

HIDDEN CAMERA DETECTOR & JAMMER USING IOT

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in Computer Science and
Engineering
by

KUCHIBATLA SRI KAMESWARA PRASAD (37110388)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC

JEPPIAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600 119

MARCH - 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with 'A' grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai - 600 119

www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this project report is the bonafide work of **KUCHIBATLA SRI KAMESWARA PRASAD (37110388)** who carried out the project entitled **'HIDDEN CAMERA DETECTOR & JAMMER USING IOT'** under my supervision from **August 2020 to March 2021**.

Internal Guide

DR. A. PRAVIN, M.E, PH. D.,

Head of the Department

Submitted for Viva voce Examination held on

Internal Examiner

Examiner

External

DECLARATION

I **KUCHIBATLA SRI KAMESWARA PRASAD** hereby declare that the Project Report entitled **"HIDDEN CAMERA DETECTOR & JAMMER USING IOT"** is done by me under the guidance of **DR. A. PRAVIN, M.E., PH. D.**, Department of Computer Science and Engineering at Sathyabama Institute of Science and Technology is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala, M.E., Ph.D., Dean, School of Computing, Dr. S. Vigneswari, M.E., Ph.D., and Dr. L. Lakshmanan, M.E., Ph.D., Heads of the Department of Computer Science and Engineering** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **DR. A. PRAVIN, M.E., Ph.D.,** for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

In our day-to-day life the usage of mobile phones has been increased in restricted area such as exam venues, places of important meeting, offices, conference halls, prison etc. and the hidden wireless camera in trial rooms and hotels, public toilets. The radio frequency signals are transmitted from wireless camera and mobile phone during the video transmission, incoming call and outgoing call, text messages from one gadget to another. The detector will detect the transmitted signal and then it is gives as input to AT mega 8 microcontroller. As soon as the Arduino microcontroller receives the signal, it will turn ON the beep alarm and the information will be displayed on the LCD display and also sends the message like mobile detected with location, room number etc. This system will be used to detect the mobile phones and the wireless hidden camera present in a room by the radio frequency signals which are transmitted by them.

TABLE OF CONTENT

S.NO	TITLE	PAGE.NO
	ABSTRACT	v
	LIST OF FIGURES	viii
1	INTRODUCTION	01
	1.1 PROBLEM STATEMENT	01
	1.2 SYNOPSIS	01
2	LITERATURE REVIEW	03
3	AIM AND SCOPE	05
	3.1 AIM	05
	3.2 SCOPE	05
	3.3 EXISTING SYSTEM	05
	3.4 PROPOSED SYSTEM	05
4	SYSTEM DESIGN AND METHODOLOGY	07
	4.1 SYSTEM ARCHITECTURE	07
	4.2 SYSTEM REQUIREMENTS	07
	4.2.1 HARDWARE USED	07
	4.2.2 SOFTWARE USED	07
	4.3 METHODOLOGY	08
	4.4 MODULES	08
	4.4.1 ARDUINO	08
	4.4.2 IR SENSOR	14
	4.4.3 BLUETOOTH MODULE	18
	4.4.4 RF DETECTOR	19
	4.4.5 POWER SUPPLY	22
	4.5 SOFTWARE SETUP	34
	4.5.1 ARDUINO IDE	34
	4.5.2 ANDROID APPLICATION	37
5	RESULTS AND DISCUSSION	40
6	CONCLUSION AND FUTURE ENHANCEMENT	44
	6.1 CONSLUSION	44
	6.2 FUTURE ENHANCEMENT	44

REFERENCE	45
APPENDIX	47
SOURCE CODE	47
JOURNAL PAPER	59
PLAGIARISM REPORT	65

LIST OF FIGURES

S.NO	TITLE	PAGE.NO
4.1	ARCHITECTURE DIAGRAM	14
4.2	ARDUINO BOARD	18
4.3	IR SENSOR CIRCUIT DIAGRAM	21
4.4	IR IMAGING	21
4.5	BLUETOOTH MODULE	22
4.6	RF DETECTOR	22
4.7	STEPS INVOLVED IN POWER SUPPLY	23
4.8	POWER SUPPLY UNIT CIRCUIT DIAGRAM	23
4.9	CIRCUIT DIAGRAM	24
4.10	AC TO DC SUPPLY	24
4.11	POWER SUPPLY	25
4.12	HIGH VOLTAGE POWER SUPPLY	25
4.13	SWITCH MODE MOBILE PHONE CHARGER	26
4.14	CHOOSE THE COMPONENTS TO INSTALL	26
4.15	CHOOSE THE INSTALLATION DIRECTORY	61
4.16	EXTRACTION OF FILES	61
5.1	CAMERA CONNECTED WITH WI-FI MODULE	62
5.2	CAMERA MODULE WITH POWER SUPPLY	62
5.3	SERVER SIDE	63
5.4	CLIENT SIDE	63
5.5	DETECTION OF CAMERA	64
5.6	JAMMING THE CAMERA	64

CHAPTER-1

INTRODUCTION

PROBLEM STATEMENT:

Internet connected cameras have become a pervasive feature in the world. Most modern mobile phones contain at least one camera as do many laptops. Additionally cheap Wi-Fi connected cameras are easy to obtain and deploy. In addition to these devices, there are a variety of hidden cameras that are designed to evade visual detection. The cost of obtaining and deploying such devices continues to drop as retailers such as Amazon include Surveillance Camera and Hidden Camera shopping categories that include thousands of results.

While Internet-connected cameras bring convenience to the owners, they also create security risks. Weak security mechanisms allow adversaries to exploit those IoT devices and have total control over such devices. In 2016, Mirai malware took advantage of the weak password settings of IoT devices and compromised 3.5 million devices, many of which were Wi-Fi cameras.

The infected devices were located globally, including most of the countries in Europe, Asia, and North and South America . While one of the most widespread, the Mirai botnet is just one of many examples of cameras being compromised. Furthermore, Wi-Fi cameras have been installed to spy on people in environments such as hotel rooms and AirBnB rentals.

SYNOPSIS:

Given the ease of which cameras can collect information on people without them knowing it, there is very little that has been done to detect cameras that are spying on people. Previous work in detecting hidden cameras has generally relied on being indoors, having significant control of the environment, or performing significant manual inspection with custom hardware. In this paper, we extend our work in automatically detecting Wi-Fi cameras to mitigate the delayed-transmission attacker model. The approach works both indoors and outdoors in

large or small areas and can be accomplished with common computing equipment such as a mobile phone or laptop.

The issue of hidden cameras at public places became a severe threat to people these days.

The cameras are secretly put up in the changing room, theatres, restrooms and other public places which affect the privacy of the people. Some people might argue that cameras are easy to find and this is unnecessary, but this is really a tough job to find a hidden camera in a room. Most of the camera is wireless and hence became very easy to hide. Manually, finding a camera is almost impossible. This is based on the fact that almost all the camera devices work within the frequency range 0.1GHz to 3 GHz. By this, we can prohibit the unauthorized use of the camera by using a detector that senses the presence of hidden camera as they radiate RF signal for transmission. By this, we can even detect the presence of small video cameras whose frequency range is 0.05GHz to 3GHz (which is a quite difficult task as we need to differentiate the video signals from WIFI signal and TV signal). The detector detects the RF signal and the signal information is indicated by the LED light and provides us an option to stop the camera data transmission by generating the same type of interference so that the receiver or base station will not understand which signal to receive.

This also has an eyeglass which can be used to detect the camera hidden with alternating pulsating frequency or if recording camera is used instead of a camera which uses Wi-Fi to transmit information. The principle on which this hidden spy camera detector works is alternating pulsating laser frequency using which hidden cameras can be detected as flashing red light once viewed through optical glass viewport.

CHAPTER -2

LITERATURE SURVEY

Human group activities detection in multi-camera CCTV surveillance videos is a pressing demand on smart surveillance. Previous works on this topic are mainly based on camera topology inference that is hard to apply to real-world unconstrained surveillance videos. In this paper, we propose a new approach for multi-camera group activities detection. Our approach simultaneously exploits intra-camera and inter-camera contexts without topology inference. Specifically, a discriminative graphical model with hidden variables is developed. The intra-camera and inter-camera contexts are characterized by the structure of hidden variables. By automatically optimizing the structure, the contexts are effectively explored. Furthermore, we propose a new spatiotemporal feature, named vigilant area (VA), to characterize the quantity and appearance of the motion in an area. This feature is effective for group activity representation and is easy to extract from a dynamic and crowded scene. We evaluate the proposed VA feature and discriminative graphical model extensively on two real-world multi-camera surveillance video data sets, including a public corpus consisting of 2.5 h of videos and a 468-h video collection, which, to the best of our knowledge, is the largest video collection ever used in human activity detection. The experimental results demonstrate the effectiveness of our approach.

This paper describes the mechanical design and a cognition system for a novel concept-of-camera robotic assistant. The system combines the advantages of intra-abdominal devices and autonomous camera navigation. The robotic assistant is composed of a magnetic intra-abdominal camera robot with two internal cable-driven degrees of freedom and an external robot that handles an external magnet. The intelligence of the robot is implemented in a cognitive architecture based on a long-term memory that stores the robot's knowledge and learning capabilities to improve the robot's behavior. The navigation strategy combines a reactive control based on instrument tracking and a proactive control based on predefined

behaviours, depending on the actual state of the task. The robot's learning capabilities include a semantic customization, to adapt the camera's behavior to the surgeon's preferences, and reinforcement learning, to improve the camera navigation strategy. This paper details both the hardware implementation of the system and the software implementation in a robotic operating system architecture. The cognition system and the performance of the cable-driven mechanism have been validated with a set of in vitro experiments. Moreover, the camera robot has been evaluated through an in-vivo experiment in a pig.

CHAPTER-3

AIM & SCOPE OF PRESENT INVESTIGATION

AIM

The primary aim of the project is to detect and jam the hidden cameras in restricted areas like movie theatres, museums, private hotels(like Oyo, Airbnb), dressing rooms in shopping malls.

SCOPE AND OBJECTIVES

- To detect camera - being operated in non-operational zone.
- To jam the camera detected- if not authorized.

EXISTING SYSTEM

The already existing system is When the device is powered by 9v dc supply, the RF antenna will receive the wireless transmission signal from mobile phone or from camera and the signal is given as an input to the microcontroller. Liquid Crystal Display is the material, which have the molecular structure and flows like a liquid. The pic microcontroller consists of In-System programmable flash memory of 8Kbytes, 1KB of SRAM and 512B EEPROM. GSM is used to send information to the required phone number. An antenna who's receiving elements such as arms of dipole is made in forms of a flexible system of metal tubes of approximately equal length. Changing the length of the antenna elements during tuning and let the size of antenna to be reduced and when is not in the operation.

PROPOSED SYSTEM

This paper detects RF signal which are emitted from the mobile phones and the hidden wireless camera during incoming and outgoing calls, messages and direct video transmission from one device to another with the alert system. This will

continuously monitors the RF level with in a room. If the RF signal level increases a warning message is send to the number via android which is registered in AT mega 8 microcontroller and the message is displayed through the LCD display as RF signal is detected. Trying to increase the detecting range by using the preamplifier stage using JFET or MOSFET transistor used in an interface between the capacitor and IC. Being able to detect the Bluetooth transfer to android application and give information to mobile numbers. and configured into IOT

CHAPTER 4

SYSTEM DESIGN & METHODOLOGY

SYSTEM

ARCHITECTURES

BLOCK DIAGRAM:

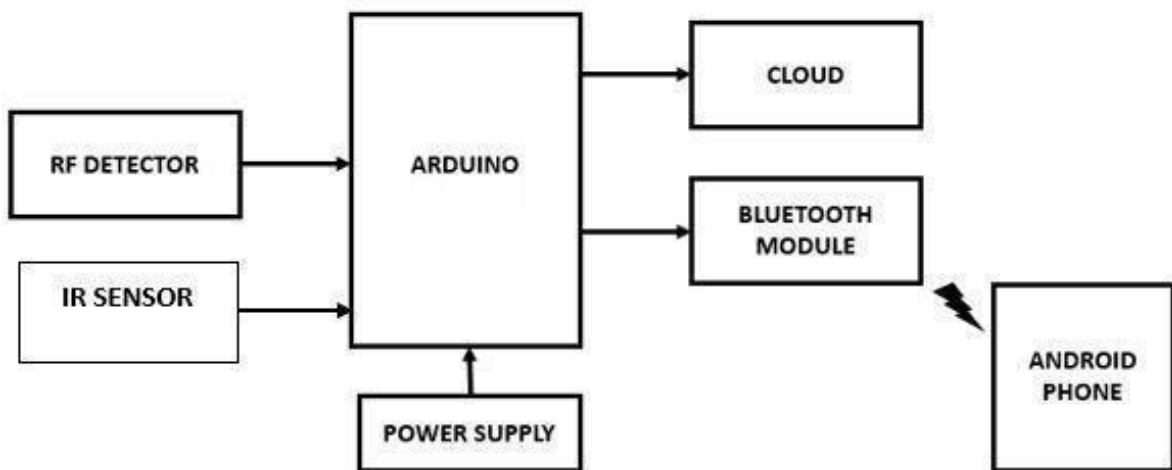


Fig 4.1: Architecture Diagram

SYSTEM REQUIREMENTS

HARDWARE USED

- Arduino
- RF detector
- IR sensor
- Bluetooth module
- Power supply

SOFTWARE USED:

- ARDUINO C
- ANDROID APPLICATION

METHODOLOGY

INTERNET OF THINGS

The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.

MODULES

ARDUINO

Arduino is a tool for making computers that can sense and control more of the physical world than your desktop computer. It's an open-source physical computing platform based on a simple microcontroller board, and a development environment for writing software for the board.

Arduino can be used to develop interactive objects, taking inputs from a variety of switches or sensors, and controlling a variety of lights, motors, and other physical outputs. Arduino projects can be stand-alone, or they can be communicate with software running on your computer. The boards can be assembled by hand or purchased preassembled; the open-source IDE can be downloaded for free.

The Arduino programming language is an implementation of Wiring, a similar physical computing platform, which is based on the Processing multimedia programming environment.

Overview

The Arduino microcontroller is an easy to use yet powerful single board computer that has gained considerable traction in the hobby and professional market. The Arduino is open-source, which means hardware is reasonably priced and development software is free. This guide is for students in ME 2011, or students anywhere who are confronting the Arduino for the first time. For advanced Arduino users, prowl the web; there are lots of resources.

This guide covers the Arduino Uno board (Spark fun DEV-09950, \$29.95), a good choice for students and educators. With the Arduino board, you can write programs

and create interface circuits to read switches and other sensors, and to control motors and lights with very little effort. Many of the pictures and drawings in this guide were taken from the documentation on the

This is what the Arduino board looks like.



Fig 4.2: Arduino Board

The Duemilanove board features an Atmel ATmega328 microcontroller operating at 5 V with 2 Kb of RAM, 32 Kb of flash memory for storing programs and 1 Kb of EEPROM for storing parameters. The clock speed is 16 MHz, which translates to about executing about 300,000 lines of C source code per second. The board has 14 digital I/O pins and 6 analog input pins. There is a USB connector for talking to the host computer and a DC power jack for connecting an external 6-20 V power source, for example a 9 V battery, when running a program while not connected to the host computer. Headers are provided for interfacing to the I/O pins using 22 g solid wire or header connectors.

The Arduino programming language is a simplified version of C/C++. If you know C, programming the Arduino will be familiar. If you do not know C, no need to worry as only a few commands are needed to perform useful functions.

An important feature of the Arduino is that you can create a control program on the host PC, download it to the Arduino and it will run automatically. Remove the USB cable connection to the PC, and the program will still run from the top each time you push the reset button. Remove the battery and put the Arduino board in a closet for six months. When you reconnect the battery, the last program you stored will run. This means that you connect the board to the host PC to develop and debug your program, but once that is done, you no longer need the PC to run the program.

The Arduino Uno is a microcontroller board based on the ATmega328. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

The Uno 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.

Summary:

Microcontroller ATmega328

Operating Voltage 5V

Input Voltage (recommended) 7-12V

Input Voltage (limits) 6-20V

Digital I/O Pins 14 (of which 6 provide PWM output)

Analog Input Pins 6

DC Current per I/O Pin 40 mA

DC Current for 3.3V Pin 50 mA

Flash Memory 32 KB (ATmega328) of which 0.5 KB used by bootloader

SRAM 2 KB (ATmega328)

EEPROM 1 KB (ATmega328)

Clock Speed 16

Pin Configuration

The Arduino Uno can be powered via the USB connection or with an external power supply. The power source is selected automatically.

External (non-USB) power can come either from an AC-to-DC adapter (wall-wart) or battery. The adapter can be connected by plugging a 2.1mm center-positive plug into the board's power jack. Leads from a battery can be inserted in the Gnd and Vin pin headers of the POWER connector.

