



ECE504 Internet of Things

Project Final Report

Project Title: Smart Security for Office

(Group 3)

Faculty: [Anurag Lakhlani](#)

TAs: [Priyesh Chaturvedi](#), [Aanshi Patwari](#)

Group Details:

Name	Enrollment Number
Kandarp Sharda	AU1940112
Abhi Patel	AU1940117
Rushil Borad	AU1940179
Vraj Parikh	AU1940185

Contents

Introduction:	4
Motivation and Problem Definition:	5
Market Survey and Literature Review:	5
Block Diagram and Explanation:	8
Features Comparations for Different Platforms:	10
PROGRAM FLOW CHART:.....	14
List of the Sensors Used:	15
Flame Sensor.....	15
Temperature and Humidity Sensor (DTH11)	17
Smoke Sensor.....	18
PIR Motion Sensor	20
LDR light sensor	24
RFID (Radio-Frequency Identification) Sensor:	25
Lcd Display:.....	26
Buzzer:.....	28
Website Details:	30
Details Of Communication Protocols:	32
Wi-Fi	32
Bluetooth.....	32
Zigbee	33
Table for Comparison:.....	33
Hardware/ Circuit 1:.....	35
Office Security System (Secure Door System Using RFID):	35
Code For communicating with 1st Hardware:	36
Hardware/ Circuit 2:.....	38
Office Security System (Fire Detection, Motion Detection, Automatic Lighting, Temperature and Humidity).....	38
Code For communicating with 2 nd Hardware:	39
References:	43
Appendix A:.....	45

Appendix B:	53
Appendix C	54
Appendix D	54
Appendix E	55

Introduction:

In recent times, technology develops and evolves rapidly. As the contemporary era keeps on developing, a number of the system needs to be continuously evolving so as now not to be obsolete. Many years in the past, company safety devices cannot be controlled without human operation but cutting-edge technology discovery particularly on the internet of factors (IoT), it had given a brand-new face for the monitoring and protection system of corporate. With the aid of expertise, the simple concept of company protection using the internet of things, the concept and its software may be explored. Once this shows up, the development the use of the technology idea is viable. Numerous company protection devices have been developed where the conversation hyperlink is using Bluetooth, RFID, Android software, and brief message offerings (SMS). All of these have a one-of-a-kind technique of corporate security devices but serve a similar reason which is to monitor the safety and protection of the company. Corporate or office security using the Internet of Things focuses on safety, security, and luxury for the user to experience comfort at the office and also to protect private statistics. New eras and gadgets had made human existence greater relaxed and handy. Smart gadgets are successful to share records intelligently and it is ideal to our community because the internet might be completely inclusive. except that, the internet of factors had made the first-rate impact on everyday life by providing better safety, saving time, and monitoring health. According to API research in 2012, greater than 1.5 million domestic/company automation structures are hooked up in the United States. Nowadays company automation is more popular and speedier makes a better role in the market and offers a greater area for paintings and studies for engineers.

We are going to develop a system that will improve corporate security. The goal of this system is to create a way for people to have an improved arrival/attendance system. We'll use a Radio Frequency Identification (RFID) card to verify user identity and track system in and out times. And, to make further progress, we will build a smart fire alarm system, where the system will detect flames caught immediately or instantly, and will immediately notify management and send an emergency message. Smoke detection systems and Temperature and Humidity sensors will be

used even before a fire occurs. Aside from that, we plan to develop a system that would reduce light waste by detecting natural light.

Motivation and Problem Definition:

A basic description of any security system is found in its name. It is literally a means or method by which something is secured through a system of interworking components and devices. In this instance, we're talking about corporate/home security systems, which are networks of integrated electronic devices working together with a central control panel to protect against any harm. Ensuring the safety of your office and the safety of your employees is essential to providing a happy and comfortable working life. In addition, when considering an increasing number of corporate risks, it is extremely important that you keep your office safe from all forms of accidents. Ensuring corporate security needs a well-planned and proficient adoption of measures. So, the problem was all these sensors were available individually. We just took all the IoT sensors such as temperature, Ultra Sonic sensor, smoke, LDR light sensor, RFID sensor etc., and created a system that is powerful and efficient.

Market Survey and Literature Review:

The design and Implementation of Security for Smart Home based on GSM technology was discussed by Govinda et al. (2014) which provides two methods to implement home security using IoT. One is using web cameras such that whenever there is any motion detected by the camera, it sounds an alarm and sends a mail to the owner. This method of detecting the intrusion is quite good, albeit somewhat expensive due to the cost of the cameras involved in the process. The cameras need to be of good quality which means it should have a wide range and the picture quality should be high enough to detect movement. Also, if you go for movable cameras such as dome cameras, they will cost even more than fixed ones. SMS based system using GSM was proposed by Karri and Daniel (2005) propose to use internet services to send messages or alerts to the house owner instead of the conventional SMS. Jayashri and Arvind (2013) have implemented a fingerprint-based authentication system to unlock a door. This system helps users by only allowing the users whose fingerprints are authorized by the owner of the house. This system can also be

used to monitor who all have used the sensor to gain entry into the house. The system is coupled with a few more home protection features such as gas leakage and fire accidents. Although a good system, fingerprint sensors are expensive and complex (as they need increased sensor resolution) to integrate into an IoT setup. Some experts also argue that only relying on a fingerprint sensor is not wise as it is relatively easy to lift someone's fingerprints and replicate them, which is why it is always advised to use fingerprint scanners in two-factor authentication systems where an additional layer of security is available in the form of a PIN, passcode, voice recognition, etc. Some researchers proposed the idea of a robust IoT home security system where a fault in of one component in the system does not lead to the failure of the whole system. The idea of using multiple devices which may or may not be directly compatible with each other but can be made to work in such a way that they can replace an existing component of the system in case of a fault. In tandem to this, the model has the ability to use overlap between various devices which would result in preserving energy thus making the model more efficient. An example provided of the said model would use a temperature sensor, Wi-Fi module and a door sensor to replace a faulty camera. The authors are successful in an effort to demonstrate the given example. However, such systems are useful for people with energy efficiency in mind and for those who need a high degree of robustness with their security systems and are willing to expend more money than usual. Laser rays and LDR sensor are used to detect intrusion using their movement was proposed in 2016. The way the system works is that a laser is focused towards an LDR sensor and the moment that the contact of the laser to LDR sensor breaks, the alarm connected to the sensor goes off alerting the neighbors and sends a SMS to the owner. This system solves the problem of covering the places which are out of range from the fixed cameras but faces the same difficulties which are faced with systems consisting of GSM modules to send text messages, which is that the delivery of messages is dependent on network coverage. Also due to the nature of lasers being a straight beam, it can be avoided by intruders who know about the system and are capable of dodging the lasers, rendering the whole system useless. A novel way to design an electronic lock using Morse code and IoT technology. The authors claim that this as an original idea which has not been tried before and is the first of its kind "optical Morse code-based electronic locking system". This system uses LEDs "s (Light emitting diodes) as an encrypting medium to send signals. To make it more accessible to general public, the LED in smartphones has been used. On the receiver's side is a photosensitive resistor as well as a microcontroller such as Arduino processor which has the ability to decrypt the

