTL) output and AO analog signal output.
- TTL output valid signal is low level. When the output is low, the signal light is on, and the micro controller or relay module can be directly connected.
- The analog output voltage increases with the concentration, the higher the voltage.
- It has better sensitivity to liquefied petroleum gas, natural gas, urban gas and smoke.
- MQ-2 MQ2 Smoke Gas LPG Butane Methane Sensor Detector Module
- With four screw holes, easy to locate.
- Product size: 32 (L), *20 (W), *22 (H)
- With long service life and reliable stability.
- Fast response recovery features

Specifications:

- Input voltage: DC5V
- Power dissipation (current): 150mA
- DO output: TTL, numeric quantities 0 and 1 (0.1 and 5V)

- AO output: 0.1-0.3V (relatively pollution-free), the highest concentration of about 4V voltage
- Special reminder: after the sensor is energized, you need to preheat 20S or so, the data to be stable, sensor heating is a normal phenomenon, because the internal heating wire, if hot, it is not normal.

Connection mode:

- VCC: power supply positive (5V)
- GND: power supply negative pole
- DO:TTL switch signal output
- AO: analog signal output
- Functions: This version supporting test procedures
- Using chips: AT89S52
- Crystal oscillator: 11.0592MHZ
- Since this Gas Sensor module is sensitive to smoke it can be used in for fire detection. MQ2 Gas Sensor is also sensitive to flammable/combustible gasses like LPG, Propane & Hydrogen.
- Baud rate: 9600

3.7 5V Regulator IC

Voltage sources in a circuit may have fluctuations resulting in not providing fixed voltage outputs. A voltage regulator IC maintains the output voltage at a constant value. 7805 IC, a member of 78xx series of fixed linear voltage regulators used to maintain such fluctuations, is a popular voltage regulator integrated circuit (IC). The xx in 78xx indicates the output voltage it provides. 7805 IC provides +5 volts regulated power supply with provisions to add a heat sink.

7805 IC Rating

- Input voltage range 7V- 35V
- Current rating Ic = 1A
- Output voltage range VMax=5.2V ,VMin=4.8V

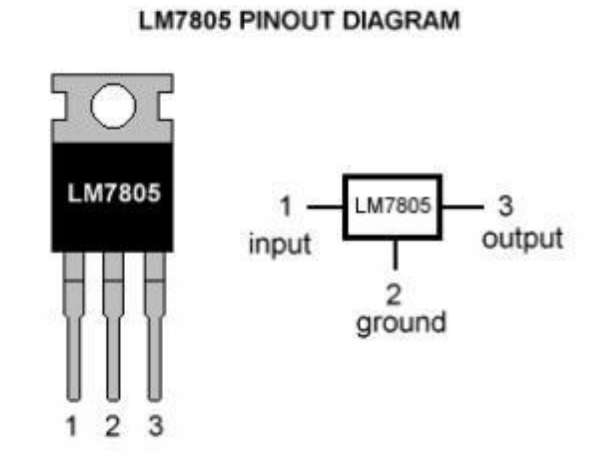

Figure 3.11: 5V Regulator IC

3.8 Buzzer

Piezo elements are actually one of the coolest crystals you’ll play with. Flex them, they generate a voltage (pretty high, actually). Pass power through them, and they’ll flex. Do it fast enough, and they’ll start to make a sound! So besides making annoying little beepy noises, you could use it as a sensor to detect a knock or other similar vibration.

Specifications

- Operating Voltage: 1.0 ~ 20.0V
- Rated Voltage: 3.0V
- Diameter: Ø12.5mm
- Total Height: 6.3mm
- Capacitance: 15,000pF
- Current Consumption: ≤2mA

- Resonance Frequency : 4,000Hz
- Sound Pressure Level at 10cm: ≥75db
- Self Drive: No

Figure 3.12 : Buzzer

3.9 Arduino Software

An intelligent micro-controller unit called the Arduino Uno can be programmed with the Arduino software. There is no need to install any software other than the Arduino first. From the Tools Board menu (according to your on-board micro-controller) select "Arduino Unio A" using the hardware programmer.