The board can operate on an external supply of 6 to 20 volts. If supplied with less than 7V, however, the 5V pin may supply less than five volts and the board may be unstable. If using more than 12V, the voltage regulator may overheat and damage the board. The recommended range is 7 to 12 volts.

The power pins are as follows:

- **VIN**. The input voltage to the Arduino 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 - 12V), the USB connector (5V), or the VIN pin of the board (7-12V). Supplying voltage via the 5V or 3.3V pins bypasses the regulator, and can damage your board.
- **3V3**. A 3.3 volt supply generated by the on-board regulator. Maximum current draw is 50 mA.
- **GND**. Ground pins.
- **IOREF**. This pin on the Arduino board provides the voltage reference with which the microcontroller operates. A properly configured shield can read the IOREF pin voltage and select the appropriate power source or enable voltage translators on the outputs for working with the 5V or 3.3V.

Memory

The ATmega328 has 32 KB (with 0.5 KB used for the bootloader). It also has 2 KB of SRAM and 1 KB of EEPROM.

Input and Output

Each of the 14 digital pins on the Uno can be used as an input or output, using pinMode(), digital Write(), and digital Read() functions. They operate at 5 volts. Each pin can provide or receive a maximum of 40 mA and has an internal pull-up resistor (disconnected by default) of 20-50 kohms. In addition, some pins have specialized functions:

1. Serial: 0 (RX) and 1 (TX). Used to receive (RX) and Transmit (TX) TTL serial data

These pins are connected to the corresponding pins of the ATmega8U2 USB-to- TTL Serial chip.

2. External Interrupts: 2 and 3

These pins can be configured to trigger an interrupt on a low value, a rising or falling edge, or a change in value. See the attach Interrupt () function for details.

3.PWM: 3, 5, 6, 9, 10, and 11

Provide 8-bit PWM output with the analog Write () function.

4.SPI: 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK)

These pins support SPI communication using the SPI library.

5.LED: 13

There is a built- in LED connected to digital pin 13. When the pin is HIGH value, the LED is on, when the pin is LOW, it's off.

The Uno has 6 analog inputs, labeled A0 through A5, each of which provide 10 bits of resolution (i.e. 1024 different values). By default they measure from ground to 5 volts, though is it possible to change the upper end of their range using the AREF pin and the analog Reference () function. Additionally, some pins have specialized functionality:

- **TWI: A4 or SDA pin and A5 or SCL pin.** Support TWI communication using the Wire library. There are a couple of other pins on the board:
- **AREF.** Reference voltage for the analog inputs. Used with analog Reference ().
- **Reset.** Bring this line LOW to reset the microcontroller. Typically used to add a reset button to shields which block the one on the board.

Communication

Microcontrollers depend on a host computer for developing and compiling programs. The software used on the host computer is known as an integrated development environment, or IDE. For the Arduino, the development environment is based on the open source Processing platform (www.processing.org) which is described by its creators as a "programming language and environment for people who want to program images, animation, and interactions." The Arduino programming language

leverages an open source project known as Wiring (wiring.org.co). The Arduino language is based on good old- fashioned C. If you are unfamiliar with this language, don't worry; it's not hard to learn, and the Arduino IDE provides some feedback when you make mistakes in your programs.

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

A Software Serial library allows for serial communication on any of the Uno's digital pins. The ATmega328 also supports I2C (TWI) and SPI communication. The Arduino software includes a Wire library to simplify use of the I2C bus; see the documentation for details. For SPI communication, use the SPI library.

As you go through the list of programming statements available in the Arduino IDE (choose Help->Reference), you might think there isn't much power for doing things like running servos, operating stepper motors, reading potentiometers, or displaying text on an LCD. Like most any language based on C, the Arduino supports the notion of "libraries" code.

Repositories that extend core programming functionality. Libraries let you re- use code without having to physically copy and paste it into all your programs. The standard Arduino software installation comes with several libraries you may use, and you can download others from the Arduino support pages and from third-party websites that publish Arduino library code. A good example of a library you'll use with the Robot and likely many other robot projects is

Servo. This library allows you to connect one or more hobby R/C servos to the Arduino's digital I/O pins. The Servo library comes with the standard Arduino installation package Library->Servo. This adds the line

```
#include <Servo.h>
```

Which tells the Arduino IDE that you wish to include the Servo library in your sketch. With the functionality of the library now available to you, you can use its various functions to control one or more servos. For example, you can use the write function to rotate a servo to a specific position, from 0 to 180 degrees. The following code

```
myServo.write(90);
```

Moves a servo to its midpoint, or 90 degree position. Structurally, Arduino sketches are very straightforward and are pretty easy to read and understand. The Arduino program contains two main parts: setup () and loop (). These are programming functions that do what their names suggest: setup () sets up the Arduino hardware, such as specifying which I/O lines you plan to use, and whether

They are inputs or outputs. The loop () function is repeated endlessly when the Arduino is operating.

Arduino IDE (Integrated development environment) is used to write the program and dump into the Arduino board

IR (Infrared) Sensor

An infrared sensor is an electronic device that emits in order to sense some aspects of the surroundings. An IR sensor can measure the heat of an object as well as detects the motion. These types of sensors measures only infrared radiation, rather than emitting it that is called as a passive IR sensor. Usually in the infrared spectrum, all the objects radiate some form of thermal radiations. These types of radiations are invisible to our eyes that can be detected by an infrared sensor. The emitter is simply an IR LED (Light Emitting Diode) and the detector is simply an IR photodiode which is sensitive to IR light of the same wavelength as that emitted by the IR LED. When IR

light falls on the photodiode, the resistances and these output voltages, change in proportion to the magnitude of the IR light received.

IR Sensor Circuit Diagram and Working Principle

An infrared sensor circuit is one of the basic and popular sensor module in an electronic device. This sensor is analogous to human's visionary senses, which can be used to detect obstacles and it is one of the common applications in real time. This circuit comprises of the following components

- LM358 IC 2 IR transmitter and receiver pair
- Resistors of the range of kilo ohms.
- Variable resistors.
- LED (Light Emitting Diode).

In this project, the transmitter section includes an IR sensor, which transmits continuous IR rays to be received by an IR receiver module. An IR output terminal of the receiver varies depending upon its receiving of IR rays. Since this variation cannot be analyzed as such, therefore this output can be fed to a comparator circuit. Here an operational amplifier (op-amp) of LM 339 is used as comparator circuit. When the IR receiver does not receive a signal, the potential at the inverting input goes higher than that non-inverting input of the comparator IC (LM339). Thus the output of the comparator goes low, but the LED does not glow. When the IR receiver module receives signal to the potential at the inverting input goes low. Thus the output of the comparator (LM 339) goes high and the LED starts glowing.

IR Sensor circuit:

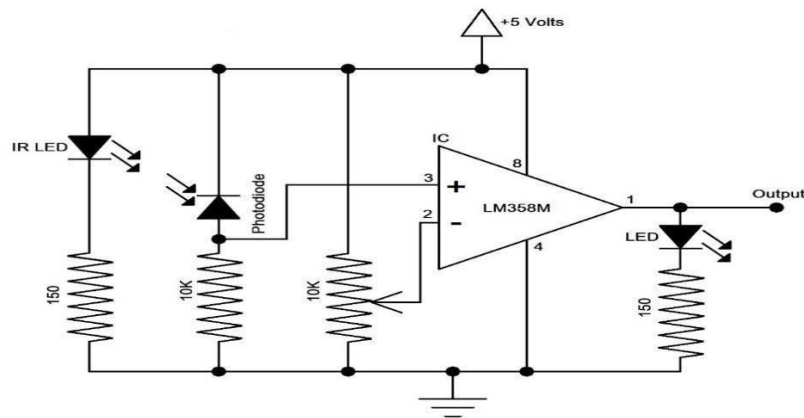


Fig 4.3: IR Sensor Circuit diagram

Resistor R1 (100 Ω), R2 (10k Ω) and R3 (330 Ω) are used to ensure that minimum 10 mA current passes through the IR LED Devices like Photodiode and normal LEDs respectively. Resistor VR2 (preset=5k) is used to adjust the output terminals. Resistor VR1 (preset=10k) is used to set the sensitivity of the circuit Diagram. Read more about IR sensors.

Different Types of IR Sensors and Their Applications

IR sensors are classified into different types depending on the applications. The speed sensor is used for synchronizing the speed of multiple motors. The temperature sensor is used for industrial temperature control. PIR sensor is used for automatic door opening system and Ultrasonic sensor are used for distance measurement.

IR Sensor Applications

IR sensors are used in various Sensor based projects and also in various electronic devices which measures the temperature that are discussed in the below.

Radiation Thermometers

IR sensors are used in radiation thermometers to measure the temperature depend upon the temperature and the material of the object and these thermometers have some of the following features

- Measurement without direct contact with the object

- Faster response
- Easy pattern measurements

Flame Monitors

These types of devices are used for detecting the light emitted from the flames and to monitor how the flames are burning. The Light emitted from flames extend from UV to IR region types. PbS, PbSe, Two-color detector, pyro electric detector are some of the commonly employed detector used in flame monitors.

Moisture Analyzers

Moisture analyzers use wavelengths which are absorbed by the moisture in the IR region. Objects are irradiated with light having these wavelengths (1.1 μm , 1.4 μm , 1.9 μm , and 2.7 μm) and also with reference wavelengths. The Lights reflected from the objects depend upon the moisture content and is detected by analyzer to measure moisture (ratio of reflected light at these wavelengths to the reflected light at reference wavelength). In GaAs PIN photodiodes, Pbs photoconductive detectors are employed in moisture analyzer circuits.

IR Imaging Devices

IR image device is one of the major applications of IR waves, primarily by virtue of its property that is not visible. It is used for thermal imagers, night vision devices, etc.



Fig 4.4: IR imaging

For examples Water, rocks, soil, vegetation, an atmosphere, and human tissue all features emit IR radiation. The Thermal infrared detectors measure these radiations in IR range and map the spatial temperature distributions of the object/area on an image. Thermal imagers usually composed of a Sb (indium antimonite), Gd Hg (mercury-doped germanium), Hg Cd Te (mercury-cadmium-telluride) sensors.

An electronic detector is cooled to low temperatures using liquid helium or liquid nitrogen's. Then the Cooling the detectors ensures that the radiant energy (photons) recorded by the detectors comes from the terrain and not from the ambient temperature of objects within the scanner itself an IR imaging electronic devices.

Thus, this is all about IR sensor circuit with working and applications. These sensors are used in many sensor based electronics projects.

BLUETOOTH MODULE

- HC-05 module is an easy to use Bluetooth SPP (Serial Port Protocol) module, designed for transparent wireless serial connection setup.
- Serial port Bluetooth module is fully qualified Bluetooth V2.0+EDR (Enhanced Data Rate) 3Mbps Modulation with complete 2.4GHz radio transceiver and baseband.
- It uses CSR Bluecore 04-External single chip Bluetooth system with CMOS technology and with AFH(Adaptive Frequency Hopping Feature).

Feature

- Typical -80dBm sensitivity
- Up to +4dBm RF transmit power
- Low Power 1.8V Operation ,1.8 to 3.6V I/O
- PIO control
- UART interface with programmable baud rate
- With integrated antenna
- With edge connector

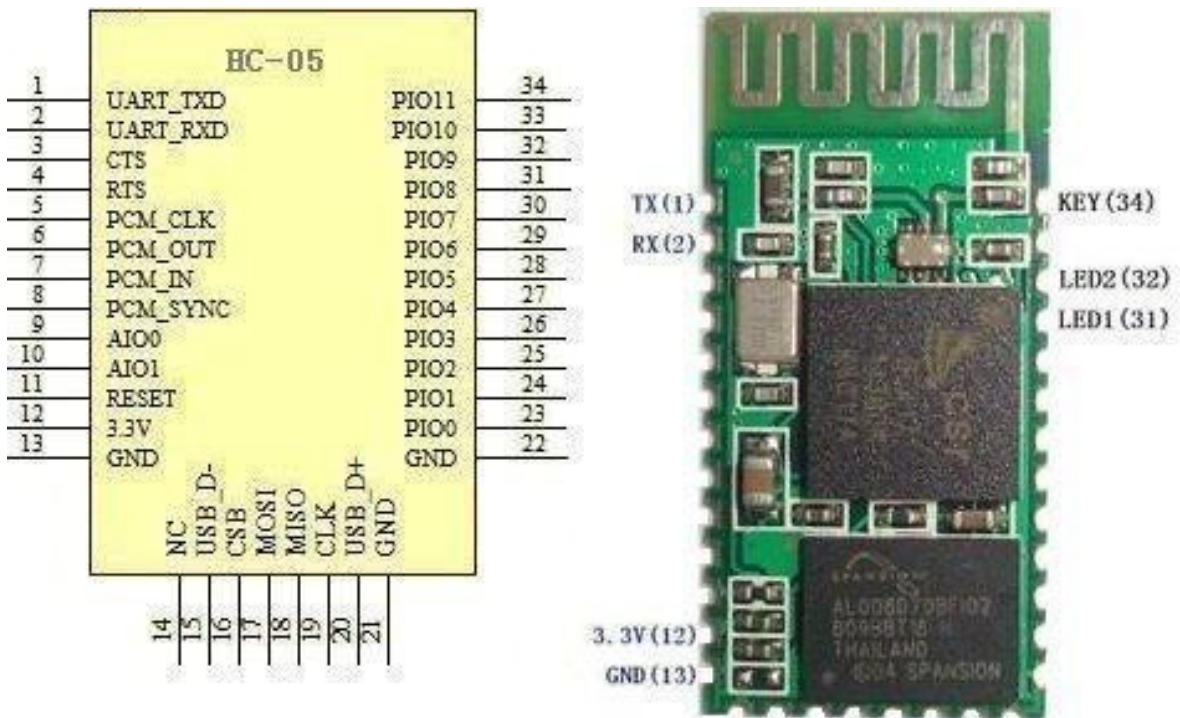


Fig 4.5: Bluetooth Module

RF DETECTOR:

Here is a circuit that can detect the presence of a radio frequency (RF) signal. If it is close to RF-emitting devices such as a television set or a computer, it shows a high reading in the UV meter, giving us an idea about the intensity of RF radiation in the room. High-intensity RF radiation from mobile phone towers in the vicinity is considered to be harmful by most.

The circuit diagram of the RF detector is shown in Fig. 4.4. It is built around AM/FM detector diodes 1N34 (D1 and D2), an operational amplifier CA3130 (IC1), npn transistor BC547 (T1), connector CON1 for VU meter and a few other components. Detector diodes D1 and D2 capture the RF from surroundings for the inverting input of IC1. The IC is configured as an inverting amplifier with non-inverting input tied to the negative rail. Feedback resistor R1 controls the gain of the inverting amplifier. IC CA3130 is a high-gain operational amplifier with sensitive inputs. It is a 15MHz BiMOS operational amplifier with MOSFET inputs and bipolar output. Its high-speed performance is suitable for low input-current applications. RF signals are amplified by the inverting amplifier built around IC1. The amplified signal is used to drive the sensitive VU meter. Potmeter VR1 is used to set zero level in the meter. When the circuit gets RF energy from a device or the surroundings,

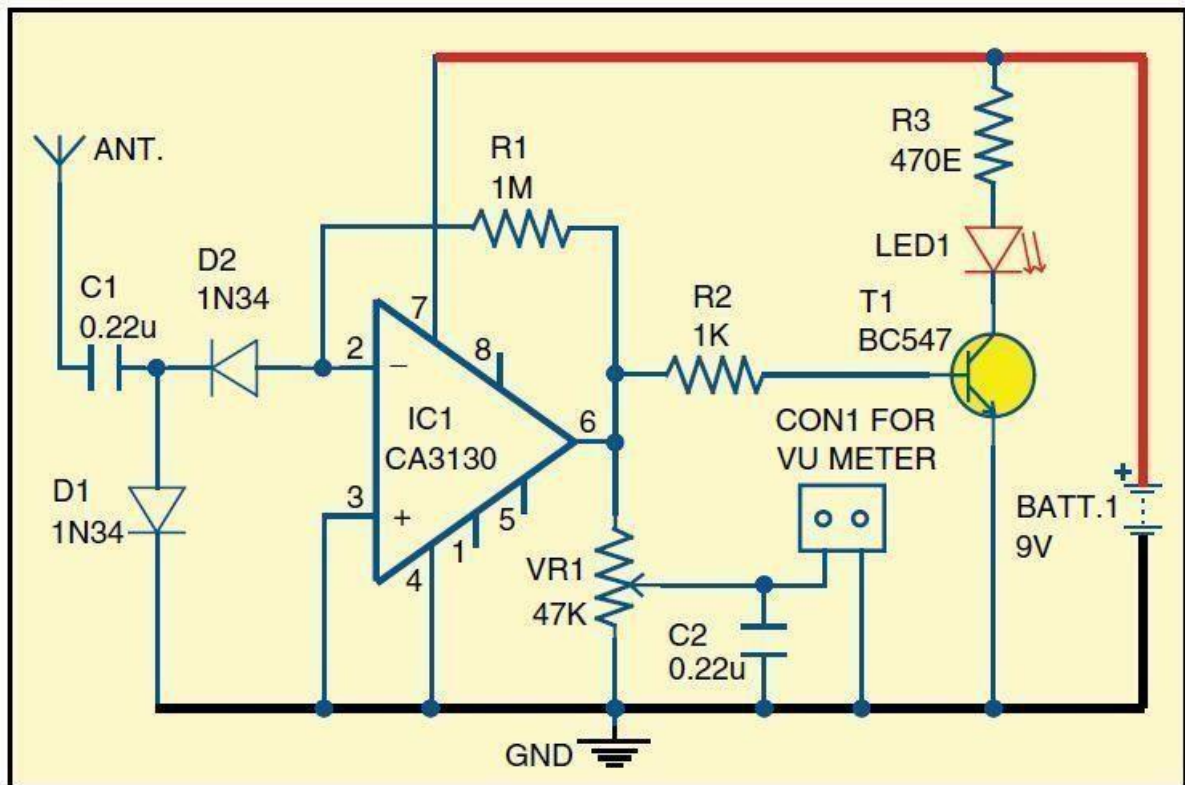


Fig 4.6:

Construction and testing

An actual-size, single-side PCB for the RF detector is shown in Fig. 2 and its component layout in Fig. 3. Enclose the PCB in a suitable small box in such a way that potmeter VR1

and VU meter can be fixed on the front side. Ensure proper wiring to avoid any mistake. Do not solder CA3130 directly on the PCB; instead, use an 8-pin IC base for the IC. A telescopic antenna is used to increase the sensitivity of the circuit. Use 9V PP3 battery as the power source. shows the author'.