optical signal after receiving them from the LED. Upon decoding the signal, it can then upload the current condition of the lock to a cloud from where the owner can monitor the system. The authors have experimented the system in real-time and it has proved to work under different illumination environments with all the functions working as they were intended to. The authors also claim to have an easy and user-friendly interface. The IoT system developed here works very well and can be used by anyone and is very convenient due to the use of mobile phones as LED, which also makes it a costly alternative.

Block Diagram and Explanation:

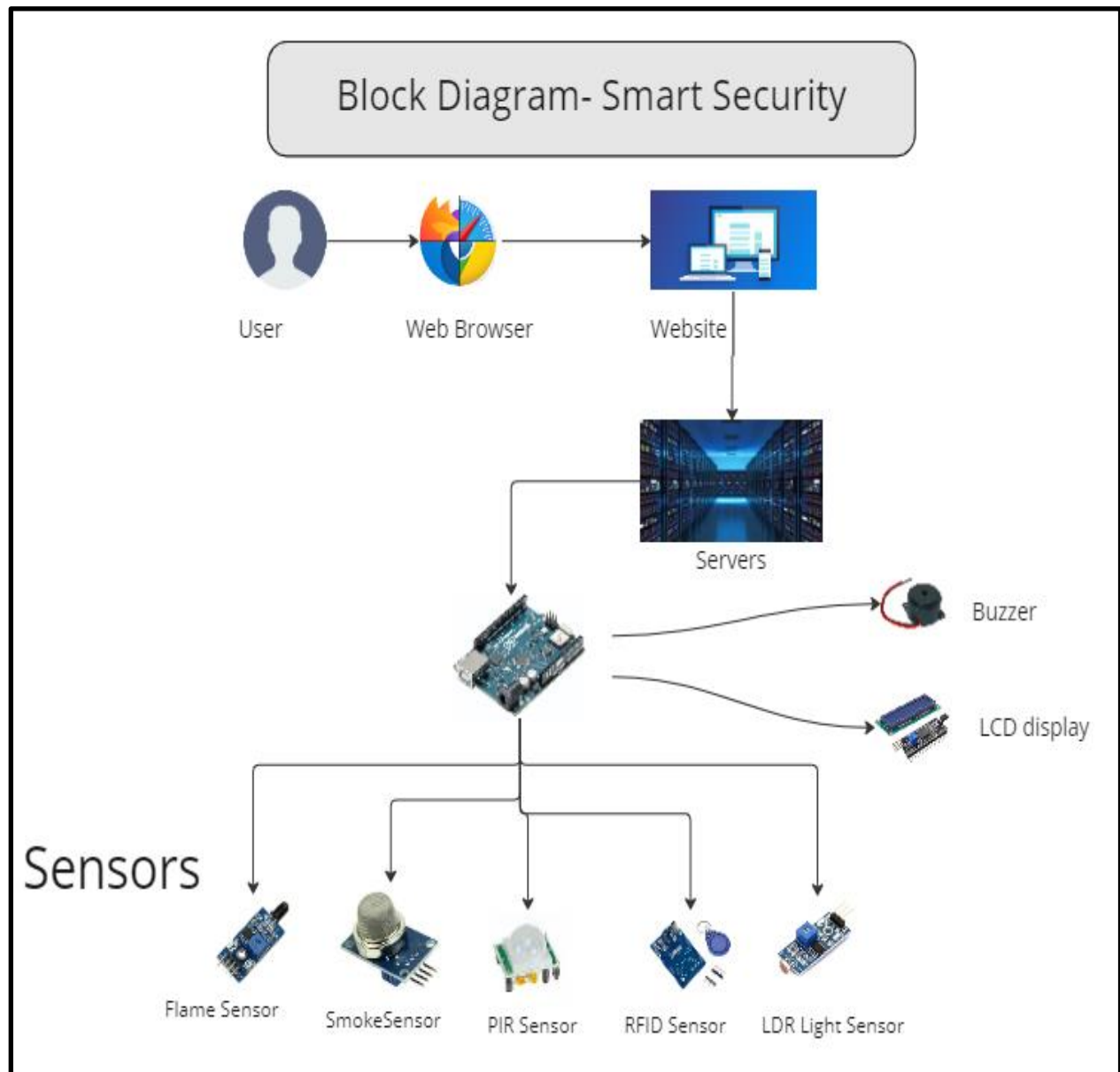




Figure 1: Block Diagram

This is a Corporate Security based web-based application. User must open any browser using computers. The user must enter his/her details to sign up. Right after the signup user needs to sign in via registered credentials. The following figure shows the overall design of this project. Afterward user is redirected to his/her dashboard where he/she can see the values of the sensors. He/she can also access the data for each sensor for example the user wants to see the temperature data and do so.

IoT and Arduino Based Corporate Security System uses four Sensors namely Temperature, Smoke, Flame, Light, Motion (PIR), and RFID sensors. Data from these sensors is then dispatched to the Arduino (Wi-Fi rev2), which has an inbuilt signal converter. Arduino then sends the data to the Wi-Fi network and creates TCP/IP connections and transmits data. The data, which is sensed by means of those sensors, is then dispatched to the IoT. An LDR-based light sensor is used to detect light and a PIR motion sensor is used to detect if there is any trespassing happening in particular areas like the server rooms. Temperature and Smoke sensors are used to detect fire. As soon as the fire is detected, the sign is sent to the microcontroller. The data is then transmitted to the website using an IoT module.