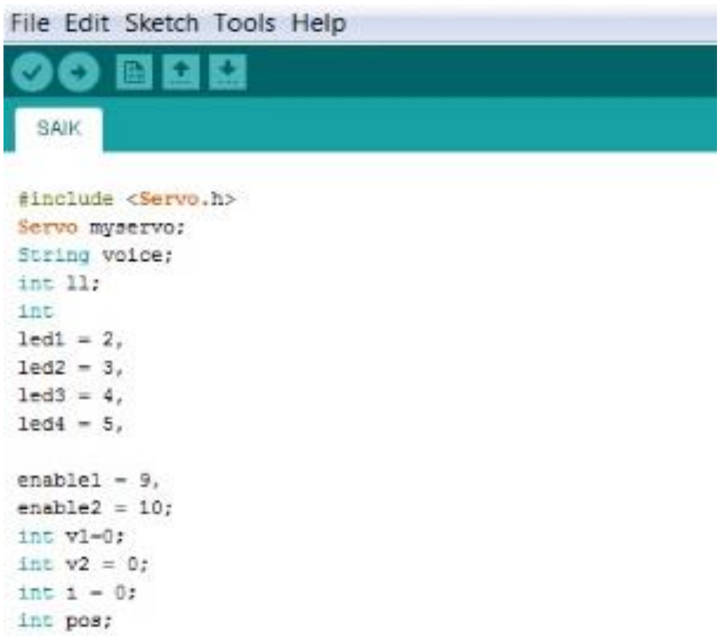

Figure 3.13: Arduino Software Interface IDE

The communication uses the native STK 500 protocol (reference C header file). We can bypass the boot loader and program the micro-controller under the ICSP (In Circuit Serial Programming) heading. Atmeg16U2 firmware source code (or 8U2 on The Rev1 and Rev2) Atmega 16U2/8U2 boards are loaded with a DFU boot loader, which can be enabled at: On the Rev 1: board, attach a solder jumper to the back of the board. Rev 2 or later: There is a resistor that pulls the 8U2/16U2 HWB wires to ground, making it easy to put in DFU mode. The Arduino Uno is the latest smart micro-controller unit and has Several advantages for communicating with other Arduino computers or other micro-controllers.

The ATMA 328 provides URT TTL with Communication Protocol (5V), available in digital PIN 0 - (RX) for data retrieved with PIN No. 1 (TX) for data transmission. The system port communicates via USB Atimega 16U2 in the port and comes out as a low-end port with computer software. '16U2 firmware uses standard USB CMM driver and no external drivers required. Anyway, Windows needs an .inf file.The Arduino file system contains a serial viewer that allows sending easy text data to and from Arduino boards. The RX and TX connectors will flash on the board when transferring data via USB-to-serial connector and USB connection to the computer (but not for serial communication on pins 0 and 1).

The software system library allows seamless communication within any digital PIN. The Atmeg 328 supports I2C information communication (TWI) and SPI. The Arduino software includes a wire library to support the use of the I2C car. Arduino programs are written in C or C ++ and the program code written for Arduino is called Sketch. Arduino IDE uses GNU and AVR LBC toolkit to compile programs, as well as upload programs using Android. For example, software for Arduino can be developed using the Arduino platform using Atmel micro-controllers, around the development of Atmel, AVR Studio or even the new Atmel Studio.

3.10 Proteus Software

The Proteus Design Suite is a software component used for automated electronic design. Engineers and electronics engineers use schematic-based applications and electronic devices to create printed circuit boards. The first version of the Proteus design suite was called PC-B, and was written in 1986 by John Jameson, president of the DOS company. Windows eventually followed the schematic retention support in 1990 with the help of local ports. The mixing pepper pepper simulation mode was first integrated into Proteus in 1996 and the Micro-controller simulation came to Proteus in 1998. 2002 Shape-based auto routing was added in 2002 and 2006. Another major product update is 3D plant visualization. Recently, IDE dedicated to simulation was added in 2011 and MCAD import / export included in 2015. Support for faster design was added in 2017. The LED products featured are usually biennial, but the working package is left to function as necessary.