Power supply

A power supply is an electronic device that supplies electric energy to an electrical load. The primary function of a power supply is to convert one form of electrical energy to another. As a result, power supplies are sometimes referred to as electric power converters. Some power supplies are discrete, stand-alone devices, whereas others are built into larger devices along with their loads. Examples of the latter include power supplies found in desktop computers and consumer electronics devices.

Every power supply must obtain the energy it supplies to its load, as well as any energy it consumes while performing that task, from an energy source. Depending on its design, a power supply may obtain energy from various types of energy sources, including electrical energy transmission systems, energy storage devices such as a batteries and fuel cells, electro-mechanical systems such as generators and alternators, solar power converters, or another power supply.

All power supplies have a power input, which receives energy from the energy source, and a power output that delivers energy to the load. In most power supplies the power input and output consist of electrical connectors or hardwired circuit connections, though some power supplies employ wireless energy transfer in lieu of galvanic connections for the power input or output. Some power supplies have other types of inputs and outputs as well, for functions such as external monitoring and control.

A power supply (sometimes known as a power supply unit or PSU) is a device or system that supplies electrical or other types of energy to an output load or group of loads. The term is most commonly applied to electrical energy supplies, less often to mechanical ones, and rarely to others.

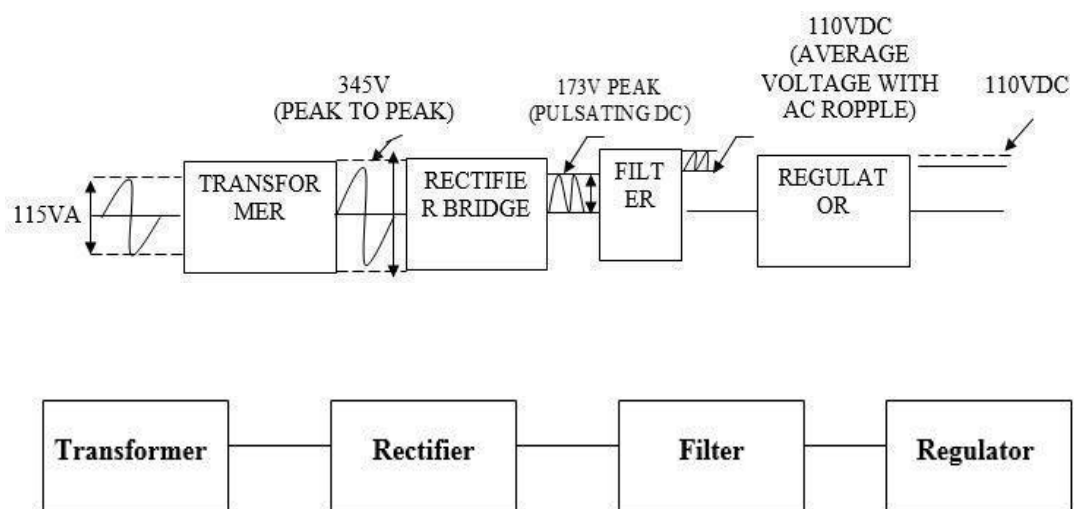


Fig 4.7:Steps Involved in Power Supply

The transformer steps up or steps down the input line voltage and isolates the power supply from the power line. The RECTIFIER section converts the alternating current input signal to a pulsating direct current. However, as you proceed in this chapter you will learn that pulsating dc is not desirable. For this reason a FILTER section is used to

convert pulsating dc to a purer, more desirable form of dc voltage.

The final section, the REGULATOR, does just what the name implies. It maintains the output of the power supply at a constant level in spite of large changes in load current or input line voltages. Now that you know what each section does, let's trace an ac signal through the power supply. At this point you need to see how this signal is altered within each section of the power supply. Later on in the chapter you will see how these changes take place. An input signal of 115 volts ac is applied to the primary of the transformer.

The transformer is a step-up transformer with a turn's ratio of 1:3. You can calculate the output for this transformer by multiplying the input voltage by the ratio of turns in the primary to the ratio of turns in the secondary; therefore, $115 \text{ volts ac} \times 3 = 345 \text{ volts ac}$ (peak-to-peak) at the output. Because each diode in the rectifier section conducts for 180 degrees of the 360-degree input, the output of the rectifier will be one-half, or approximately 173 volts of pulsating dc. The filter section, a network of resistors, capacitors, or inductors, controls the rise and fall time of the varying signal; consequently, the signal remains at a more constant dc level. You will see the filter process more clearly in the discussion of the actual filter circuits. The output of the filter is a signal of 110 volts dc, with ac ripple riding on the dc. The reason for the lower voltage (average voltage) will be explained later in this chapter. The regulator maintains its output at a constant 110-volt dc level, which is used by the electronic equipment (more commonly called the load).

POWER SUPPLY UNIT

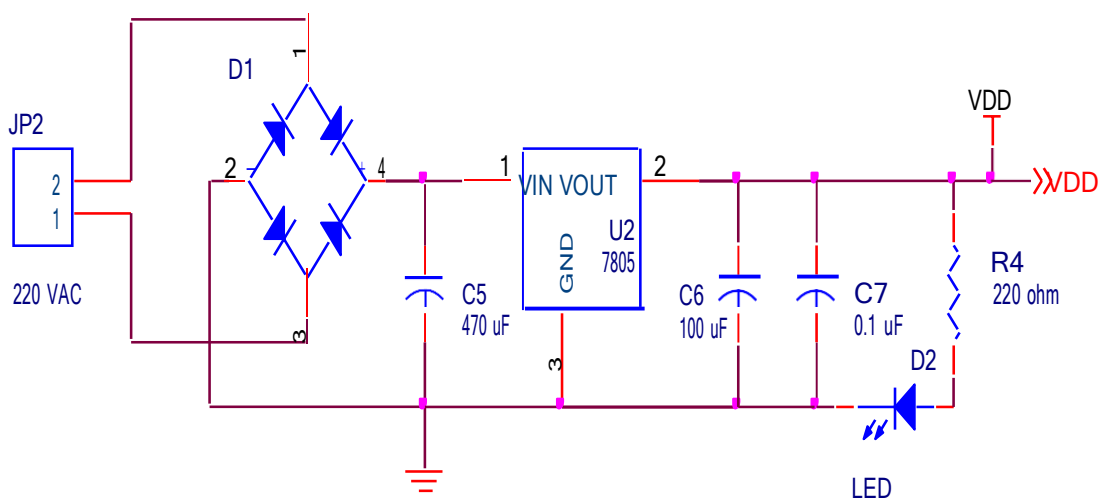


Fig 4.8:Power Supply Unit Circuit Diagram

CIRCUIT DIAGRAM OF POWER SUPPLY

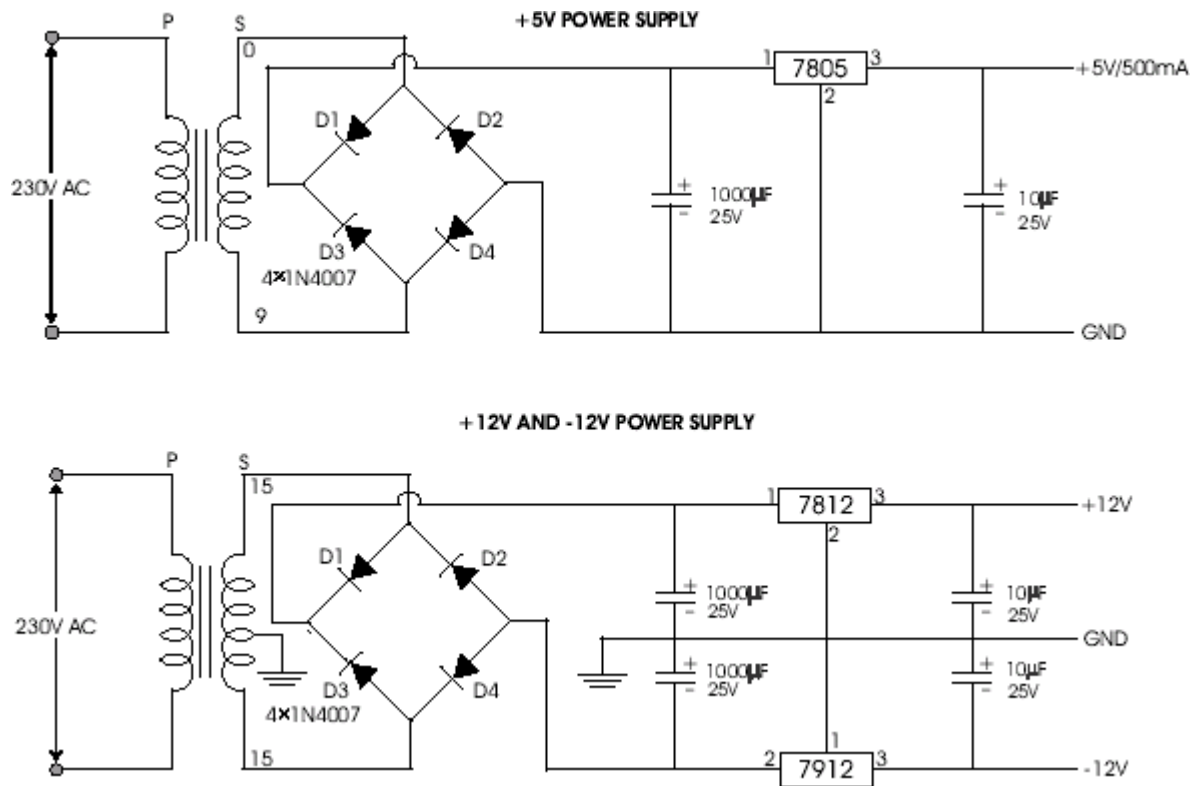


Fig 4.9: Circuit diagram

WORKING PRINCIPLE:

The AC voltage, typically 220V rms, is connected to a transformer, which steps that ac voltage down to the level of the desired DC output. A diode rectifier then provides a full-wave rectified voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting dc voltage usually has some ripple or ac voltage variation. A regulator circuit removes the ripples and also remains the same dc value even if the input dc voltage varies, or the load connected to the output dc voltage changes.

TRANSFORMER:

The potential transformer will step down the power supply voltage (0-230V) to (0-6V) level. Then the secondary of the potential transformer will be connected to the precision rectifier, which is constructed with the help of op-amp. The advantages of using precision rectifier are it will give peak voltage output as DC, rest of the circuits will give only RMS output.

BRIDGE RECTIFIER:

When four diodes are connected as shown in figure, the circuit is called as bridge rectifier. The input to the circuit is applied to the diagonally opposite corners of the network, and the output is taken from the remaining two corners.

Let us assume that the transformer is working properly and there is a positive potential, at point A and a negative potential at point B. the positive potential at point A will forward bias D3 and reverse bias D4.

The negative potential at point B will forward bias D1 and reverse D2. At this time D3 and D1 are forward biased and will allow current flow to pass through them; D4 and D2 are reverse biased and will block current flow.

The path for current flow is from point B through D1, up through RL, through D3, through the secondary of the transformer back to point B. this path is indicated by the solid arrows. Waveforms (1) and (2) can be observed across D1 and D3.

One-half cycle later the polarity across the secondary of the transformer reverse, forward biasing D2 and D4 and reverse biasing D1 and D3. Current flow will now be from point A through D4, up through RL, through D2, through the secondary of T1, and back to point A. This path is indicated by the broken arrows. Waveforms (3) and (4) can be observed across D2 and D4. The current flow through RL is always in the same direction.

In flowing through RL this current develops a voltage corresponding to that shown waveform (5). Since current flows through the load (RL) during both half cycles of the applied voltage, this bridge rectifier is a full-wave rectifier.

One advantage of a bridge rectifier over a conventional full-wave rectifier is that with a given transformer the bridge rectifier produces a voltage output that is nearly twice that of the conventional full-wave circuit.

This may be shown by assigning values to some of the components shown in views A and B. assume that the same transformer is used in both circuits. The peak voltage developed between points X and y is 1000 volts in both circuits. In the conventional full-wave circuit shown—in view A, the peak voltage from the center tap to either X or Y is 500 volts.

Since only one diode can conduct at any instant, the maximum voltage that can be rectified at any instant is 500 volts.

The maximum voltage that appears across the load resistor is nearly-but never exceeds-500 v0lts, as result of the small voltage drop across the diode. In the bridge rectifier shown in view B, the maximum voltage that can be rectified is the full secondary voltage, which is 1000 volts. Therefore, the peak output voltage across the load resistor is nearly 1000 volts. With both circuits using the same transformer, the bridge rectifier circuit produces a higher output voltage than the conventional full-wave rectifier circuit.

IC VOLTAGE REGULATORS:

Voltage regulators comprise a class of widely used ICs. Regulator IC units contain the circuitry for reference source, comparator amplifier, control device, and overload protection all in a single IC. IC units provide regulation of either a fixed positive voltage, a fixed negative voltage, or an adjustable set voltage. The regulators can be selected for operation with load currents from hundreds of milli amperes to tens of amperes, corresponding to power ratings from milli watts to tens of watts.

A fixed three-terminal voltage regulator has an unregulated dc input voltage, V_i , applied to one input terminal, a regulated dc output voltage, V_o , from a second terminal, with the third terminal connected to ground. The series 78 regulators provide fixed positive regulated voltages from 5 to 24 volts. Similarly, the series 79 regulators provide fixed negative regulated voltages from 5 to 24 volts.

Simple 5V power supply for digital circuits

- Brief description of operation: Gives out well regulated +5V output, output current capability of 100 mA
- Circuit protection: Built-in overheating protection shuts down output when regulator IC gets too hot
- Circuit complexity: Very simple and easy to build
- Circuit performance: Very stable +5V output voltage, reliable operation
- Availability of components: Easy to get, uses only very common basic components
- Design testing: Based on datasheet example circuit, I have used this circuit successfully as part of many electronics projects
- Applications: Part of electronics devices, small laboratory power supply

- Power supply voltage: Unregulated DC 8-18V power supply
- Power supply current: Needed output current + 5 mA
- Component costs: Few dollars for the electronics components + the input transformer cost

General classification

1. Functional:

Power supplies are categorized in various ways, including by functional features. For example, a regulated power supply is one that maintains constant output voltage or current despite variations in load current or input voltage. Conversely, the output of an unregulated power supply can change significantly when its input voltage or load current changes. Adjustable power supplies allow the output voltage or current to be programmed by mechanical controls (e.g., knobs on the power supply front panel), or by means of a control input, or both. An adjustable regulated power supply is one that is both adjustable and regulated. An isolated power supply has a power output that is electrically independent of its power input; this is in contrast to other power supplies that share a common connection between power input and output.

2. Mechanical:

Power supplies are packaged in different ways and classified accordingly. A bench power supply is a stand-alone desktop unit used in applications such as circuit test and development. Open frame power supplies have only a partial mechanical enclosure, sometimes consisting of only a mounting base; these are typically built into machinery or other equipment. Rack mount power supplies are designed to be secured into standard electronic equipment racks. An integrated power supply is one that shares a common printed circuit board with its load.