Features Comparisons for Different Platforms:

Table 1

<h2>Arduino</h2> 	<ul style="list-style-type: none">● Arduino is an open-source project. Both its software and hardware design are open source.● From Atmega Family● Requires less RAM (2kB)● 16 MHz (Arduino UNO),8-bit● Consumes about 200 MW of power● Arduino boards are programmable using C/C++ languages.● Arduino boards are cheaper.● Higher current drive strength● Arduino's logic level is 5V.● Traffic light countdown timer, Parking lot counter, Weighing machines, etc.
<h2>Raspberry Pi</h2> 	<ul style="list-style-type: none">● Both hardware and software of Raspberry Pi are closed source.● From ARM Family● Requires more RAM (more than 1GB)● Up to 1.5 GHz in Raspberry Pi 4 B,64-bit● Consumes about 700 MW of power● Raspberry Pi supports its own Linux-based operating system Raspberry Pi OS.● Raspberry Pi boards are expensive.● Lower current drive strength● Raspberry Pi's logic level is 3V.● Robot controller, Game servers, Stop motion cameras, etc

Beagle Bone



- Black is a low-cost, community-supported development platform for developers and hobbyists. Boot Linux in under 10 seconds and get started on development in less than 5 minutes with just a single USB cable.

Processor: AM335x 1GHz ARM® Cortex-A8

- ☐ 512MB DDR3 RAM
- ☐ 4GB 8-bit eMMC on-board flash storage
- ☐ 3D graphics accelerator
- ☐ NEON floating-point accelerator
- ☐ 2x PRU 32-bit microcontrollers

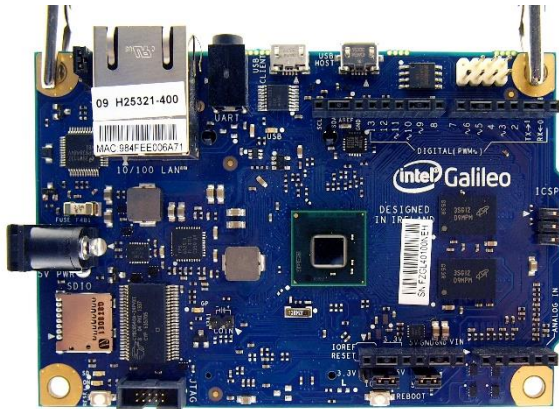
Connectivity

- ☐ USB client for power & communications
- ☐ USB host
- ☐ Ethernet
- ☐ HDMI
- ☐ 2x 46 pin headers

Software Compatibility

- ☐ Debian
- ☐ Android
- ☐ Ubuntu
- ☐ Cloud9 IDE on Node.js w/ Bone Script library

Intel Galileo

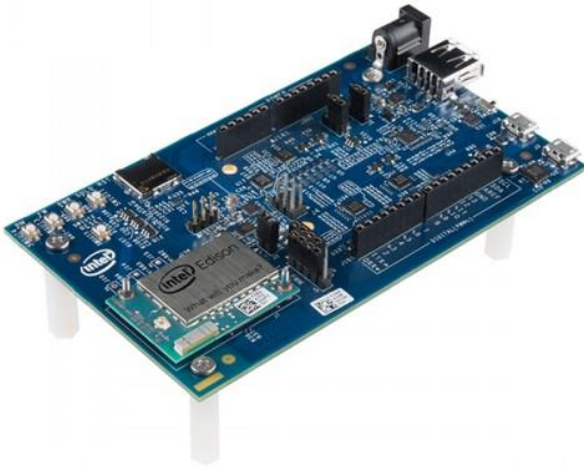


Galileo is a microcontroller board based on the Intel® Quark SoC X1000 Application Processor, a 32-bit Intel Pentium-class system on a chip.

400MHz 32-bit Intel® Pentium instruction set architecture (ISA)-compatible processor

- 16 KByte L1 cache
- 512 KBytes of on-die embedded SRAM
- Simple to program: Single thread, single core, constant speed
- ACPI compatible CPU sleep states supported on an integrated.
- 10-100 Ethernet connector
- Support up to 128 USB end point devices
- 8 MByte Legacy SPI Flash whose main purpose is to store the firmware (or bootloader) and the latest sketch. Between 256 KByte and 512 KByte is dedicated for sketch storage.
- The recommended output rating of the power adapter is 5V at up to 3A.
- Input Voltage (recommended) =5V
- Input Voltage (limits) =5V
- Digital I/O Pins =14 (of which 6 provide PWM output)
- Analog Input Pins =6
- Total DC Output Current on all I/O lines =- 80 mA
- DC Current for 3.3V Pin =800 mA
- DC Current for 5V Pin =800 mA

Intel® Edison



The Intel® Edison development platform is designed to lower the barriers to entry for a range of inventors, entrepreneurs, and consumer product designers to rapidly prototype and produce “Internet of Things” (IoT) and wearable computing products.

Supports Arduino Sketch, Linux, Wi-Fi, and Bluetooth. Board I/O: Compatible with Arduino Uno (except 4 PWM instead of 6 PWM):

- 20 digital input/output pins, including 4 pins as PWM outputs.
- 6 analog inputs.
- 1 UART (Rx/Tx). • 1 I2C. • 1 ICSP 6-pin header (SPI).
- Micro USB device connector OR (via mechanical switch) dedicated standard size USB host Type-A connector.
- Micro USB device (connected to UART). • SD card connector.
- DC power jack (7 to 15 VDC input).
- Provides seamless Device-to-Device and Device-to-Cloud communication.
- Ability to run rules on your data stream that trigger alerts based on advanced analytics.
- Foundational tools for collecting, storing, and processing data in the cloud.
- Free for limited and noncommercial use.