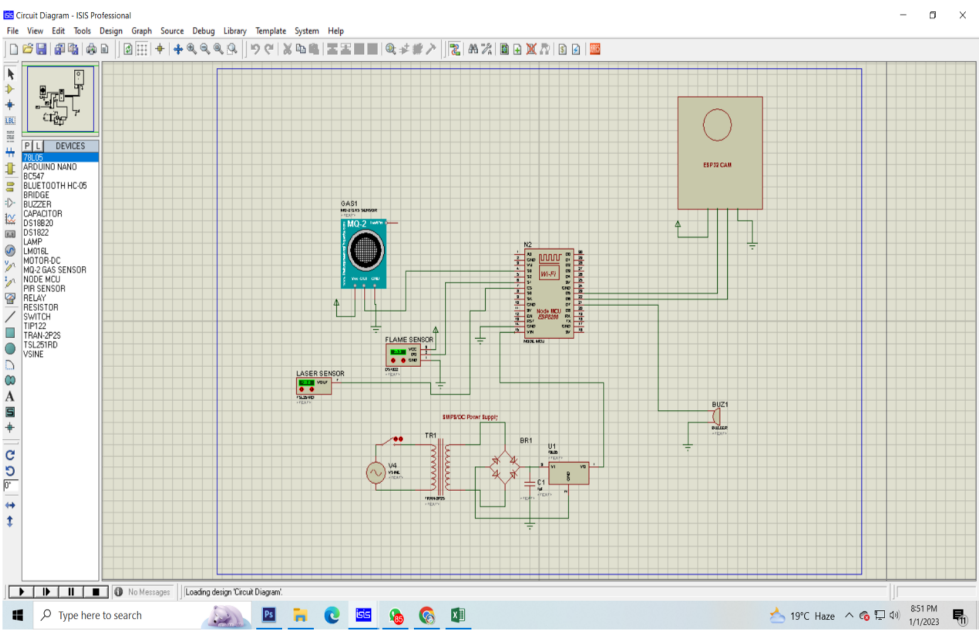

Figure 3.14: Proteus Software Interface

3.11 Blynk App

Blynk is an Internet-of-Thing's platform designed to make development and implementation of smart IOT devices quick and easy. It can be used to read, store, and visualize sensor data and control hardware remotely.

Internet of Things has been all the buzz lately and more and more devices are being talking to internet every day. With the rise of such amazing technology, the risk of security has also increased substantially. Some of the major concerns in IOT are:

- If IOT devices are sending your data to the internet, the communication needs to be closed and encrypted which cannot be possible without using a dedicated and closed server which is really hard to manage.
- The IOT devices also need to be responsive and again, that is not possible without a server with low latency and high responsiveness.
- In IOT, the platform needs to be compatible with many different types of hardware architecture and devices, so that it doesn't restrict its users with single type of hardware with limited capabilities.