Power conversion method

Power supplies can be broadly divided into linear and switching types. Linear power converters process the input power directly, with all active power conversion components operating in their linear operating regions. In switching power converters, the input power is converted to AC or to DC pulses before processing, by components that operate predominantly in non-linear modes (e.g., transistors that spend most of their time in cutoff or saturation). Power is "lost" (converted to heat) when components

operate in their linear regions and, consequently, switching converters are usually more efficient than linear converters because their components spend less time in linear operating regions.

Types

1. DC power supply

A DC power supply is one that supplies a constant DC voltage to its load. Depending on its design, a DC power supply may be powered from a DC source or from an AC source such as the power mains.

2. AC-to-DC supply

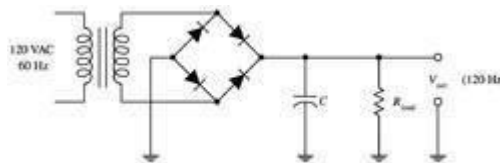


Fig 4.10:

Schematic of basic AC-to-DC power supply, showing (from L-R) transformer, full-wave bridge rectifier, filter capacitor and resistor load.

Some DC power supplies use AC mains electricity as an energy source. Such power supplies will sometimes employ a transformer to convert the input voltage to a higher or lower AC voltage. A rectifier is used to convert the transformer output voltage to a varying DC voltage, which in turn is passed through an electronic filter to convert it to an unregulated DC voltage.

The filter removes most, but not all of the AC voltage variations; the remaining AC voltage is known as ripple. The electric load's tolerance of ripple dictates the minimum amount of filtering that must be provided by a power supply. In some applications, high ripple is tolerated and therefore no filtering is required. For example, in some battery charging applications it is possible to implement a mains-powered DC power supply with nothing more than a transformer and a single rectifier diode, with a resistor in series with the output to limit charging current.

Linear regulator

The function of a linear voltage regulator is to convert a varying DC voltage to a constant, often specific, lower DC voltage. In addition, they often provide a current limiting function to protect the power supply and load from overcurrent (excessive,

potentially destructive current).

A constant output voltage is required in many power supply applications, but the voltage provided by many energy sources will vary with changes in load impedance. Furthermore, when an unregulated DC power supply is the energy source, its output voltage will also vary with changing input voltage. To circumvent this, some power supplies use a linear voltage regulator to maintain the output voltage at a steady value, independent of fluctuations in input voltage and load impedance. Linear regulators can also reduce the magnitude of ripple and noise on the output voltage.

AC power supplies

An AC power supply typically takes the voltage from a wall outlet (mains supply) and lowers it to the desired voltage. Some filtering may take place as well.

In modern use, AC power supplies can be divided into single phase and three phase systems. "The primary difference between single phase and three phase AC power is the constancy of delivery." ^[1] AC power Supplies can also be used to change the frequency as well as the voltage, they are often used by manufacturers to check the suitability of their products for use in other countries. 230V 50 Hz or 115 60 Hz or even 400 Hz for avionics testing.

Switched-mode power supply

In a switched-mode power supply (SMPS), the AC mains input is directly rectified and then filtered to obtain a DC voltage. The resulting DC voltage is then switched on and off at a high frequency by electronic switching circuitry, thus producing an AC current that will pass through a high-frequency transformer or inductor. Switching occurs at a very high frequency (typically 10 kHz – 1 MHz), thereby enabling the use of transformers and filter capacitors that are much smaller, lighter, and less expensive than those found in linear power supplies operating at mains frequency. After the inductor or transformer secondary, the high frequency AC is rectified and filtered to produce the DC output voltage. If the SMPS uses an adequately insulated high-frequency transformer, the output will be electrically isolated from the mains; this feature is often essential for safety. Switched-mode power supplies are usually regulated, and to keep the output voltage constant, the power supply employs a feedback controller that monitors current drawn by the load. The switching duty cycle increases as power output requirements increase.

SMPSSs often include safety features such as current limiting or a crowbar circuit to help protect the device and the user from harm. In the event that an abnormal high-current power draw is detected, the switched-mode supply can assume this is a direct short and will shut itself down before damage is done. PC power supplies often provide a good signal to the motherboard; the absence of this signal prevents operation when abnormal supply voltages are present.

Some SMPSSs have an absolute limit on their minimum current output. They are only able to output above a certain power level and cannot function below that point. In a no-load condition the frequency of the power slicing circuit increases to great speed, causing the isolated transformer to act as a Tesla coil, causing damage due to the resulting very high voltage power spikes. Switched-mode supplies with protection circuits may briefly turn on but then shut down when no load has been detected. A very small low-power load such as a ceramic power resistor or 10-watt light bulb can be attached to the supply to allow it to run with no primary load attached.

The switch-mode power supplies used in computers have historically had low power factors and have also been significant sources of line interference (due to induced power line harmonics and transients). In simple switch-mode power supplies, the input stage may distort the line voltage waveform, which can adversely affect other loads (and result in poor power quality for other utility customers), and cause unnecessary heating in wires and distribution equipment. Furthermore, customers incur higher electric bills when operating lower power factor loads. To circumvent these problems, some computer switch-mode power supplies perform power factor correction, and may employ input filters or additional switching stages to reduce line interference.

Programmable power supply



Fig 4.11: Power supply

Programmable power supplies

A programmable power supply is one that allows remote control of its operation through an analog input or digital interface such as RS232 or GPIB. Controlled properties may include voltage, current, and in the case of AC output power supplies, frequency. They are used in a wide variety of applications, including automated equipment testing, crystal growth monitoring, semiconductor fabrication, and x-ray generators.

Programmable power supplies typically employ an integral microcomputer to control and monitor power supply operation. Power supplies equipped with a computer interface may use proprietary communication protocols or standard protocols and device control languages such as SCPI.

Uninterruptible power supply

An uninterruptible power supply (UPS) takes its power from two or more sources simultaneously. It is usually powered directly from the AC mains, while simultaneously charging a storage battery. Should there be a dropout or failure of the mains, the battery instantly takes over so that the load never experiences an interruption. In a computer installation, this gives the operators time to shut down the system in an orderly way. Other UPS schemes may use an internal combustion engine or turbine to continuously supply power to a system in parallel with power coming from the AC. The engine-driven generators would normally be idling, but could come to full power in a matter of a few seconds in order to keep vital equipment running without interruption. Such a scheme might be found in hospitals or telephone central offices.

High-voltage power supply



Fig 4.12:

A 30 kV high-voltage power supply with Federal Standard connector, used in electron microscopes.

A high-voltage power supply is one that outputs hundreds or thousands of volts. A special output connector is used that prevents arcing, insulation breakdown and accidental human contact. Federal Standard connectors are typically used for applications above 20 kV, though other types of connectors (e.g., SHV connector) may be used at lower voltages. Some high-voltage power supplies provide an analog input or digital communication interface that can be used to control the output voltage. High-voltage power supplies are commonly used to accelerate and manipulate electron and ion beams in equipment such as x-ray generators, electron microscopes, and beam columns, and in a variety of other applications, including electrophoresis and electrostatics.

High-voltage power supplies typically apply the bulk of their input energy to a power inverter, which in turn drives a voltage multiplier or a high turns ratio, high-voltage transformer, or both (usually a transformer followed by a multiplier) to produce high voltage. The high voltage is passed out of the power supply through the special connector and is also applied to a voltage divider that converts it to a low-voltage metering signal compatible with low-voltage circuitry. The metering signal is used by a closed-loop controller that regulates the high voltage by controlling inverter input power, and it may also be conveyed out of the power supply to allow external circuitry to monitor the high-voltage output.

Specification

The suitability of a particular power supply for an application is determined by various attributes of the power supply, which are typically listed in the power supply's specification. Commonly specified attributes for a power supply include:

- Input voltage type (AC or DC) and range
- Efficiency of power conversion
- The amount of voltage and current it can supply to its load
- How stable its output voltage or current is under varying line and load conditions
- How long it can supply energy without refueling or recharging (applies to power supplies that employ portable energy sources)
- Operating and storage temperature ranges

Power supply applications

Power supplies are a fundamental component of many electronic devices and therefore used in a diverse range of applications. This list is a small sample of the many applications of power supplies.

Computer power supply

A modern computer power supply is a switch-mode power supply that converts AC power from the mains supply, to several DC voltages. Switch-mode supplies replaced linear supplies due to cost, weight, and size improvement. The diverse collection of output voltages also have widely varying current draw requirements.

Electric Vehicle power supply

Electric vehicles are those which rely on energy created through electricity generation. A power supply unit is part of the necessary design to convert high voltage vehicle battery power.

Welding power supply

Arc welding uses electricity to melt the surfaces of the metals in order to join them together through coalescence. The electricity is provided by a welding power supply, and can either be AC or DC. Arc welding typically requires high currents typically between 100 and 350 amperes. Some types of welding can use as few as 10 amperes, while some applications of spot welding employ currents as high as 60,000 amperes for an extremely short time. Older welding power supplies consisted of transformers or engines driving generators. More recent supplies use semiconductors and microprocessors reducing their size and weight.

Aircraft power supply

Both commercial and military avionic systems require either a DC-DC or AC/DC power supply to convert energy into usable voltage.

AC adapter



Fig 4.13: Switch-mode mobile phone charger

An AC adapter is a power supply built into an AC mains power plug. AC adapters are also known by various other names such as "plug pack" or "plug-in adapter", or by slang terms such as "wall wart". AC adapters typically have a single AC or DC output that is conveyed over a hardwired cable to a connector, but some adapters have multiple outputs that may be conveyed over one or more cables. "Universal" AC adapters have interchangeable input connectors to accommodate different AC mains voltages.

Adapters with AC outputs may consist only of a passive transformer (plus a few diodes in DC-output adapters), or they may employ switch-mode circuitry. AC adapters consume power (and produce electric and magnetic fields) even when not connected to a load; for this reason they are sometimes known as "electricity vampires", and may be plugged into power strips to allow them to be conveniently turned on and off.

Overload protection

Power supplies often have protection from short circuit or overload that could damage the supply or cause a fire. Fuses and circuit breakers are two commonly used mechanisms for overload protection.^[5]

A fuse contains a short piece of wire which melts if too much current flows. This effectively disconnects the power supply from its load, and the equipment stops working until the problem that caused the overload is identified and the fuse is replaced. Some power supplies use a very thin wire link soldered in place as a fuse. Fuses in power supply units may be replaceable by the end user, but fuses in consumer equipment may require tools to access and change.

A circuit breaker contains an element that heats, bends and triggers a spring which

shuts the circuit down. Once the element cools, and the problem is identified the breaker can be reset and the power restored.

Some PSUs use a thermal cut-out buried in the transformer rather than a fuse. The advantage is it allows greater current to be drawn for limited time than the unit can supply continuously. Some such cut-outs are self-resetting, some are single use only.

Current limiting

Some supplies use current limiting instead of cutting off power if overloaded. The two types of current limiting used are electronic limiting and impedance limiting. The former is common on lab bench PSUs, the latter is common on supplies of less than 3 watts output.

A fold back current limiter reduces the output current to much less than the maximum non-fault current.

Terminology

- SCP - Short circuit protection
- OPP - Overpower (overload) protection
- OCP - Overcurrent protection
- OTP - Over temperature protection
- OVP - Overvoltage protection
- UVP - Under voltage protection
- UPS - Uninterruptable Power Supply
- PSU - Power Supply Unit
- SMPSU - Switch-Mode Power Supply Unit

SOFTWARE SETUP DETAILS:

Arduino IDE

Get the latest version from the download page. You can choose between the Installer (.exe) and the Zip packages. We suggest you use the first one that installs directly everything you need to use the Arduino Software (IDE), including the drivers. With the Zip package you need to install the drivers manually. The Zip file is also useful if you want to create a portable installation.

When the download finishes, proceed with the installation and please allow the driver installation process when you get a warning from the operating system.

Arduino is a tool for making computers that can sense and control more of the physical world than your desktop computer. It's an open-source physical computing platform based on a simple microcontroller board, and a development environment for writing software for the board.

Arduino can be used to develop interactive objects, taking inputs from a variety of switches or sensors, and controlling a variety of lights, motors, and other physical outputs. Arduino projects can be stand-alone, or they can be communicate with software running on your computer (e.g. Flash, Processing, MaxMSP.) The boards can be assembled by hand or purchased preassembled; the open-source IDE can be downloaded for free.

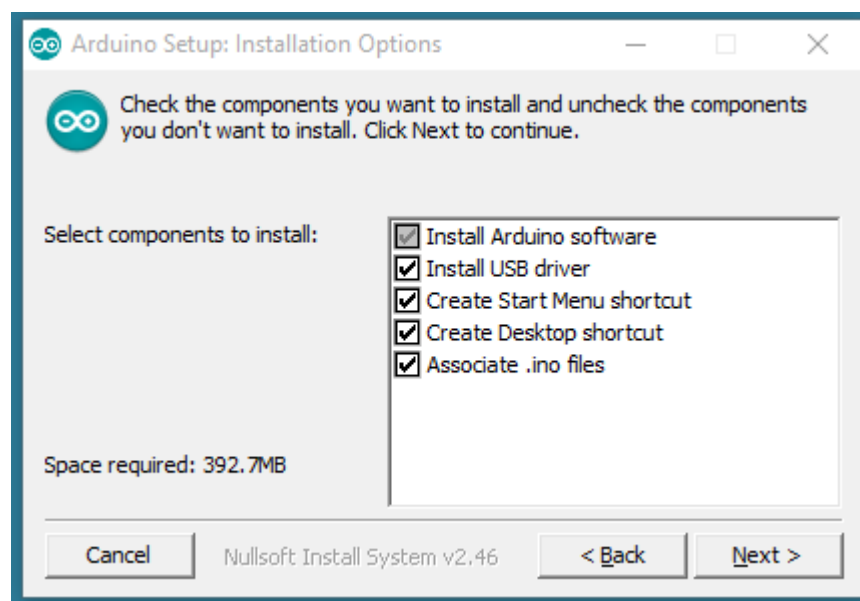


Fig 4.14: Choose the components to install

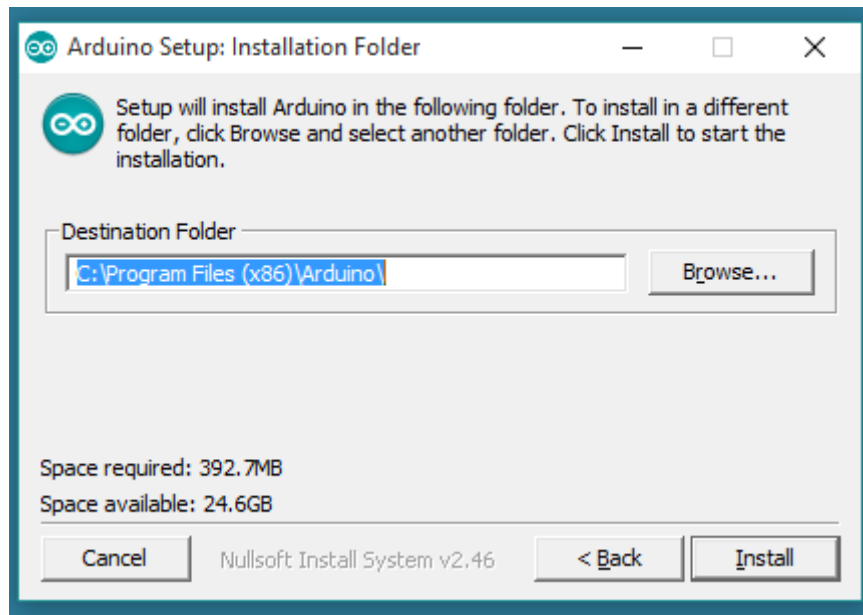


Fig 4.15: Choose the installation directory (we suggest to keep the default one)

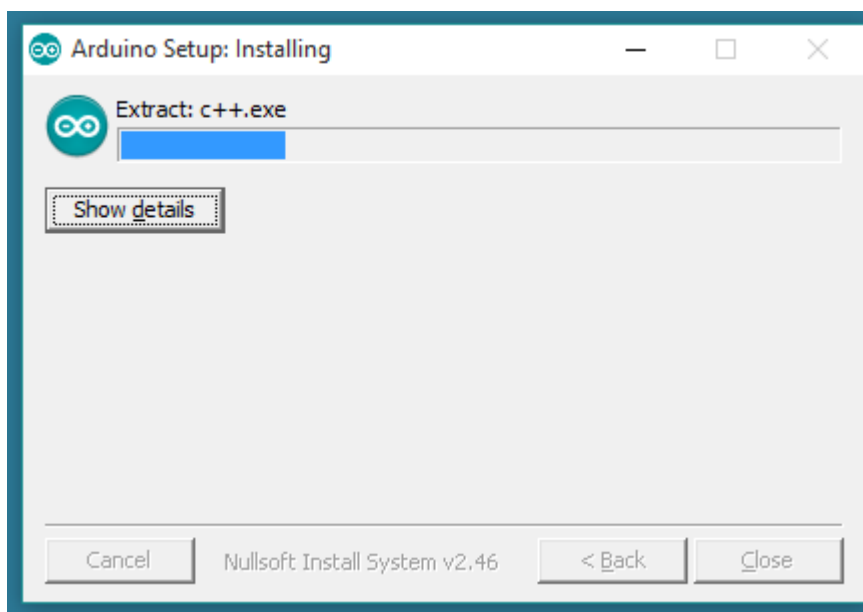


Fig4.16: Extraction of files

The process will extract and install all the required files to execute properly the Arduino Software (IDE)

Proceed with board specific instructions

When the Arduino Software (IDE) is properly installed you can go back to the Getting Started Home and choose your board from the list on the right of the page

Android Application:

Installation of the required softwares for android

Followings are the softwares and plugins need to be installed step by step before working on

1. Java JDK

It is required to be able to write and compile Java applications. Follow these steps to install it.