PROGRAM FLOW CHART:

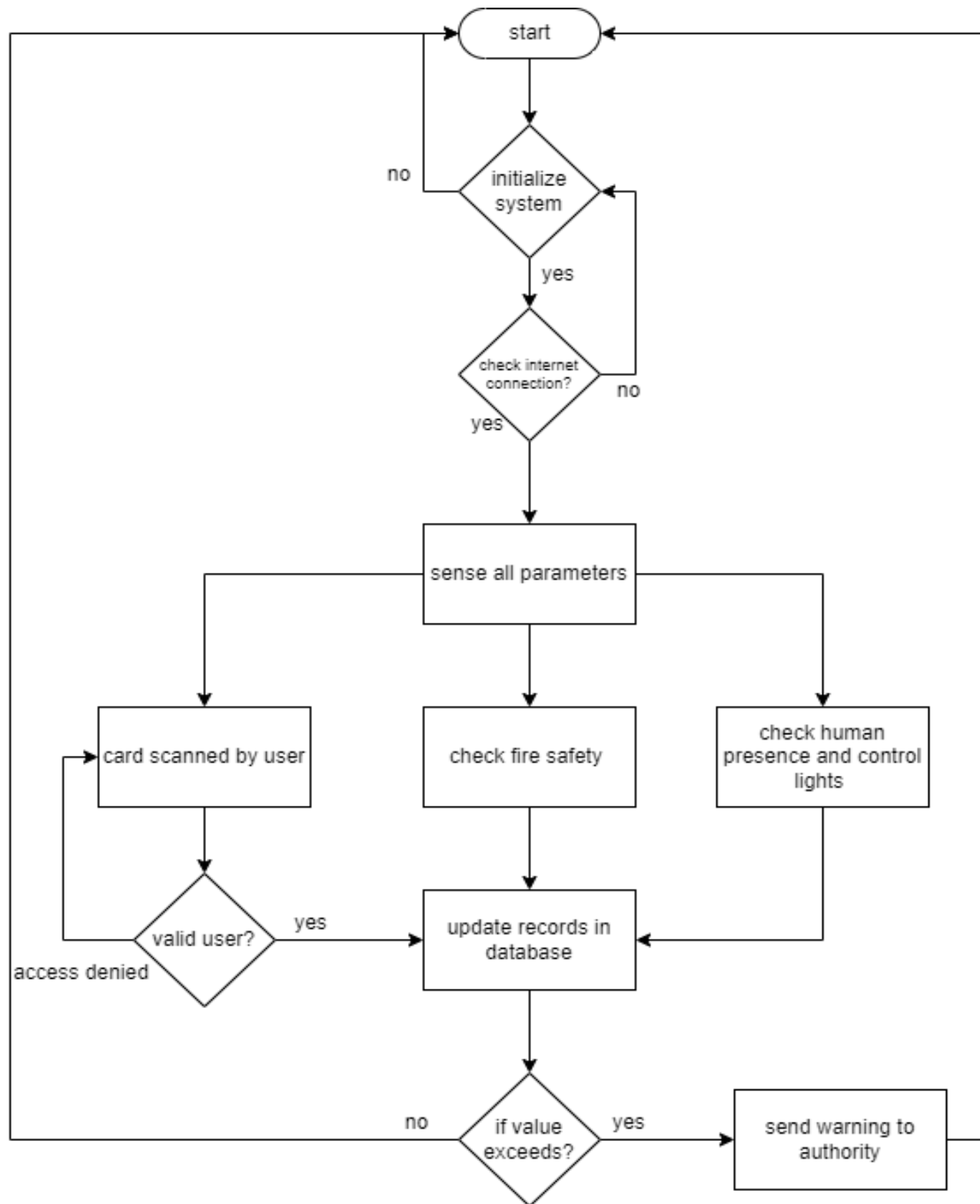


Figure 2: Flowchart of the program

List of the Sensors Used:

Flame Sensor

Working Principle:

The sensor is a short length of thin metallic rod that creates a small current of electricity in order to confirm there is fire burning within the furnace. As the gas valve opens to begin the combustion process, the current is sent out from the sensor in order to detect the presence of heat from a flame.

Pin Diagram:

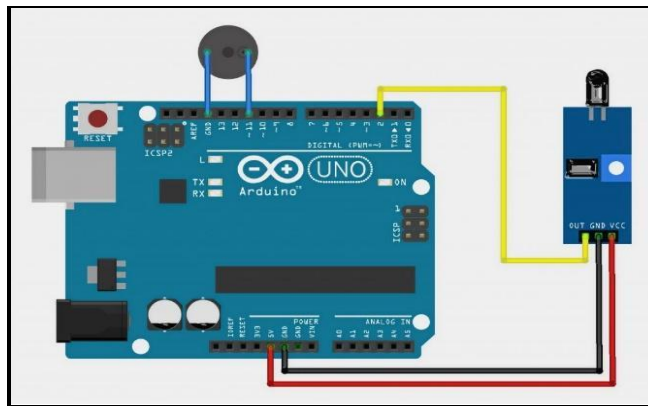


Figure 3 Arduino with Flame Sensor

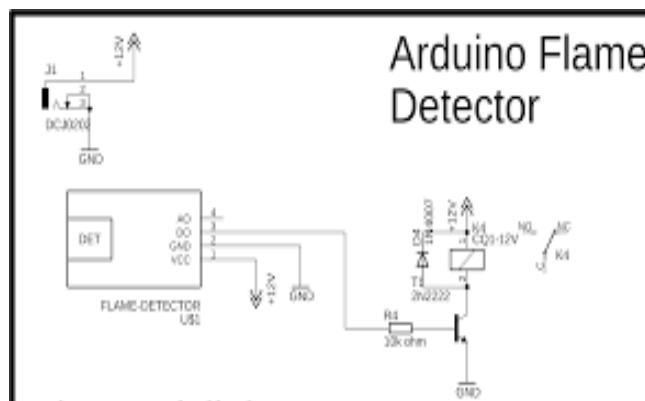


Figure 4 Circuit Diagram Flame Sensor

Interface with Arduino:

- 1) VCC -- 3.3V-5V voltage
- 2) GND -- GND

- 3) DO -- board digital output interface (0 and 1)
- 4) AO -- board analog output interface

Physical Dimensions:

The PCB size is 3cm X 1.6cm. Power indicator & digital switch o/p indicator. If the flame intensity is lighter within 0.8m then the flame test can be activated, if the flame intensity is high, then the detection of distance will be improved.

Details of power ratings: Operating voltage of this sensor is 3.3V to 5V. Analog voltage o/ps and digital switch o/ps.

Code to communicate with the sensors:

```
const int buzzerPin = 12;
const int flamePin = 11;
int Flame = HIGH;

void setup()
{
  pinMode(buzzerPin, OUTPUT);
  pinMode(flamePin, INPUT);
  Serial.begin(9600);
}

void loop()
{
  Flame = digitalRead(flamePin);
  if (Flame== LOW)
  {
    Serial.println("Fire!!!");
    digitalWrite(buzzerPin, HIGH);
  }
  else
  {
    Serial.println("No worries");
    digitalWrite(buzzerPin, LOW);
  }
}
```


Temperature and Humidity Sensor (DHT11)

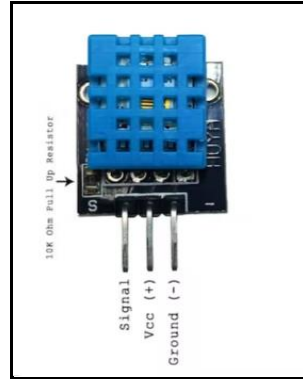


Figure 5 DTH 11 Sensor

Working Principle:

Temperature sensors work by measuring the voltage across the diode terminals. When the voltage increases, the temperature also increases, which is then followed by a voltage drop between the transistor terminals and the emitter (in a diode). The DHT-11 Digital Temperature and Humidity Sensor is a basic, ultra-low-cost digital temperature and humidity sensor. It uses a capacitive humidity sensor and a thermistor to measure the surrounding air and spits out a digital signal on the data pin (no analog input pins needed).