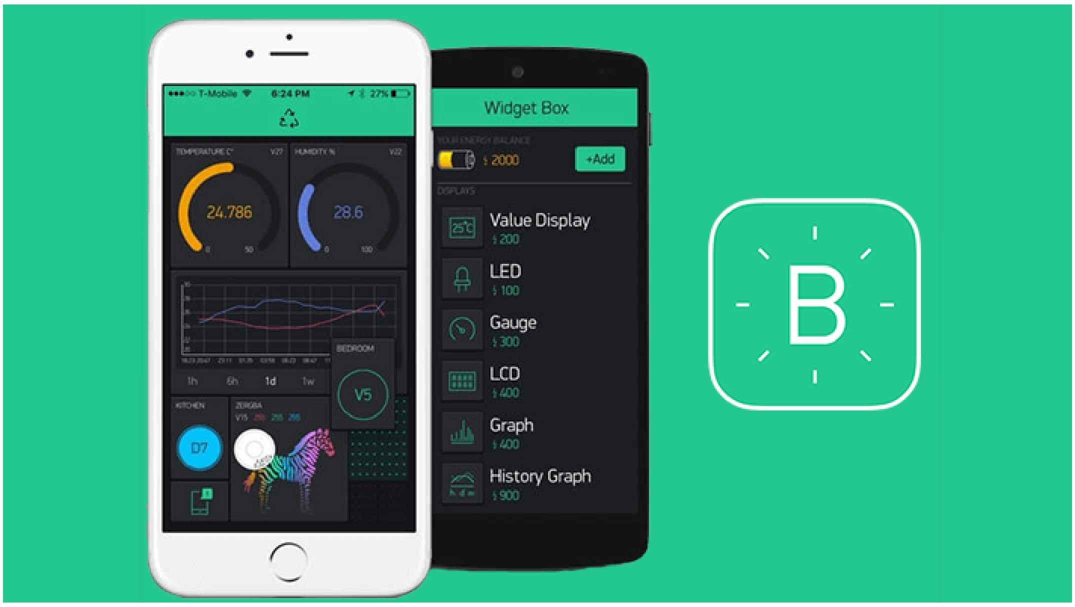

Figure 3.15: Blynk App

Keeping in view the problems mentioned above, Blynk is the perfect solution for all these problems. Blynk consists of the following three major components:

Blynk App – The mobile app developed by Blynk works as a control panel for visualizing and controlling your hardware. It is available for both Android and IOS. The app offers a very productive interface and various different widgets for different purposes. Blynk works on a currency of its own called energy. New users get 2000 amount of Blynk energy with a free Blynk account and this energy is used to buy and deploy widgets in the projects.

Blynk Server – The most amazing component of the Blynk Platform which makes it all possible is the Blynk Server. Blynk offers a secure, responsive and centralized cloud service through its server which allows all of this communication between the devices. The Blynk server is also available as open source so you can literally make your own server and make it even more secure with a little tinkering.

Blynk Library – The key feature of Blynk platform which makes it scalable and amazing, is the Blynk Library. The Blynk Library makes it possible to connect your hardware and get it up and running in a blink. The support for multiple hardware devices including Arduino, ESP8266 and Raspberry Pi is included in the library and it also makes it possible to connect with hardware through many different ways of communication like Wi-Fi, Bluetooth, BLE, USB and GSM.

Features:

- Similar API & UI for all supported hardware & devices
- Connection to the cloud using:
    - Wi-Fi
    - Bluetooth and BLE
    - Ethernet
    - USB (Serial)
    - GSM
    - Set of easy-to-use Widgets

- Direct pin manipulation with no code writing
- Easy to integrate and add new functionality using virtual pins
- History data monitoring via Super Chart widget
- Device-to-Device communication using Bridge Widget
- Sending emails, tweets, push notifications, etc.

CHAPTER 4

METHODOLOGY

4.1 Our methodologies for the project

Our methodologies for the project:

- Creating an idea for design and construction of **Automated Home Surveillance System Using IOT**. And designing a block diagram & circuit diagram to know which components we need to construct it.
- Collecting all the components and programming the micro-controller to control the whole system.
- Setting up all the components in a PCB board & then soldering. Lastly, assembling all the blocks in a board and to run the system & for checking purposes.

4.2 System Design and Components

The main processing brain of the system is the Node MCU. Firstly, to run the micro-controller switch mood power supply the main voltage. Then the system will be on and ready for operation. Here this system will able to measure the system condition and able to take command.Here we use SMPS, Node MCU, ESP32 Camera, laser light, MQ2 Sensor,Flame Sensor, Buzzer etc. All of this equipments are combined work together and full fill our required as we desire.

4.3 Block Design Specifications

In this diagram we will show by block the individual parts.