- Go to www.oracle.com/technetwork/java/javase/downloads/index.html
- Download the latest version of Java JDK

2. Eclipse IDE

It is the Integrated Development Environment (a software used to edit, compile and run the apps) which we will use to write Android applications. Here are the steps:

- Go to www.eclipse.org/downloads/
- Download the latest version on Eclipse Classic

3. Android SDK

It is the software package which contains Android libraries, emulators and all the related stuff that one needs to make Android applications:

Go to <http://developer.android.com/sdk/index.html>

Download the latest version of Windows Installer (.exe file)

Set your browser at no proxy (since the Android SDK does not have the option for

proxy authentication)

Run the above downloaded .exe file and let it download the required components

4. ADT Plugin

It is required to link Android SDK with Eclipse IDE. Go to <http://developer.android.com/sdk/eclipse-adt.html> and follow the instructions to install ADT plugin.

* Common queries :-

1. While installing Java JDK , go for Java platform (JDK) 7u4.
2. Install Eclipse Classic 3.7.2 when installing Eclipse IDE.
3. Don't forget to keep your browser to no proxy while running .exe file of android sdk manager.

* Problems faced by us while installing following softwares and plugins

1. One of us firstly installed Android 4.0.3 from the SDK manager then later he was trying to install other versions of it but was unable to do so due to errors like :

Skipping 'Google APIs, Android API 8, revision 2'; it depends on 'SDK Platform Android 2.2, API 8, revision 3' which was not installed.

Skipping 'Dual Screen APIs, Android API 8, revision 1'; it depends on 'SDK Platform Android 2.2, API 8, revision 3' which was not installed.

Skipping 'Real3D, Android API 8, revision 1'; it depends on 'SDK Platform Android 2.2, API 8, revision 3' which was not installed.

Skipping 'GALAXY Tab, Android API 8, revision 1'; it depends on 'SDK Platform Android 2.2, API 8, revision 3' which was not installed.

Done. Nothing was installed.

Downloading Samples for SDK API 13, revision 1

File not found: C:\Program Files (x86)\Android\android-sdk\temp\samples-3.2_r01-linux.zip (Access is denied)

Downloading Samples for SDK API 12, revision 1

File not found: C:\Program Files (x86)\Android\android-sdk\temp\samples-3.1_r01-linux.zip (Access is denied)

Downloading Samples for SDK API 11, revision 1

File not found: C:\Program Files (x86)\Android\android-sdk\temp\samples-3.0_r01-linux.zip (Access is denied)

Downloading Samples for SDK API 10, revision 1

File not found: C:\Program Files (x86)\Android\android-sdk\temp\samples-2.3.3_r01-linux.zip (Access is denied)

Downloading Samples for SDK API 8, revision 1

File not found: C:\Program Files (x86)\Android\android-sdk\temp\samples-2.2_r01-linux.zip (Access is denied)

Skipping 'XOOM2, Android API 13, revision 2'; it depends on 'SDK Platform Android 3.2, API 13, revision 1' which was not installed.

Skipping 'Google APIs, Android API 12, revision 1'; it depends on 'SDK Platform Android 3.1, API 12, revision 3' which was not installed.

Skipping 'OpenSense SDK for Tablets, Android API 12, revision 2'; it depends on 'SDK Platform Android 3.1, API 12, revision 3' which was not installed.

Skipping 'Google APIs, Android API 11, revision 1'; it depends on 'SDK Plat

CHAPTER-5

RESULTS AND DISCUSSION

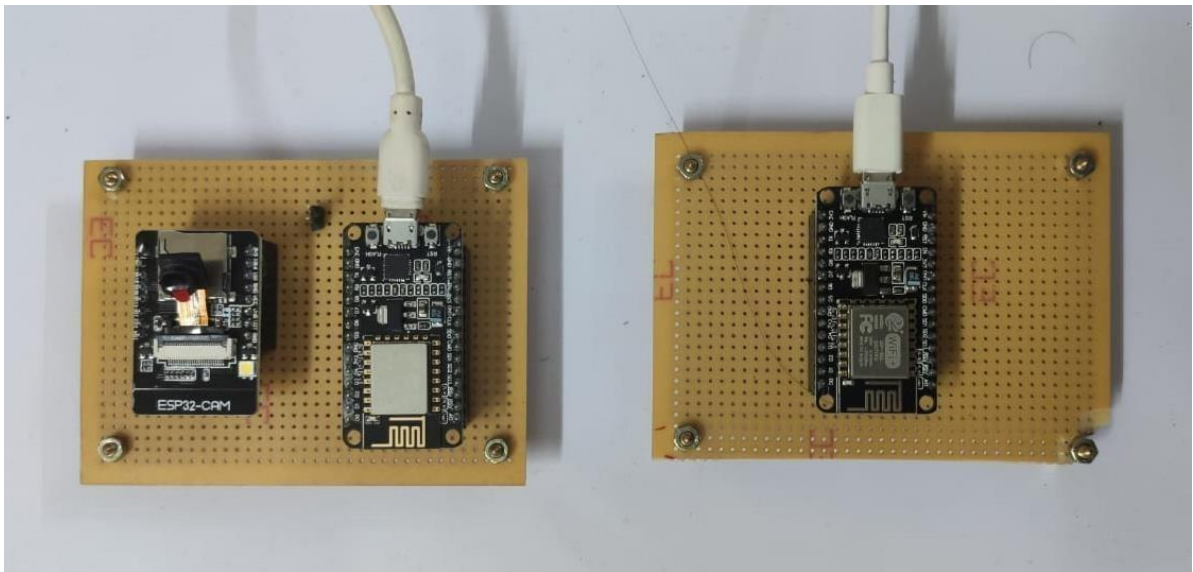


Fig 5.1:
Camera connected with Wi-fi Module

When Camera module has power supply it starts recording the surroundings with in the range, so the server side can be detected by using the client side.

When client side detects the recording camera it jams the camera

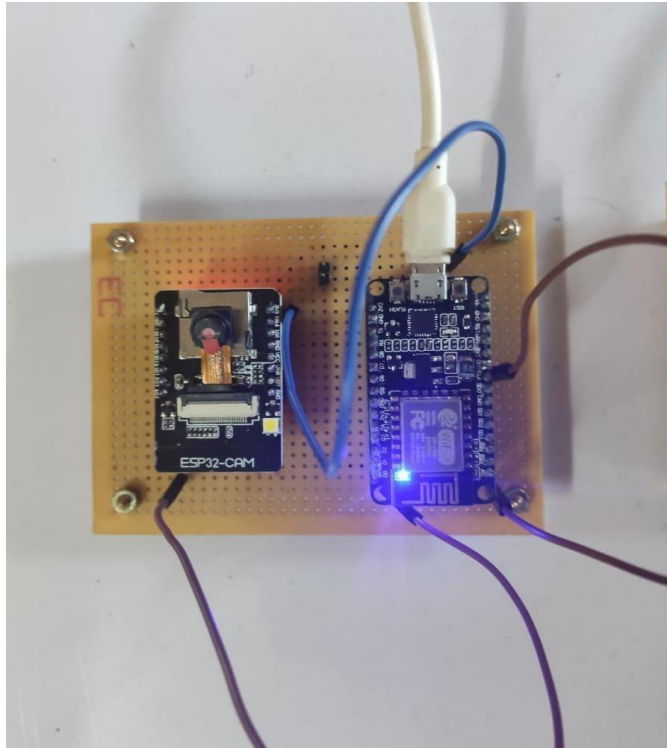


Fig 5.2:
Camera Module with Power Supply

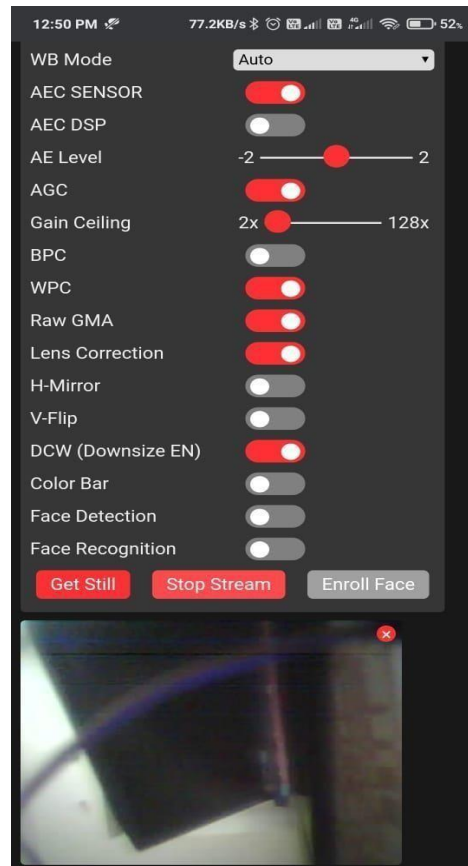


Fig 5.3: Server Side

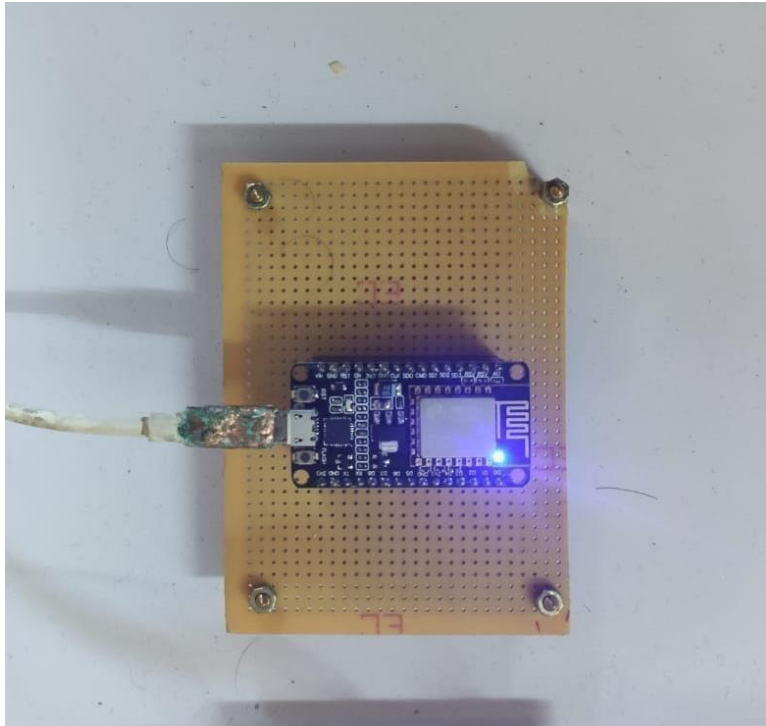


Fig 5.4: Client Side

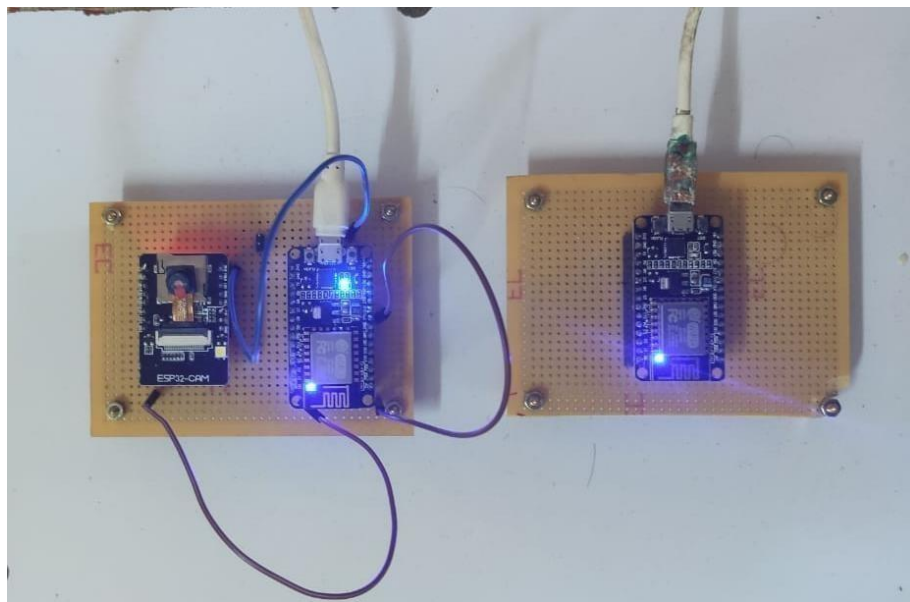


Fig 5.5: Detection of Camera

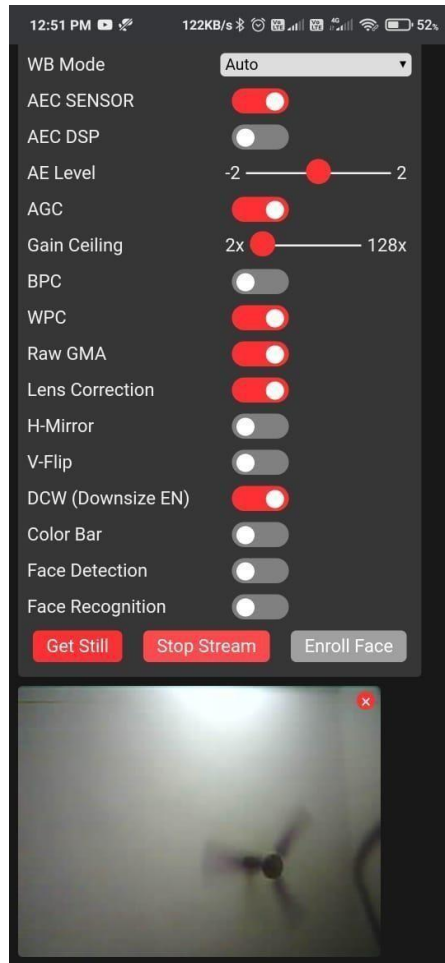


Fig 5.6: Jamming the camera

Above Pictures represents the camera jamming process , Here at first camera is detected and then it jams the camera using IoT , this leads to stop the recording camera and prevents in sharing the data.

CHAPTER-6

CONCLUSION AND FUTURE ENHANCEMENT

CONCLUSION

This paper has proposed and evaluated a novel method, Similarity of Simultaneous Observation, for detecting streaming Wi-Fi cameras. From these results, we conclude that Similarity of Simultaneous Observation is an effective approach to detecting hidden streaming cameras in a variety of environments where previous work has failed. We have identified that there are some environments in which the technique performs better than others, but even in the most difficult environments our work is valuable.

FUTURE ENHANCEMENT

Camera Jammers were everywhere in no time but it just needs development, Using this technique one can find another solution which will be an updated one, like increasing range and more compactable.

This will result in having less privacy issues in public places.

REFERENCES

1. A.Anusha,K Kiran, and J Dayanika –compressing the data secure authorized deduplication checker in hybrid cloud|| published on semantic scholar
2. Chaoling li, Yue Chen and Yanzhou Zhou –a data assured deletion scheme in clous storage|| published in china communication (volume 11, issue: 4, April 2014)
3. G.uma and L.Jayasimman –enhanced convergent encryption key generation for secured data deduplication in cloud storage|| published in journals of physics conference series
4. Huiqi Xu, Shumin Guo and Keke Chen –Building confidential and efficient query services in the cloud with RASP data perturbation|| published in IEEE transaction on knowledge and data engineering.
5. J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou. Secure deduplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.
6. J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl. A secure data deduplication scheme for cloud storage. In Technical Report, 2013.
7. Ming Li and Pan Li –crowdsourcing in cyberphysical systems: stochastic optimization with strong ability|| published in IEEE transactions on emerging topics in computing.
8. M. Bellare and A. Palacio. Gq and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In CRYPTO, pages 162-177, 2002.
9. S. Halevi, D. Harnik, B. Pinkas, and A. ShulmanPeleg. Proofs of ownership in remote storage systems. In Y. Chen, G. Danezis, and V. Shmatikov, editors, ACM Conference on Computer and Communications Security, pages 491-500. ACM, 2011
10. W. K. Ng, Y. Wen, and H. Zhu. Private data deduplication protocols in cloud storage. In S. Ossowski and P. Lecca, editors, Proceedings of the 27th Annual ACM Symposium on Applied Computing, pages 441-446. ACM, 2012.