Pin Diagram:

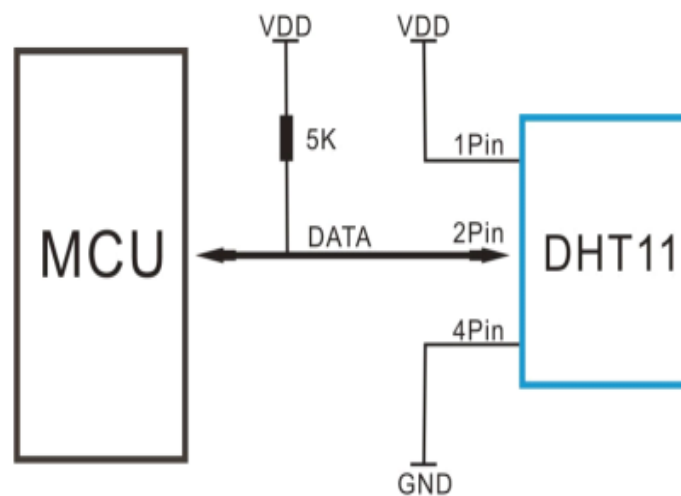


Figure 6 Circuit Diagram DTH 11 (temperature and humidity)

Interface with Arduino:

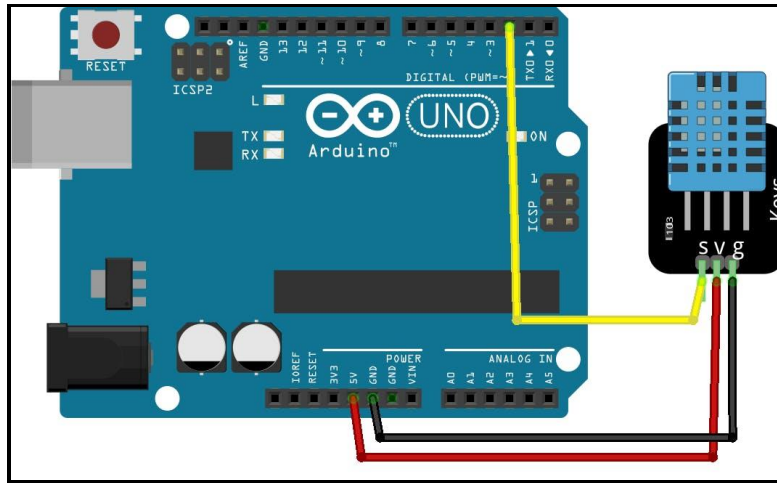


Figure 7 Interface with Arduino DTH11

Physical Dimensions and Details of power ratings:

- Low cost
- 3 to 5V power and I/O
- 2.5mA max current use during conversion (while requesting data)
- Good for 20-80% humidity readings with 5% accuracy
- Good for 0-50°C temperature readings $\pm 2^{\circ}\text{C}$ accuracy
- No more than 1 Hz sampling rate (once every second)
- Body size 15.5mm x 12mm x 5.5mm
- 4 pins with 0.1" spacing

Code to communicate with the sensors: (Below: Code for 2nd Hardware)

Smoke Sensor

Working Principle:

Ionization-type smoke alarms have a small amount of radioactive material between two electrically charged plates, which ionizes the air and causes current to flow between the plates. When smoke enters the chamber, it disrupts the flow of ions, thus reducing the flow of current and activating the alarm.

Pin Diagram:

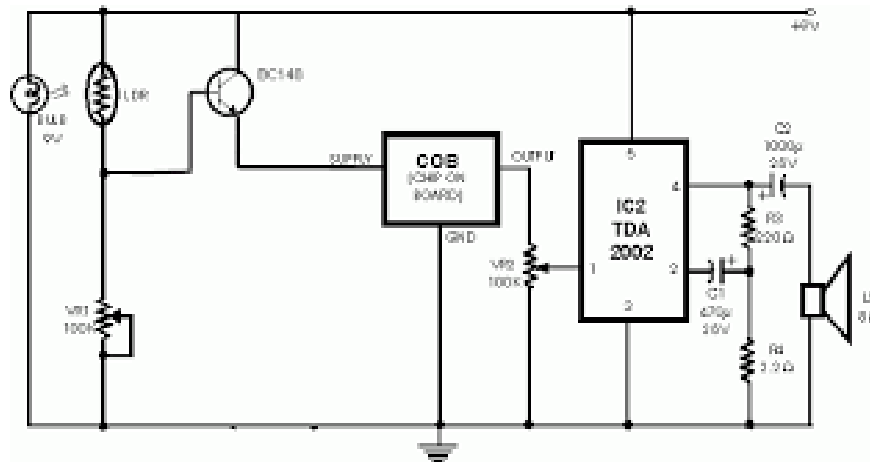


Figure 8 Circuit Diagram- Smoke Sensor

Interface with Arduino:

1. Connect the VCC pin of the sensor to the 5V of the Arduino.
2. Connect the GND of the sensor to the GND of the Arduino.
3. Connect the digital pin of the sensor D0 to any digital pin of the Arduino
4. Connect the analog pin of the sensor to the analog pin A0 of the Arduino.

Physical Dimensions:

Smoke detectors are usually housed in plastic enclosures, typically shaped like a disk about 150 millimeters (6 in) in diameter and 25 millimeters (1 in) thick, but shape and size vary.

Details of power ratings:

A 4.5-V to the 15-V power supply is recommended on VCC and VSLC. If a blue LED is used with the LED driver, a higher voltage may be required. Ensure the power supply can tolerate transient currents caused by the LED driver. A supply capable of 5

mA average current is generally sufficient. Ensure the power supply's rise time is less than 100 ms.