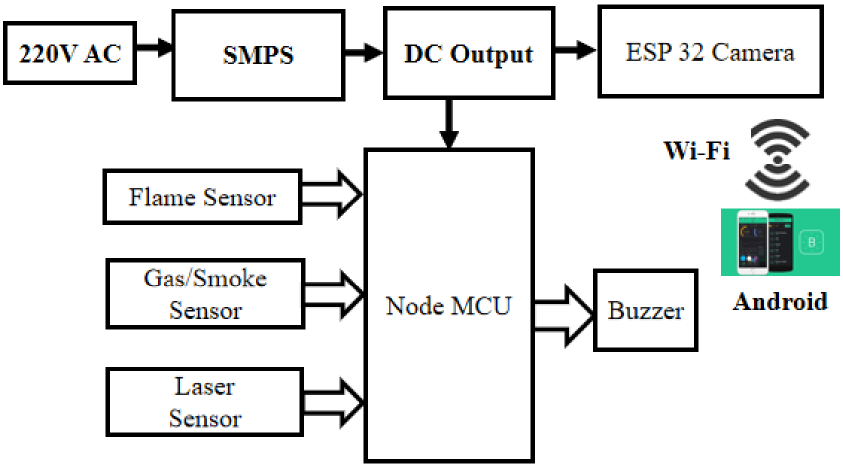

Figure 4.1: Block Diagram diagram of a Torch

4.4 Circuit Design Analysis

The schematic diagram here is representing the electrical circuit and the components of our System. Here we connect equipment with he smart wire connection.

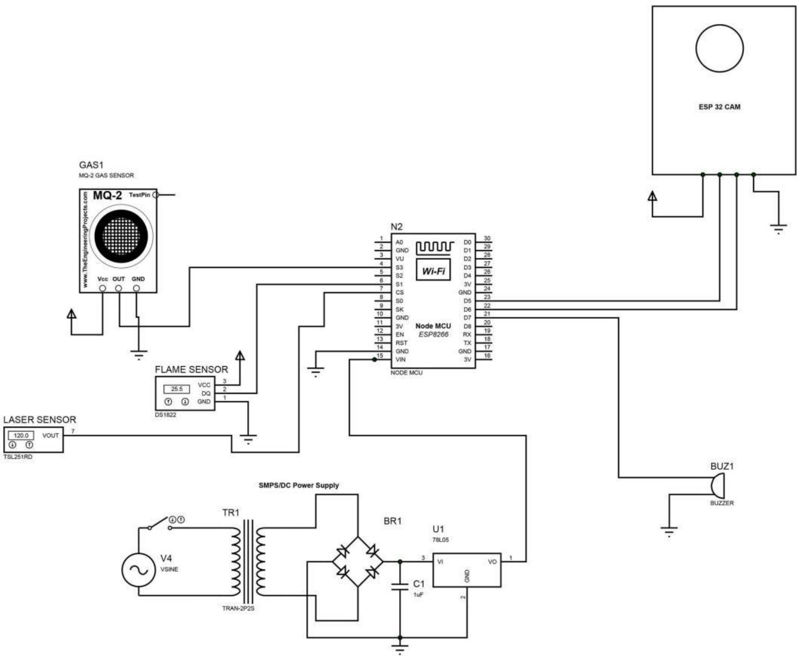

Figure 4.2: Circuit Diagram of our system

4.5 Working Principle

The way our Advance Home Security Surveillance System that we take the 220V rms from the supply voltage and then give it to the SMPS, the SMPS has a step-down transformer inside that stepped that voltage down to 12V. This 12V supply is still alternating in nature so now, we use a Full Wave Bridge Rectifier to rectify that output. Now we use Capacitors to smooth the curve and turn the 12V pulsating current to pure 12V direct current. But this 12V dc is still much high for our project. So, we use a 7805 5V Regulator IC to make that voltage come down to 5V. This power is directly connected with the main circuit. Here we use node MCU for IoT communication, gas sensor, flame sensor, laser sensor, SMPS, ESP 32 camera. When a person come inside of our home at night then laser sensor detect object and alert home authority. If there create gas leakage and flame then will send in mobile apps and buzzer will be ring. And ESP 32 camera will show web view in mobile. This the main approach of our system. This is the main procedure of our system.

4.6 Experimental Setup of Our System

After completing our block diagram and circuit diagram we connect the all equipments together then we make made a home structure with PCB Board and fitted the sensor and camera where we need. Here is our structural setup of our design is given below -