11. Yang Tang, Patrick P.C Lee, John C.S.Lui and Radia Perlman – Secure overlay cloud storage with access control and Assured Deletion|| published in IEEE transactions on Dependable and secure Compuring

APPENDIX

SOURCE CODE

Jammer:

```
#include "esp_camera.h"

#include <WiFi.h>

//

// WARNING!!! Make sure that you have either selected ESP32 Wrover Module,

// or another board which has PSRAM enabled

//

// Select camera model

#define CAMERA_MODEL_WROVER_KIT

#define CAMERA_MODEL_ESP_EYE

#define CAMERA_MODEL_M5STACK_PSRAM

#define CAMERA_MODEL_M5STACK_WIDE

#define CAMERA_MODEL_AI_THINKER

#include "camera_pins.h"

const char* ssid = "jammer";

const char* password = "12345678";
```

```
IPAddress staticIP(192,168,43,82);
```

```
IPAddress Gateway(192,168,43,1);
```

```
IPAddress Subnet(255,255,255,0);
```

```
WiFiClient client;
```

```
WiFiServer server1(85);
```

```
void startCameraServer();
```

```
void setup() {
```

```
    Serial.begin(115200);
```

```
    Serial.setDebugOutput(true);
```

```
    Serial.println();
```

```
    pinMode(2,INPUT_PULLUP);
```

```
    camera_config_t config;
```

```
    config.ledc_channel = LEDC_CHANNEL_0;
```

```
    config.ledc_timer = LEDC_TIMER_0;
```

```
    config.pin_d0 = Y2_GPIO_NUM;
```

```
    config.pin_d1 = Y3_GPIO_NUM;
```

```
    config.pin_d2 = Y4_GPIO_NUM;
```

```

config.pin_d3 = Y5_GPIO_NUM;

config.pin_d4 = Y6_GPIO_NUM;

config.pin_d5 = Y7_GPIO_NUM;

config.pin_d6 = Y8_GPIO_NUM;

config.pin_d7 = Y9_GPIO_NUM;

config.pin_xclk = XCLK_GPIO_NUM;

config.pin_pclk = PCLK_GPIO_NUM;

config.pin_vsync = VSYNC_GPIO_NUM;

config.pin_href = HREF_GPIO_NUM;

config.pin_sscb_sda = SIOD_GPIO_NUM;

config.pin_sscb_scl = SIOC_GPIO_NUM;

config.pin_pwdn = PWDN_GPIO_NUM;

config.pin_reset = RESET_GPIO_NUM;

config.xclk_freq_hz = 20000000;

config.pixel_format = PIXFORMAT_JPEG;

//init with high specs to pre-allocate larger buffers

if(psramFound()){

    config.frame_size = FRAMESIZE_UXGA;

    config.jpeg_quality = 10;

    config.fb_count = 2;

} else {

    config.frame_size = FRAMESIZE_SVGA;

```

```
config.jpeg_quality = 12;

config.fb_count = 1;

}
```

```
#if defined(CAMERA_MODEL_ESP_EYE)
```

```
pinMode(13, INPUT_PULLUP);
```

```
pinMode(14, INPUT_PULLUP);
```

```
#endif
```

```
// camera init
```

```
esp_err_t err = esp_camera_init(&config);
```

```
if (err != ESP_OK) {
```

```
    Serial.printf("Camera init failed with error 0x%x", err);
```

```
    return;
```

```
}
```

```
sensor_t * s = esp_camera_sensor_get();
```

```
//initial sensors are flipped vertically and colors are a bit saturated
```

```
if (s->id.PID == OV3660_PID) {
```

```
    s->set_vflip(s, 1);//flip it back
```

```
    s->set_brightness(s, 1);//up the blightness just a bit
```

```
    s->set_saturation(s, -2);//lower the saturation
```

```
}
```

```
//drop down frame size for higher initial frame rate
```

```
s->set_framesize(s, FRAMESIZE_QVGA);
```

```
#if defined(CAMERA_MODEL_M5STACK_WIDE)
```

```
s->set_vflip(s, 1);
```

```
s->set_hmirror(s, 1);
```

```
#endif
```

```
WiFi.begin(ssid, password);
```

```
WiFi.config(staticIP, Gateway, Subnet);
```

```
pinMode(33,OUTPUT);
```

```
while (WiFi.status() != WL_CONNECTED) {
```

```
    delay(500);
```

```
    Serial.print(".");
```

```
}
```

```
Serial.println("");
```

```
Serial.println("WiFi connected");
```

```
digitalWrite(33,HIGH);
```

```
delay(500);
```

```
digitalWrite(33,LOW);
```

```
delay(500);

digitalWrite(33,HIGH);

delay(500);

digitalWrite(33,LOW);

delay(500);digitalWrite(33,HIGH);

delay(500);

digitalWrite(33,LOW);

delay(500);digitalWrite(33,HIGH);

delay(500);

digitalWrite(33,LOW);

delay(500);digitalWrite(33,HIGH);

delay(500);

digitalWrite(33,LOW);

delay(500);

Serial.println("Connected to wifi");

client.println("Connected to wifi");

Serial.print("Status: "); Serial.println(WiFi.status()); // Network parameters

Serial.print("IP: "); Serial.println(WiFi.localIP());

Serial.print("Subnet: "); Serial.println(WiFi.subnetMask());

Serial.print("Gateway: "); Serial.println(WiFi.gatewayIP());

Serial.print("SSID: "); Serial.println(WiFi.SSID());

Serial.print("Signal: "); Serial.println(WiFi.RSSI());
```

```

startCameraServer();

Serial.print("Camera Ready! Use 'http://");

Serial.print(WiFi.localIP());

Serial.println(" to connect");

}

void loop()

{

    if (digitalRead(2) == LOW) ESP.restart();

}

// WiFiClient client = server1.available();

// if (!client)

// {

//     return;

// }

// Serial.println("new client");

// while(!client.available()){

//     delay(1);

// }

//     String request_from_bike = client.readStringUntil('\r');

```

```
// Serial.println(request_from_bike);  
  
//}
```

Camera Pin:

```
#include "esp_camera.h"  
#include <WiFi.h>  
  
//  
// WARNING!!! Make sure that you have either selected ESP32 Wrover Module,  
// or another board which has PSRAM enabled  
//  
  
// Select camera model  
//#define CAMERA_MODEL_WROVER_KIT  
//#define CAMERA_MODEL_ESP_EYE  
//#define CAMERA_MODEL_M5STACK_PSRAM  
//#define CAMERA_MODEL_M5STACK_WIDE  
#define CAMERA_MODEL_AI_THINKER  
  
#include "camera_pins.h"  
  
const char* ssid = "jammer";  
const char* password = "12345678";  
  
IPAddress staticIP(192,168,43,82);  
IPAddress Gateway(192,168,43,1);  
IPAddress Subnet(255,255,255,0);  
  
WiFiClient client;  
WiFiServer server1(85);  
  
void startCameraServer();
```

```

void setup() {
    Serial.begin(115200);
    Serial.setDebugOutput(true);
    Serial.println();
    pinMode(2,INPUT_PULLUP);

    camera_config_t config;
    config.ledc_channel = LEDC_CHANNEL_0;
    config.ledc_timer = LEDC_TIMER_0;
    config.pin_d0 = Y2_GPIO_NUM;
    config.pin_d1 = Y3_GPIO_NUM;
    config.pin_d2 = Y4_GPIO_NUM;
    config.pin_d3 = Y5_GPIO_NUM;
    config.pin_d4 = Y6_GPIO_NUM;
    config.pin_d5 = Y7_GPIO_NUM;
    config.pin_d6 = Y8_GPIO_NUM;
    config.pin_d7 = Y9_GPIO_NUM;
    config.pin_xclk = XCLK_GPIO_NUM;
    config.pin_pclk = PCLK_GPIO_NUM;
    config.pin_vsync = VSYNC_GPIO_NUM;
    config.pin_href = HREF_GPIO_NUM;
    config.pin_sscb_sda = SIOD_GPIO_NUM;
    config.pin_sscb_scl = SIOC_GPIO_NUM;
    config.pin_pwdn = PWDN_GPIO_NUM;
    config.pin_reset = RESET_GPIO_NUM;
    config.xclk_freq_hz = 20000000;
    config.pixel_format = PIXFORMAT_JPEG;
    //init with high specs to pre-allocate larger buffers
    if(psramFound()){
        config.frame_size = FRAMESIZE_UXGA;
        config.jpeg_quality = 10;
        config.fb_count = 2;
    }
}

```

```

    } else {
        config.frame_size = FRAMESIZE_SVGA;
        config.jpeg_quality = 12;
        config.fb_count = 1;
    }

#ifdef CAMERA_MODEL_ESP_EYE
    pinMode(13, INPUT_PULLUP);
    pinMode(14, INPUT_PULLUP);
#endif

    // camera init
    esp_err_t err = esp_camera_init(&config);
    if (err != ESP_OK) {
        Serial.printf("Camera init failed with error 0x%x", err);
        return;
    }

    sensor_t * s = esp_camera_sensor_get();
    //initial sensors are flipped vertically and colors are a bit saturated
    if (s->id.PID == OV3660_PID) {
        s->set_vflip(s, 1); //flip it back
        s->set_brightness(s, 1); //up the blightness just a bit
        s->set_saturation(s, -2); //lower the saturation
    }
    //drop down frame size for higher initial frame rate
    s->set_framesize(s, FRAMESIZE_QVGA);

#ifdef CAMERA_MODEL_M5STACK_WIDE
    s->set_vflip(s, 1);
    s->set_hmirror(s, 1);
#endif

```

```

WiFi.begin(ssid, password);
WiFi.config(staticIP, Gateway, Subnet);
pinMode(33,OUTPUT);

while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
}
Serial.println("");
Serial.println("WiFi connected");
digitalWrite(33,HIGH);
delay(500);
digitalWrite(33,LOW);
delay(500);
digitalWrite(33,HIGH);
delay(500);
digitalWrite(33,LOW);
delay(500);digitalWrite(33,HIGH);
delay(500);
digitalWrite(33,LOW);
delay(500);digitalWrite(33,HIGH);
delay(500);
digitalWrite(33,LOW);
delay(500);digitalWrite(33,HIGH);
delay(500);
digitalWrite(33,LOW);
delay(500);
Serial.println("Connected to wifi");
client.println("Connected to wifi");
Serial.print("Status: "); Serial.println(WiFi.status()); // Network parameters
Serial.print("IP: "); Serial.println(WiFi.localIP());
Serial.print("Subnet: "); Serial.println(WiFi.subnetMask());
Serial.print("Gateway: "); Serial.println(WiFi.gatewayIP());

```

```

Serial.print("SSID: "); Serial.println(WiFi.SSID());
Serial.print("Signal: "); Serial.println(WiFi.RSSI());

startCameraServer();

Serial.print("Camera Ready! Use 'http://'");
Serial.print(WiFi.localIP());
Serial.println(" to connect");
}

void loop()
{
  if (digitalRead(2) == LOW) ESP.restart();
}
// WiFiClient client = server1.available();
// if (!client)
// {
//   return;
// }
// Serial.println("new client");
// while(!client.available()){
//   delay(1);
// }
//   String request_from_bike = client.readStringUntil('\r');
//   Serial.println(request_from_bike);
//}

```

JOURNAL PAPER

HIDDEN CAMERA DETECTION & JAMMING Using IoT

Kshatri Manas Singh¹, Kuchibhatla Sri Kameswara Prasad²

¹B.E. Computer science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India

²B.E. Computer science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India

ABSTRACT: *Hidden Camera so called “Spy Camera” used to record something without having prior knowledge, it is not visible for objects that are being recorded. Usage of this cameras in public places increased rapidly, hidden camera videos can be shared through a network.*

The client side detects the network where camera is recording/streaming and jams the camera that is connected to that network using IoT. Here the cameras connected to the whole network can be jammed. Extension to this RFID is added to detect Hidden camera signals and can predict that a camera is present in that area.

Keywords:- NODEMCU, MICROCONTROLLER, DETECTOR, JAMMING

I. INTRODUCTION

A hidden camera can be anywhere. We should know about this aspect, because we might be in particular place where our action will be recorded without us being aware of it. Unfortunately, reason that makes this device so effective can also leads to its misuse by someone. Profits are made through exploiting this to others whose actions have been monitored by a hidden. There should be same way which can help the person from spy to maintain their privacy Camera is the most common thing that is being used by each and every person in the world, some people use camera for good purposes and some for bad once. To stop using camera for bad we came with an idea of jamming the camera in restricted areas. In this if a camera is hidden and cannot be seen anywhere we use RFID to detect the signals and then camera which is connect to a network can be jammed using IoT technology. Till now there is no proper camera jammer in the world still many researches were undergoing on this one.

II. LITERATURE SURVEY

Literature survey is that the most vital step in package development technique. Preceding to developing up the device it's mandatory to see the time problem, financial and friends strength. When this stuff ar glad, at that point back to back advance is to see that bundle and language is utilized for building up the device. When the developers start fabricating the device the software engineers need load of outer help. This help is acquired from senior software engineers, from publications or from websites. Preceding to developing the framework the on top of thought AR contemplated for building up the arranged framework. the key a piece of the

venture advancement area considers and thoroughly study every one of the ideal needs for building up the undertaking. for each task Literature overview is that the most crucial area in bundle improvement strategy. Before developing the tools and also the associated planning it's necessary to see and survey the time issue, resource demand, man power, economy, and company strength. Once this stuff ar happy and totally surveyed, then consecutive step is to see regarding the package specifications within the individual system like what variety of package the project would need and what ar all the required package AR required to proceed with consecutive step like developing the tools, and also the associated operations. Here we've got taken the reviews of varied authors and noted down the most key-points concerning their work. during this project literature survey plays a dominant role in get resources from varied domains and every one the connected topics that ar terribly helpful below this section. the simplest half if this can be the approach things get so as and helps North American nation to suite our add relevance the present information.

1. “IoT Localization for Bistatic Passive UHF RFID Systems with 3D Radiation Pattern” ,Abdullah Kadri - 2017

Passive Radio-Frequency Identification (RFID) systems carry important importance for Internet of Things (IoT) applications because of their energy harvest home capabilities

Disadvantages:

In these paper they identify the rf signal and gives the 3d map level of RF not to give any notification to the persons

2. DroidDetector: Android Malware Characterization and Detection Using Deep Learning – Zhenlong Yun - 2016

Smartphones and mobile tablets square measure quickly turning into necessity in everyday living. golem was the foremost widespread mobile software system from 2012. Nevertheless, thanks to the open nature of golem, myriad malwares square measure unseen during a sizable ammount of good apps in golem retailers that solemnly frighten golem security. Deep learning could be a current space of machine learning analysis that has acquired rising observation in computer science Artificial Intelligence.

Disadvantages:

By using these method we have to install android app, Some time it may not gives an alert

3.A Learning Approach Towards Detection and Tracking of Lane Markings – Raghuraman Gopalan - 2012

Street scene examination is a difficult issue that has applications in self-sufficient route of vehicles. A necessary segment of this framework is the powerful location and following of path checking.

Disadvantages:

The given proposed system is done by using image processing method to identify the camera using edge detection but in real time camera must me in hidden so to find camera is not possible

4.A Predictable Framework for Safety-Critical Embedded Systems – Sidharta Andalam - 2013

Security basic installed frameworks, normally seen in auto, space, and health-care, are profoundly responsive and simultaneous. Their maximum significant qualities are that they need both utilitarian and timing rightness. C has been the language of decision for programming such frameworks.

Diadvantages:

By using embedded sensor to give security to the women's if she got arrestment by some one means send the message to police station. But in these project they never identifies the camera

5. PRESENCE OF ACTIVE MOBILE PHONES AND HIDDEN CAMERA DETECTION - T.Sivasakthi – 2017

In our everyday life the use of cell phones has been upgraded in limited space like test settings, spots of vital gathering, workplaces, meeting lobbies, jail and so forth and thusly the secret remote camera in preliminary rooms and inns, public swamps. The recurrence signals region unit communicated from remote camera and movable all through the video transmission, approaching choice and active choice, instant messages from one doohickey to an alternate. The noticeor

can identify the sent sign at that point it's proposals as contribution to AT super eight microcontroller. As by and by in light of the fact that the Arduino microcontroller gets the sign, it'll initiate the blare caution and hence the information will be appeared on the alphanumeric presentation show and conjointly sends the message like portable distinguished with area, zone assortment and so on to the versatile assortment keep inside the microcontroller by victimisation the GSM module. this method are wont to see the cell phones and hence the remote secret camera blessing in an incredibly region by the recurrence flags that region unit sent by them.