Code to communicate with the sensors: (Below: Code for 2nd Hardware)

PIR (Passive Infrared Sensor) Motion Sensor

PIR sensor is a small low-priced Passive infrared motion detector sensor. As the name suggests it doesn't emit radiation (unlike an Infrared (IR) sensor which emits infrared radiation) but it detects the changes in infrared radiation of the source. It's very facile to use and hence used in diverse applications.

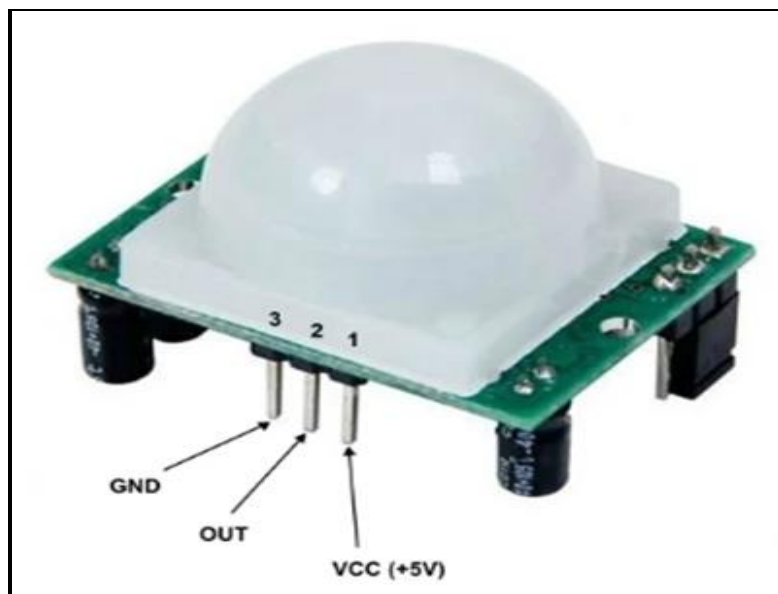


Figure 9 PIR (Passive Infrared Sensor)

Working Principle:

It works on the principle that whenever it detects a change in infrared radiation, it generates a digital output signal.

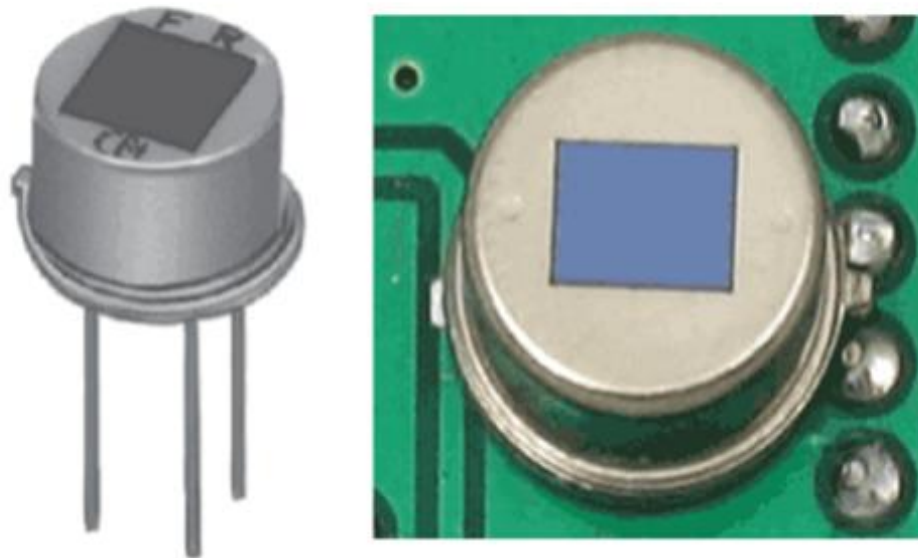


Figure 10 PIR (Passive Infrared Sensor)- Inside

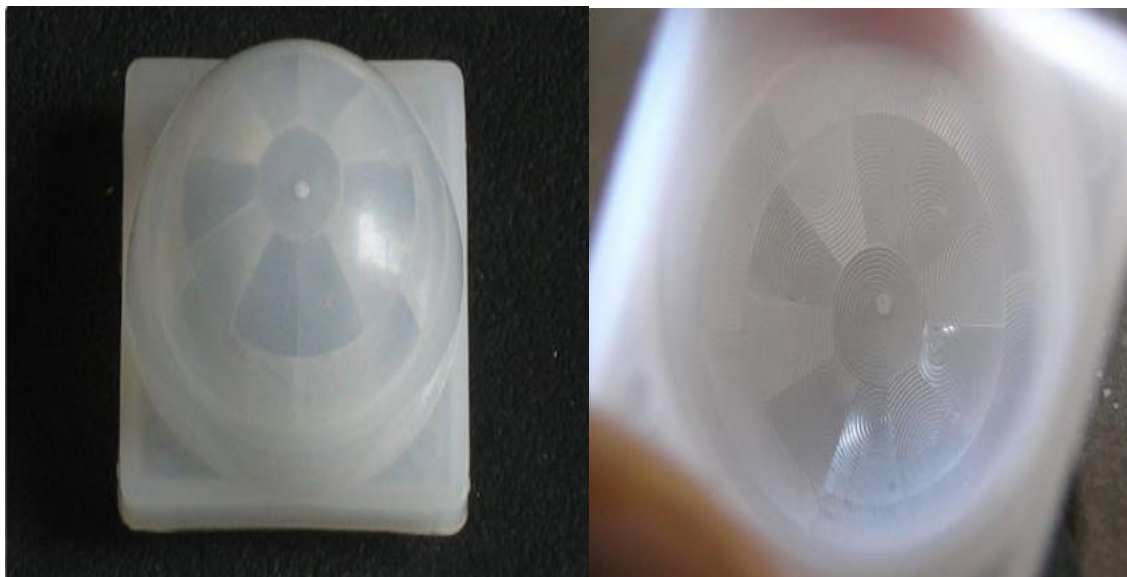


Figure 10 PIR (Passive Infrared Sensor)- Fresnel lens

PIR sensor consists of a Fresnel lens, pyroelectric material (metal can and a rectangular crystal). A Fresnel lens which is made of high-density polythene concentrates the incoming infrared radiations so that they fall on the pyroelectric material. Metal can help to make the sensor more immune to temperature, humidity, and noise. Pyroelectric material detects the changes in infrared radiation and generates an output signal.