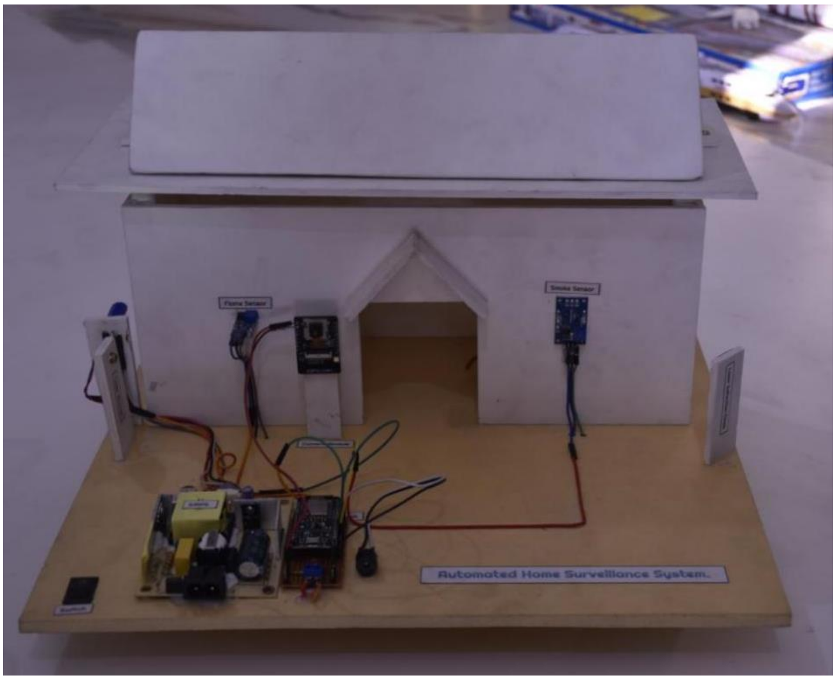

Figure 4.3: Our System Structural set up.

CHAPTER 5
RESULT AND DISCUSSION

5.1 Discussion

While working on our project, we did face some difficulties as it is a very complex system but the end results, we came up with were quite satisfactory. We have put the whole system through several tasks to validate our work and also have taken necessary notes for future improvements. Some future recommendations that we have involves improvement in system design and wiring, adding features for more efficient.

5.2 Result

Now, it's time to talk about the results. We have written our commands using the Arduino IDE and the following things can happen:

- After power on the system connected with Wi-Fi then able to work.
- Then when we make fire in-front of flame sensor then the system send a notification on mobile apps.
- When we come closer to home are then laser sensor detect object and alert the home authority.
- Then when we sense flame to MQ2 sensor then the sensor detect smoke and send notification on mobile apps.
- And camera will show the in-front of the door human and show the web view on mobile.
- All kind of incident our system ring buzzer and alert to user.

5.3 Advantages

There are certainly many advantages of our project and some of the major ones have been given below:

- Ensure safety and security
- Standards living status
- Unnecessary Energy loss will be prevented.
- Cost Effective.

- Saves time and physical work.
- This project is easy to use.
- Easy to use by smart mobile.
- Smart home automation.

5.4 Disadvantages

This project has some disadvantages. These are –

- No extra power supply
- Must be cover with internet coverage.
- It may take delay in work for weak internet.

5.5 Application

Some of the application areas of the project have been pointed out below:

- Hospital & Clinic.
- Class rooms.
- House.
- Commercial Place.
- Shopping Mall.

CHAPTER 6
CONCLUSION

6.1 Conclusion

We are now in the digital era and with the improvements of technology, our energy consumption rate has gone very high as well. This project firstly, controls many loads of the house by turning the loads on or off by the commands of the user with blink app . The project doesn’t cost that much to build and it’s very easy to use. It was built with the intention that everyone should be able to use it for reduce human use, save electricity and home automation. Our project is in its pilot phase and now we doing practical tests with it to validate our work and taking notes for future improvements as well. At last we can say that this project is necessary for our country and we hope we can succeed on our mission of making our homes smarter.

6.2 Future Scope

Recommendation for future work to improvise the project is given below -

- In future, we are thinking about adding password based door lock system.
- In future we are thinking about adding voice control device to control our house load.
- In future, we are thinking about 100% accuracy.