6. Detecting Hidden Streaming Cameras Through Similarity of Simultaneous Observation – Kevin - 2019

Little, minimal effort, remote cameras are getting progressively ordinary making clandestine perception of individuals harder to find. Past add police examination covered up cameras has exclusively self-tended to limited conditions in little zones where the client has imperative administration of the environmental factors. To address this drawback in an incredibly less constrained extent of conditions, we present the prospect of likeness of synchronal perception any place the client uses a camera (Wi-Fi camera, camera on a compact or PC) to coordinate with worldly request examples of information sent by presumably covered up cameras and subsequently the fleeting request designs that square measure anticipated from the moment that the better-realized camera is running. To research the examples, they tend to apply numerous comparability estimates Associate in Nursingd incontestible a precision of more than 87 and F1 score of zero.88 abuse Associate in Nursing efficient edge based grouping. Besides, we tend to utilized our insight laid to mentor a neural organization and considered improvised to have exactness as maximum as 97 and a F1 score over zero.95 for each inside and outside settings. From these outcomes, we will in general presume that similitude of synchronal perception could be a potential system for police examination covered up remote cameras that square measure real time video of a client. Our work eliminates huge limits that are put on past location strategy.

7. DeWiCam: Detecting Hidden Wireless Cameras via Smartphones – Yushi Cheng – 2018

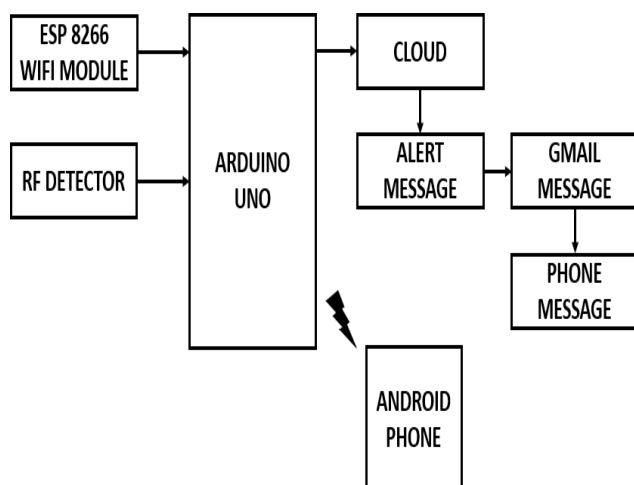
Remote cameras square measure wide sent in police work frameworks for security guarding. Notwithstanding, the protection issues identified with unapproved recording, square measure drawing partner expanding consideration as of late. Existing recognition ways for unapproved remote cameras square measure either limited by their discovery exactness or requiring committed gadgets. during the paper, they tend to propose DeWiCam, a light-weight and successful identification instrument misuse smartphones. the essential arrangement of DeWiCam is to use the characteristic traffic examples of streams from remote cameras. Contrasted and old course examination, DeWiCam is more troublesome because of it can't get to the scrambled information inside the information bundles. However, DeWiCam conquers the issue

and may see close to remote cameras dependably. To more decide if a camera is in partner intrigued space, we tend to propose a human-helped distinguishing proof model. we tend to execute DeWiCam on the humanoid stage and valuate it with inside and out probes twenty cameras. The investigation results show that DeWiCam will see cameras with partner precision of 99 among a couple of.7 s.

III. PROPOSED SYSTEM:

The Given Proposed System Is Done By Using Arduino Lilly pad microcontroller. The esp8266 is a Wi-Fi module to provide internet connection to an controller. The RF sensor is used to find the hidden camera. When an hidden camera is detected RF sensor is getting trigger and send the value to the cloud. By using cloud it send the alert message to the person and also to the family person and also gives the siren sound through the buzzer

IV. BLOCK DIAGRAM:



V. HARDWARE USED:

- ARDUINO LILLYPAD
- RF DETECTOR
- ESP8266 WIFI MODULE

ARDUINO

“Arduino is an open-source physical computing platform. It is based on a simple i/o board and a development environment

that implements the Processing / Wiring language. Arduino can be used to develop stand-alone interactive objects

Otherwise it can be connected to software on your computer.“ A physical Input / Output board (I/O) with a programmable Integrated Circuit (IC).

Arduino is a platform

Arduino includes an Integrated Development Environment (IDE) for programming. The language itself is deployed in C but is widely prototyped upon the www.processing.org language.

Microcontroller (ATmega-8A)

- ❖ Maximum-performance, Minimal-power AVR® 8-bit Microcontroller
- ❖ Up to date RISC Architecture
- ❖ High Endurance Non-volatile Memory segments
- ❖ Peripheral Features
- ❖ Special Microcontroller Features
- ❖ Input/Output and Packages
- ❖ Operating Voltages
- ❖ 2.7 - 5.5V (ATmega8L)
- ❖ Speed Grades
- ❖ 0 - 8 MHz (ATmega8L)
- ❖ 0 - 16 MHz (ATmega8)
- ❖ Power Consumption at 4 MHz, 3V, 25°C

Node mcu:

Node MCU is an open-source Lua based firmware and advancement board uncommonly focused for IoT based Applications. It assimilates firmware that sudden rise in request for the ESP8266 Wi-Fi SoC from Espressif Systems, and tools which based on the ESP-12 module. The Nodemcu ESP8266 development board to go with the ESP-12E module having ESP8266 chip having Tensilica Xtensa 32-cycle LX106 RISC microchip. This chip upholds RTOS and works at 80MHz to 160 MHz customizable clock frequency. NodeMCU has 128 KB RAM and 4MB of Flash memory to save information and projects. Its high preparing power with in-gathered Wi-Fi/Bluetooth and Deep Sleep Operating highlights make it ideal for IoT projects. NodeMCU can be fueled utilizing Micro USB jack and VIN pin (External Supply Pin). It upholds UART, SPI, and I2C interface.

Applications of NodeMCU

- Modelling of IoT devices
- Minimal power battery worked applications
- Network designs
- Designs needing various Input/Output interfaces with Wi-Fi and Bluetooth functionalities

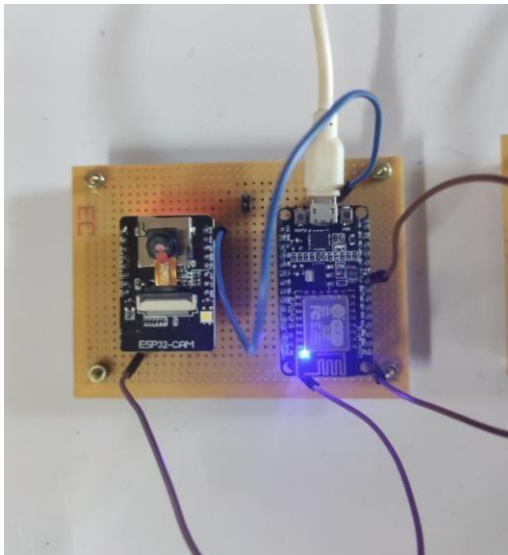
RF detector:

A radio frequency (RF) finder is a gadget used to distinguish the presence of RF waves either in a remote or wired actual transmission medium. They are otherwise called RF power indicators or RF reacting identifiers and are accessible as gadgets or modules. In the present innovative world, reconnaissance cameras are all over. Secret camera indicator applications are accessible on your Android or iPhone or at a local security store "A secret camera finder can discover a camera anyplace regardless of how well it's covered up.

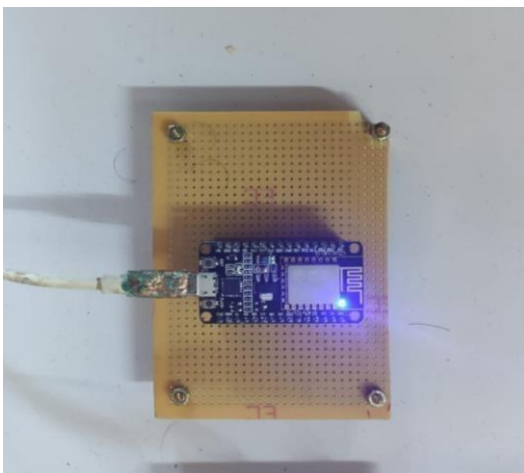
VI. SOFTWARE USED:

- ARDUINO C

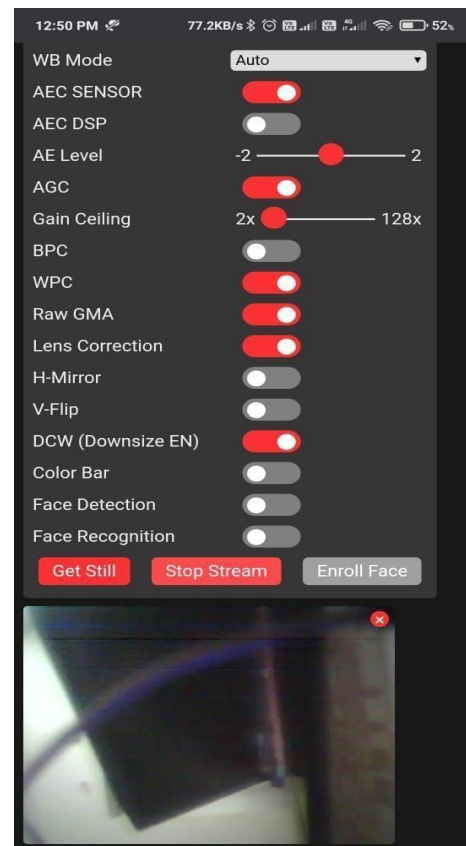
VII. OUTPUT



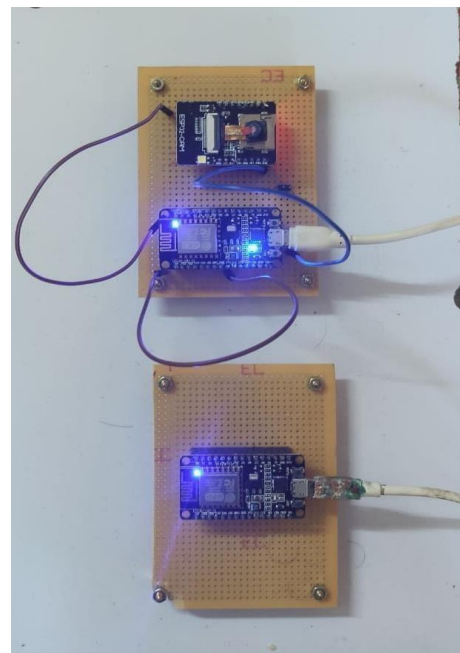
Output



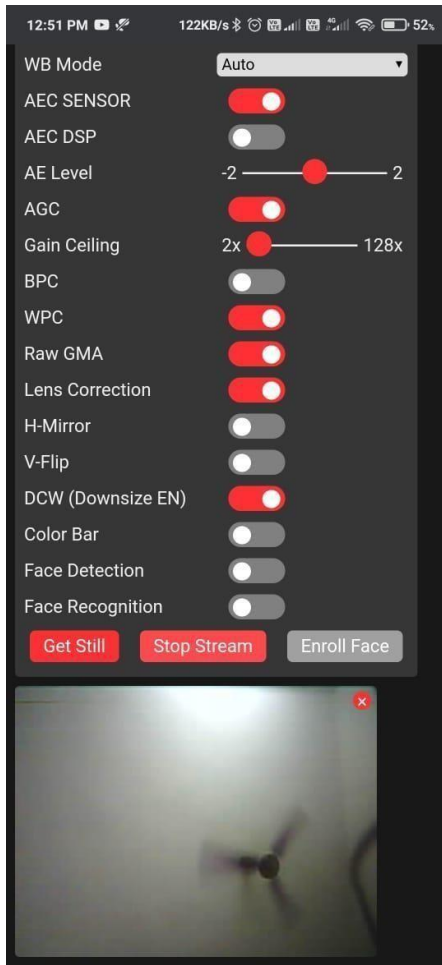
Client Side



Server Side



Detection of Camera



Jamming the camera

VIII. CONCLUSION AND FUTURE WORK

This paper has put forward and analysed a tentative method, Closeness of Simultaneous Observation, for recognizing surging Wi-Fi cameras. From these outputs, we assume that Closeness of Simultaneous Observation is a convincing method to manage recognizing concealed streaming cameras in a grouping of conditions where past work has not passed. We have perceived that there are a couple of conditions where the methodology work better contrasted with others, yet even in most problematic conditions our project is significant.

REFERENCES:

- [1] W. Zai-jian, Y. n. Dong, H. x. Shi, Y. Lingyun, and T. Pingping. Internet video trace classification using qos features. ICNC, 2016.
- [2] S. Zhu, C. Zhang, and X. Zhang. Automating visual privacy protection using a smart led. ACM MobiCom, 2017.
- [3] Z. Li, Z. Xiao, Y. Zhu, I. Pattarachanyakul, B. Y. Zhao, and H. Zheng. Adversarial localization against wireless cameras. ACM HotMobile, 2018.
- [4] B. Nassi, R. Ben-Netanel, A. Shamir, and Y. Elovici. Game of drones - detecting streamed POI from encrypted FPV channel. CoRR, 2018.
- [5] P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han, and T. Vu. Matthan: Drone presence detection by

identifying physical signatures in the drone's rf communication. ACM MobiSys, 2017.

- [6] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall. 802.11 user ngerprinting. ACM MobiCom, 2007.
- [7] A. Rao, A. Legout, Y.-s. Lim, D. Towsley, C. Barakat, and W. Dabbous. Network characteristics of video streaming trac. ACM CoNEXT, 2011.
- [8] B. Saltaformaggio, H. Choi, K. Johnson, Y. Kwon, Q. Zhang, X. Zhang, D. Xu, and J. Qian. Eavesdropping on ne-grained user activities within smartphone apps over encrypted network trac. Usenix WOOT, 2016. [28] S. Siby, R. R. Maiti, and N. O. Tippenhau

PLAGIARISM REPORT

155_Paper 66 report

by Plagiarism Checker

Submission date: 06-Apr-2021 11:33AM (UTC-0400)

Submission ID: 1512279468

File name: 1617722261523_1617721953155_Paper_66.docx (569.62K)

Word count: 2360

Character count: 12736

HIDDEN CAMERA DETECTION & JAMMING Using IoT

Kshatri Manas Singh¹, Kuchibhatla Sri Kameswara Prasad²

¹B.E. Computer science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India

²B.E. Computer science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India

ABSTRACT: Hidden Camera so called “Spy Camera” used to record something without having prior knowledge, it is not visible for objects that are being recorded. Usage of this cameras in public places increased rapidly, hidden camera videos can be shared through a network.

The client side detects the network where camera is recording/streaming and jams the camera that is connected to that network using IoT. Here the cameras connected to the whole network can be jammed. Extension to this RFID is added to detect Hidden camera signals and can predict that a camera is present in that area.

Keywords:- NODEMCU, MICROCONTROLLER, DETECTOR, JAMMING

I. INTRODUCTION

A hidden camera can be anywhere. We should know about this aspect, because we might be in particular place where our action will be recorded without us being aware of it. Unfortunately, reason that makes this device so effective can also leads to its misuse by someone. Profits are made through exploiting this to others whose actions have been monitored by a hidden. There should be same way which can help the person from spy to maintain their privacy. Camera is the most common thing that is being used by each and every person in the world, some people use camera for good purposes and some for bad once. To stop using camera for bad we came with an idea of jamming the camera in restricted areas. In this if a camera is hidden and cannot be seen anywhere we use RFID to detect the signals and then camera which is connect to a network can be jammed using IoT technology. Till now there is no proper camera jammer in the world still many researches were undergoing on this one.

II. LITERATURE SURVEY

Literature survey is that the most vital step in package development technique. Preceding to developing up the device it's mandatory to see the time problem, financial and friends strength. When this stuff ar glad, at that point back to back advance is to see that bundle and language is utilized for building up the device. When the developers start fabricating the device the software engineers need load of outer help. This help is acquired from senior software engineers, from publications or from websites. Preceding to developing the framework the on top of thought AR contemplated for building up the arranged framework. the key a piece of the

venture advancement area considers and thoroughly study every one of the ideal needs for building up the undertaking. for each task Literature overview is that the most crucial area in bundle improvement strategy. Before developing the tools and also the associated planning it's necessary to see and survey the time issue, resource demand, man power, economy, and company strength. Once this stuff ar happy and totally surveyed, then consecutive step is to see regarding the package specifications within the individual system like what variety of package the project would need and what ar all the required package AR required to proceed with consecutive step like developing the tools, and also the associated operations. Here we've got taken the reviews of varied authors and noted down the most key-points concerning their work. during this project literature survey plays a dominant role in get resources from varied domains and every one the connected topics that ar terribly helpful below this section. the simplest half if this can be the approach things get so as and helps North American nation to suite our add relevance the present information.