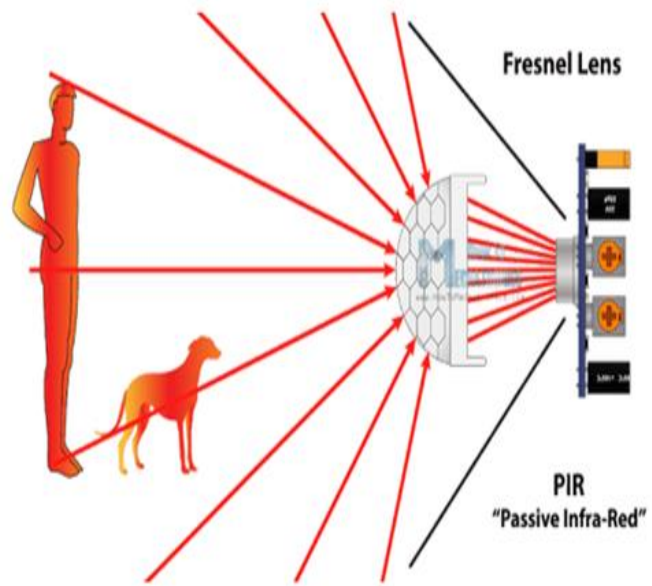
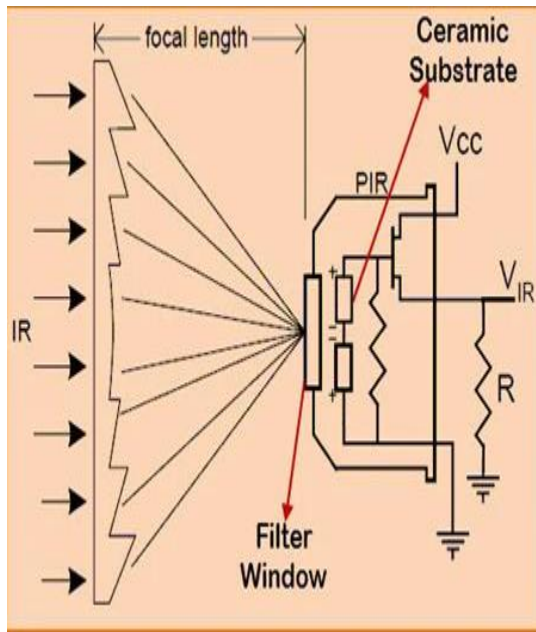


Figure 11 PIR motion detection

It is made up of 2 slots of special material sensitive to IR. When a person comes in the range of the sensor, the first slot creates a positive differential voltage and when the person leaves the second slot creates a negative differential voltage. These changes are detected.

Interface with Arduino:

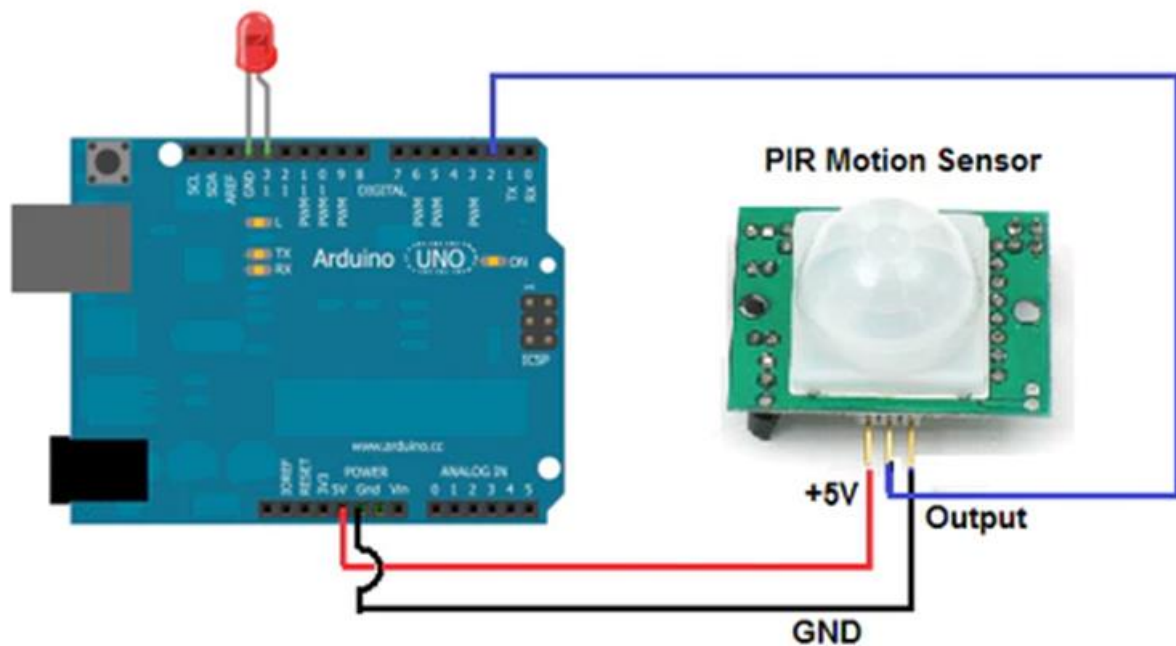


Figure 12 PIR interface with arduino

As shown in the image, Vcc goes to 5V, Gnd goes to Gnd, and Output is connected to digital input pin 2 of Arduino. Whenever there is motion detected output pin of the PIR motion sensor goes high. So based on this result we can read the digital input pin 2 of the Arduino and take the action such as glowing LED.

We can put the PIR sensor in two modes as shown in the above image the jumper is used to connect it in H mode repeatable trigger and L mode non-repeatable trigger. In retriggering or H mode, the LED stays on while the person is moving in the PIR sensor range. Whereas in non-retriggering or L mode, LED blinks or turns on and off every 1 second when a person is moving in the PIR range.

Also, there are two potentiometers (Yellow Color) of 1M ohm resistance available for adjusting sensitivity and time delay.