REFERENCE

[1]. Govinda K and Sai Krishna Prasad K and Sai Ram Susheel 2014 Intrusion detection system for smart home using laser rays International Journal for Scientific Research & Development (IJSRD) 2 176-78

[2]. Karri V and Daniel Lim J S 2005 Method and Device to Communicate via SMS after a Security Intrusion 1st International Conf. on Sensing Technology Palmerston North New Zealand 21-23

[3]. Jayashri B and Arvind S 2013 Design and Implementation of Security for Smart Homebased on GSM technology International Journal of Smart Home 7 201-08

[4]. Sowjanya G and Nagaraju S 2016 Design and Implementation Of Door Access Control And Security System Based On IOT Inventive Computation Technologies (ICICT),International Conference on Inventive

[5]. Cristian C, Ursache A, Popa D O and Florin Pop 2016 Energy efficiency and robustness for IOT: building a smart home security system Faculty of Automatic Control and Computers University Politehnica of Bucharest, Bucharest, Romania 43

[6]. Lee C T, Shen T C, Lee W D and Weng K W 2016 A novel electronic lock using optical Morse code based on the Internet of Things Proceedings of the IEEE International Conference on Advanced Materials for Science and Engineering eds. Meen, Prior & Lam

[7]. Pooja P, Mitesh P, Vishwa P and Vinit N 2016 Home Automation Using Internet of Things Imperial Journal of Interdisciplinary Research (IJIR) 2 648- 51

[8]. Anitha A, Paul G and Kumari S 2016 A Cyber defence using Artificial Intelligence International Journal of Pharmacy and Technology 8 25352-57

[9]. Anitha A, Kalra S and Shrivastav 2016 A Cyber defence using artificial home automation system using IoT International Journal of Pharmacy and Technology 8 25358-64

[10]. Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana, "IoT Based Smart Security and Home Automation System"

[11]. Vamsikrishna Patchava, Hari Babu Kandala,P Ravi Babu,"A Smart Home Automation technique with Raspberry Pi using IoT",2015

[12]. Ian Summerville, “Software Implementation and Testing”, Software Engineering Pearson Education Asia, Sixth Edition, 60-62 (Ch.3) Third Indian Reprint 2003

APPENDIX

Program Code:

```
int data1 = D5;
int data2 = D6;
int data3 = D7;
int buzzar = D1;

#define BLYNK_TEMPLATE_ID "TMPLWXsEtwJ5"
#define BLYNK_DEVICE_NAME "project"
#define BLYNK_AUTH_TOKEN "OcVzH8xgbbgIdUO9wBCyfJYIfPYdjd4R"
// Comment this out to disable prints and save space
#define BLYNK_PRINT Serial


#include <ESP8266WiFi.h>
#include <BlynkSimpleEsp8266.h>

char auth[] = BLYNK_AUTH_TOKEN;

// Your WiFi credentials.
// Set password to "" for open networks.
char ssid[] = "abcde";
char pass[] = "123456789";

void setup()
{
  // Debug console
  Serial.begin(115200);
  pinMode(D7,INPUT);
  pinMode(D6,INPUT);
  pinMode(D5,INPUT);
  pinMode(D1,OUTPUT);
  Blynk.begin(auth, ssid, pass);
  // You can also specify server:
  //Blynk.begin(auth, ssid, pass, "blynk.cloud", 80);
  //Blynk.begin(auth, ssid, pass, IPAddress(192,168,1,100), 8080);
}
WidgetLCD lcd(V1);

void loop()
{
  Blynk.run();
int fire = digitalRead(D5);
int laser = digitalRead(D6);
int smoke = digitalRead(D7);
```

```
  lcd.print(0, 0, "System Normal   "); // use: (position X: 0-15, position Y: 0-1,
"Message you want to print")

if(fire == LOW ){
  lcd.print(0, 0, "Fire Detected   "); // use: (position X: 0-15, position Y: 0-1, "Message
you want to print")

digitalWrite(D1,HIGH);
delay(3000);
}
if(fire == HIGH){
digitalWrite(D1,LOW);

}
if(smoke == LOW ){

  lcd.print(0, 0, "Smoke Detected   "); // use: (position X: 0-15, position Y: 0-1,
"Message you want to print")

digitalWrite(D1,HIGH);
delay(2000);
}
if(smoke == HIGH){

}

if(laser == HIGH ){

  lcd.print(0, 0, "Intruder Alert"); // use: (position X: 0-15, position Y: 0-1, "Message
you want to print")

digitalWrite(D1,HIGH);
delay(2000);
}

if(laser == LOW){
}
}
```