12

1. “IoT Localization for Bistatic Passive UHF RFID Systems with 3D Radiation Pattern” ,Abdullah Kadri - 2017

11

Passive Radio-Frequency Identification (RFID) systems carry important importance for Internet of Things (IoT) applications because of their energy harvest home capabilities

Disadvantages:

In these paper they identify the rf signal and gives the 3d map level of RF not to give any notification to the persons

14

2.DroidDetector: Android Malware Characterization and Detection Using Deep Learning – Zhenlong Yun - 2016

Smartphones and mobile tablets square measure quickly turning into necessity in everyday living. golem was the foremost widespread mobile software system from 2012. Nevertheless, thanks to the open nature of golem, myriad malwares square measure unseen during a sizable ammount of good apps in golem retailers that solemnly frighten golem security. Deep learning could be a current space of machine learning analysis that has acquired rising observation in computer science Artificial Intelligence.

Disadvantages:

By using these method we have to install android app, Some time it may not gives an alert

5

3.A Learning Approach Towards Detection and Tracking of Lane Markings – Raghuraman Gopalan - 2012

Street scene examination is a difficult issue that has applications in self-sufficient route of vehicles. A necessary segment of this framework is the powerful location and following of path checking.

Disadvantages:

The given proposed system is done by using image processing method to identify the camera using edge detection but in real time camera must me in hidden so to find camera is not possible

5

4.A Predictable Framework for Safety-Critical Embedded Systems – Sidharta Andalam - 2013

Security basic installed frameworks, normally seen in auto, space, and health-care, are profoundly responsive and simultaneous. Their maximum significant qualities are that they need both utilitarian and timing rightness. C has been the language of decision for programming such frameworks.

Diadvantages:

By using embedded sensor to give security to the women's if she got arrestment by some one means send the message to police station. But in these project they never identifies the camera

5.PRESENCE OF ACTIVE MOBILE PHONES AND HIDDEN CAMERA DETECTION - T.Sivasakthi – 2017

In our everyday life the use of cell phones has been upgraded in limited space like test settings, spots of vital gathering, workplaces, meeting lobbies, jail and so forth and thusly the secret remote camera in preliminary rooms and inns, public swamps. The recurrence signals region unit communicated from remote camera and movable all through the video transmission, approaching choice and active choice, instant messages from one doohickey to an alternate. The noticeor

can identify the sent sign at that point it's proposals as contribution to AT super eight microcontroller. As by and by in light of the fact that the Arduino microcontroller gets the sign, it'll initiate the blare caution and hence the information will be appeared on the alphanumeric presentation show and conjointly sends the message like portable distinguished with area, zone assortment and so on to the versatile assortment keep inside the microcontroller by victimisation the GSM module. this method are wont to see the cell phones and hence the remote secret camera blessing in an incredibly region by the recurrence flags that region unit sent by them.

15

6.Detecting Hidden Streaming Cameras Through Similarity of Simultaneous Observation – Kevin - 2019

Little, minimal effort, remote cameras are getting progressively ordinary making clandestine perception of individuals harder to find. Past add police examination covered up cameras has exclusively self-tended to limited conditions in little zones where the client has imperative administration of the environmental factors. To address this drawback in an incredibly less constrained extent of conditions, we present the prospect of likeness of synchronal perception any place the client uses a camera (Wi-Fi camera, camera on a compact or PC) to coordinate with worldly request examples of information sent by presumably covered up cameras and subsequently the fleeting request designs that square measure anticipated from the moment that the better-realized camera is running. To research the examples, they tend to apply numerous comparability estimates Associate in Nursingd incontestible a precision of more than 87 and F1 score of zero.88 abuse Associate in Nursinging efficient edge based grouping. Besides, we tend to utilized our insight laid to mentor a neural organization and considered improvised to have exactness as maximum as 97 and a F1 score over zero.95 for each inside and outside settings. From these outcomes, we will in general presume that similitude of synchronal perception could be a potential system for police examination covered up remote cameras that square measure real time video of a client. Our work eliminates huge limits that are put on past location strategy.

7

7.DeWiCam: Detecting Hidden Wireless Cameras via Smartphones – Yushi Cheng – 2018

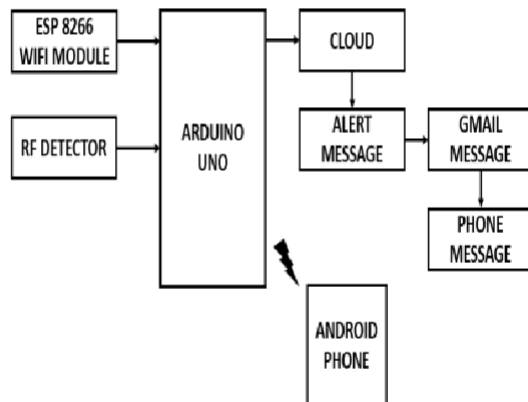
Remote cameras square measure wide sent in police work frameworks for security guarding. Notwithstanding, the protection issues identified with unapproved recording, square measure drawing partner expanding consideration as of late. Existing recognition ways for unapproved remote cameras square measure either limited by their discovery exactness or requiring committed gadgets. during the paper, they tend to propose DeWiCam, a light-weight and successful identification instrument misuse smartphones. the essential arrangement of DeWiCam is to use the characteristic traffic examples of streams from remote cameras. Contrasted and old course examination, DeWiCam is more troublesome because of it can't get to the scrambled information inside the information bundles. However, DeWiCam conquers the issue

and may see close to remote cameras dependably. To more decide if a camera is in partner intrigued space, we tend to propose a human-helped distinguishing proof model. we tend to execute DeWiCam on the humanoid stage and value it with inside and out probes twenty cameras. The investigation results show that DeWiCam will see cameras with partner precision of 99 among a couple of 7 s.

III. PROPOSED SYSTEM:

The Given Proposed System Is Done By Using Arduino Lilly pad microcontroller. The esp8266 is a Wi-Fi module to provide internet connection to an controller. The RF sensor is used to find the hidden camera. When an hidden camera is detected RF sensor is getting trigger and send the value to the cloud. By using cloud it send the alert message to the person and also to the family person and also gives the siren sound through the buzzer

IV. BLOCK DIAGRAM:



V. HARDWARE USED:

- ARDUINO LILLYPAD
- RF DETECTOR
- ESP8266 WIFI MODULE

6 ARDUINO

“Arduino is an open-source physical computing platform. It is based on a simple i/o board and a development environment

that implements the Processing / Wiring language. Arduino can be used to develop stand-alone interactive objects

Otherwise it can be connected to software on your computer.” A physical Input / Output board (I/O) with a programmable Integrated Circuit (IC).

Arduino is a platform

Arduino includes an Integrated Development Environment (IDE) for programming. The language itself is deployed in C but is widely prototyped upon the www.processing.org language.

Microcontroller (ATmega-8A)

- ❖ Maximum-performance, Minimal-power AVR® 8-bit Microcontroller
- ❖ Up to date RISC Architecture
- ❖ High Endurance Non-volatile Memory segments
- ❖ Peripheral Features
- ❖ Special Microcontroller Features
- ❖ Input/Output and Packages
- ❖ Operating Voltages
- ❖ 2.7 - 5.5V (ATmega8L)
- ❖ Speed Grades
- ❖ 0 - 8 MHz (ATmega8L)
- ❖ 0 - 16 MHz (ATmega8)
- ❖ Power Consumption at 4 MHz, 3V, 25°C

Node mcu:

Node MCU is an open-source Lua based firmware and advancement board uncommonly focused for IoT based Applications. It assimilates firmware that sudden rise in request for the ESP8266 Wi-Fi SoC from Espressif Systems, and tools which based on the ESP-12 module. The Nodemcu ESP8266 development board to go with the ESP-12E module having ESP8266 chip having Tensilica Xtensa 32-cycle LX106 RISC microchip. This chip upholds RTOS and works at 80MHz to 160 MHz customizable clock frequency. NodeMCU has 128 KB RAM and 4MB of Flash memory to save information and projects. Its high preparing power with in-gathered Wi-Fi/Bluetooth and Deep Sleep Operating highlights make it ideal for IoT projects. NodeMCU can be fueled utilizing Micro USB jack and VIN pin (External Supply Pin). It upholds UART, SPI, and I2C interface.

Applications of NodeMCU

- Modelling of IoT devices
- Minimal power battery worked applications
- Network designs
- Designs needing various Input/Output interfaces with Wi-Fi and Bluetooth functionalities

17

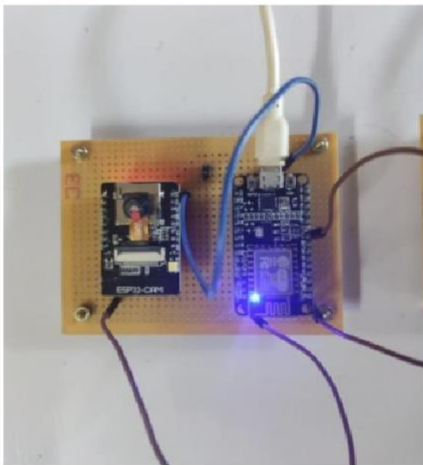
RF detector:

A radio frequency (RF) finder is a gadget used to distinguish the presence of RF waves either in a remote or wired actual transmission medium. They are otherwise called RF power indicators or RF reacting identifiers and are accessible as gadgets or modules. In the present innovative world, reconnaissance cameras are all over. Secret camera indicator applications are accessible on your Android or iPhone or at a local security store. ... "A secret camera finder can discover a camera anyplace regardless of how well it's covered up.

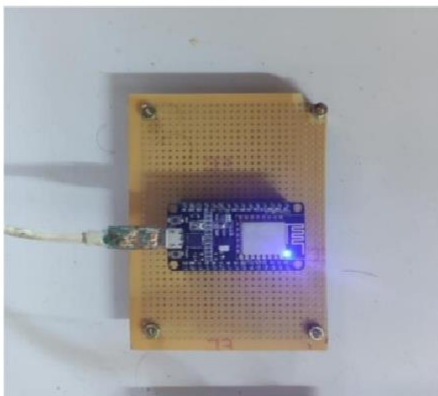
VI. SOFTWARE USED:

- ARDUINO C

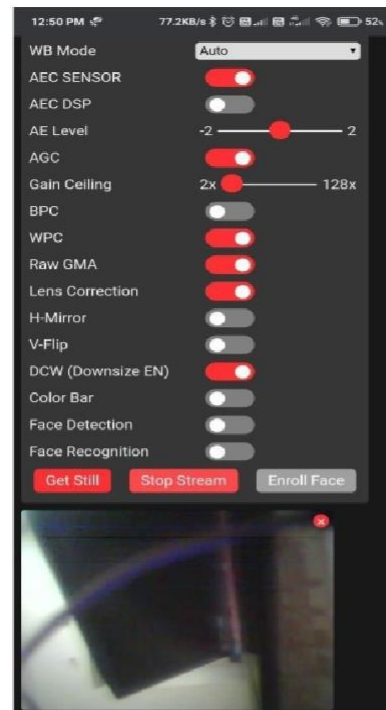
VII. OUTPUT



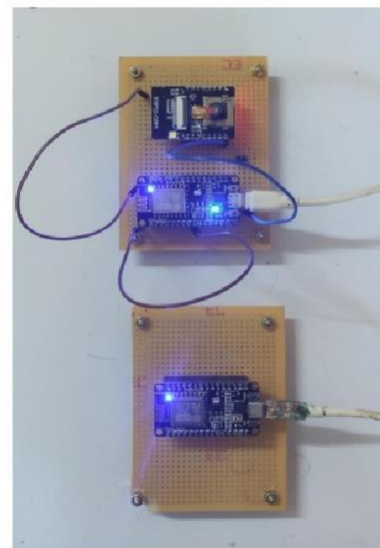
Output



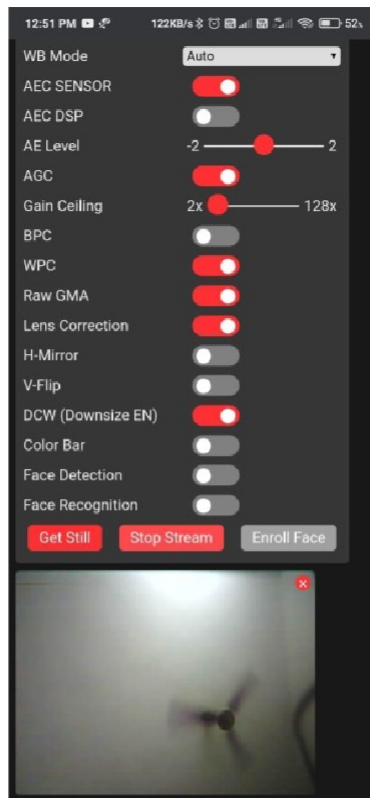
Client Side



Server Side



Detection of Camera



Jamming the camera

VIII. CONCLUSION AND FUTURE WORK

³ This paper has put forward and analysed a tentative method, Closeness of Simultaneous Observation, for recognizing surging Wi-Fi cameras. From these outputs, we assume that Closeness of Simultaneous Observation is a convincing method to manage recognizing concealed streaming cameras in a grouping of conditions where past work has not passed. We have perceived that there are a couple of conditions where the methodology work better contrasted with others, yet even in most problematic conditions our project is significant.

REFERENCES:

- [1] W. Zai-jian, Y. n. Dong, H. x. Shi, Y. Lingyun, and T. Pingping. Internet video trace classification using qos features. ICNC, 2016.
- [2] S. Zhu, C. Zhang, and X. Zhang. Automating visual privacy protection using a smart led. ACM MobiCom, 2017.
- [3] Z. Li, Z. Xiao, Y. Zhu, I. Pattarachanyakul, B. Y. Zhao, and H. Zheng. Adversarial localization against wireless cameras. ACM HotMobile, 2018.
- [4] B. Nassi, R. Ben-Netanel, A. Shamir, and Y. Elovici. Game of drones - detecting streamed POI from encrypted FPV channel. CoRR, 2018.
- [5] P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han, and T. Vu. Matthan: Drone presence detection by

identifying physical signatures in the drone's rf communication. ACM MobiSys, 2017.

[6] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall. 802.11 user fingerprinting. ACM MobiCom, 2007.

[7] A. Rao, A. Legout, Y.-s. Lim, D. Towsley, C. Barakat, and W. Dabbous. Network characteristics of video streaming trac. ACM CoNEXT, 2011.

[8] B. Saltaformaggio, H. Choi, K. Johnson, Y. Kwon, Q. Zhang, X. Zhang, D. Xu, and J. Qian. Eavesdropping on ne-grained user activities within smartphone apps over encrypted network trac. Usenix WOOT, 2016. [28] S. Siby, R. R. Maiti, and N. O. Tippenhau

155_Paper 66 report

ORIGINALITY REPORT

22%

SIMILARITY INDEX

19%

INTERNET SOURCES

11%

PUBLICATIONS

13%

STUDENT PAPERS

PRIMARY SOURCES

1

www.ijareeie.com

Internet Source

4%

2

ijrise.org

Internet Source

4%

3

Kevin Wu, Brent Lagesse. "Detecting hidden webcams with delay-tolerant similarity of simultaneous observation", Pervasive and Mobile Computing, 2020

Publication

2%

4

www.ijert.org

Internet Source

2%

5

www.semanticscholar.org

Internet Source

2%

6

www.coursehero.com

Internet Source

2%

7

asiaccs2018.org

Internet Source

1%

8

Submitted to Govind Ballabh Pant Engineering College, Pauri-Garhwal

1%

- | | | |
|----|---|-----|
| 9 | www.i-scholar.in
Internet Source | 1% |
| 10 | Submitted to Madanapalle Institute of Technology and Science
Student Paper | 1% |
| 11 | mafiadoc.com
Internet Source | 1% |
| 12 | Bekir Sait Ciftler, Abdullah Kadri, Ismail Guvenc. "IoT Localization for Bistatic Passive UHF RFID Systems with 3D Radiation Pattern", IEEE Internet of Things Journal, 2017
Publication | 1% |
| 13 | Submitted to Universiti Teknologi MARA
Student Paper | 1% |
| 14 | ieeexplore.ieee.org
Internet Source | <1% |
| 15 | researchr.org
Internet Source | <1% |
| 16 | Sidharta Andalam, Partha S Roop, Alain Girault, Claus Traulsen. "A Predictable Framework for Safety-Critical Embedded Systems", IEEE Transactions on Computers, 2014
Publication | <1% |
| 17 | components101.com | |

Exclude quotes On

Exclude matches Off

Exclude bibliography On