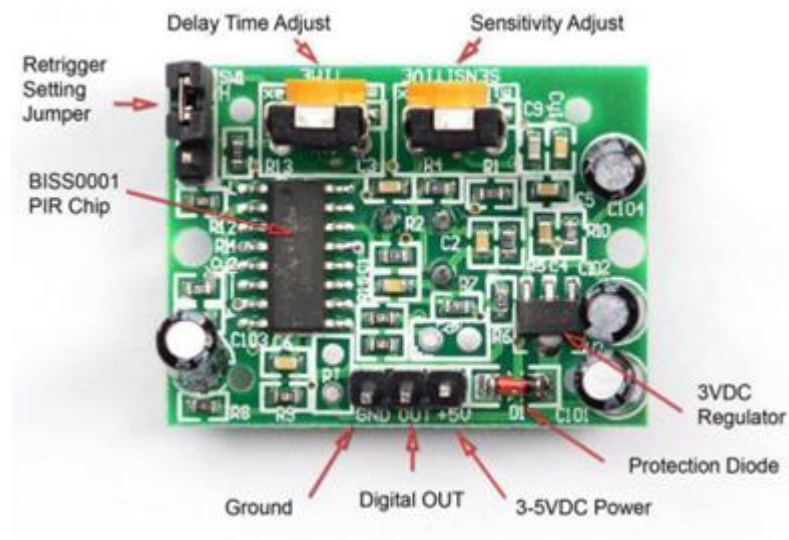


Figure 13 PIR sensitivity

The sensitivity pot is used to adjust the distance from 2-5m and the time delay pot is used to adjust the time for which the output pin should remain high when the motion is detected.

Range: We can set the range from 5 seconds to 5 minutes. We can turn it fully anti-clock so that we can decide the time delay from the Arduino.

Physical Dimensions and Details of power ratings: [Link](#)

Article name	Passive infrared motion detector
Sensor	Fresnel-Lens
Range	Up to 12 m, adjustable in 4 steps
Signal bandwidth	0.4...10Hz
Opening angle	Horizontal $\pm 50^\circ$, vertical $\pm 30^\circ$
Digital output	Open Collector max. 5 V, 20 mA
Analog output	0V...Vcc -0,5V
Application temperature	-20...+60 °C
Environmental conditions	Ambient humidity: 0...90% RH, Dew not permitted
Power supply	3...5 V DC
Operating current	Calm, output „H“ 40 μ A / Activ output „L“ 400 μ A
Dimensions	(LxWxH) 25 x 25 x 26 mm
Weight	0.022 kg

Code to communicate with the sensors: (Below: Code for 2nd Hardware)

LDR light sensor

Working Principle:

The working principle of an LDR is photoconductivity, which is nothing but an optical phenomenon. When the light is absorbed by the material then the conductivity of the material enhances. When the light falls on the LDR, then the electrons in the valence band of the material are eager to the conduction band.

Pin Diagram:

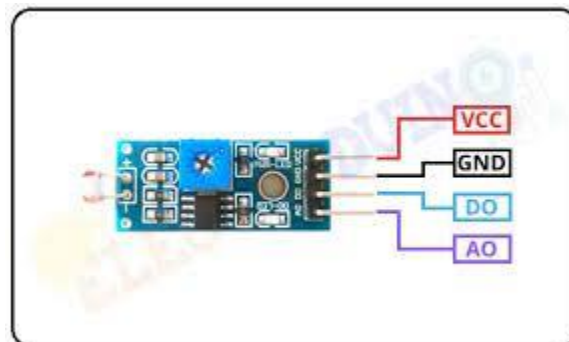


Figure 14 LDR Light Sensor Pin diagram

Interface with Arduino:

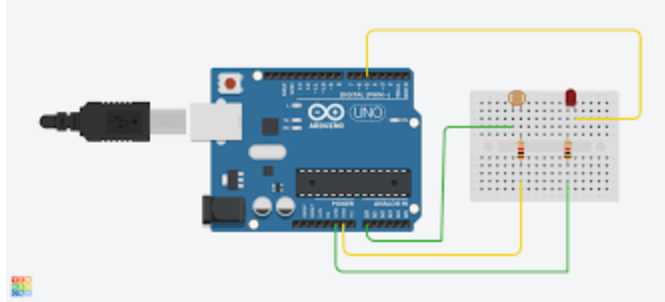


Figure 14 LDR Light Sensor Interface with Arduino

Physical Dimensions:

Light Dependent Resistor is of 5mm Diameter

Details of power ratings:

LDR has multiple options of power depending on the usage i.e. 1 Mohm, 250 mW, 320 V.

Code to communicate with the sensor: (Below: Code for 2nd Hardware)

RFID (Radio-Frequency Identification) Sensor:

Working Principle:

The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data. The transponder is in the RFID tag itself.

Pin Diagram:

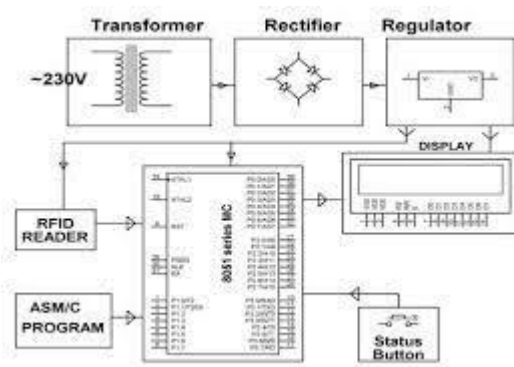


Figure 15 RFID (Radio-Frequency Identification) Sensor- pin diagram

Interface with Arduino:

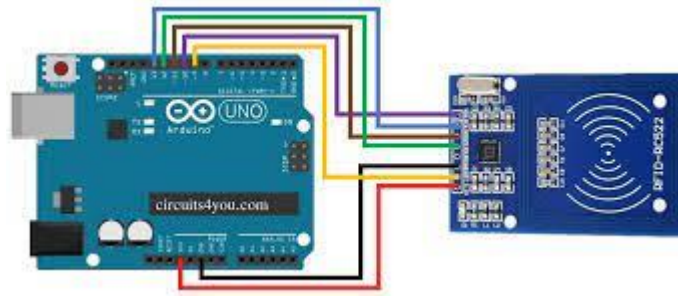


Figure 16 RFID interface with arduino

Physical Dimensions:

RFID card varies from 0.5mm-1mm depend on the different production processes

Details of power ratings:

RFID readers have a minimum transmit power of 0 or 10 dBm and a maximum transmit power between 30 and 33 dBm.

Code to communicate with the sensors: (RFID, LCD, Buzzer system combined-Hardware 1)

Lcd Display:

Working Principle:

The LCDs have a parallel interface, meaning that the microcontroller has to manipulate several interface pins at once to control the display. The interface consists of the following pins: A register select (RS) pin that controls where in the LCD's memory you're writing data to.

Pin Diagram:

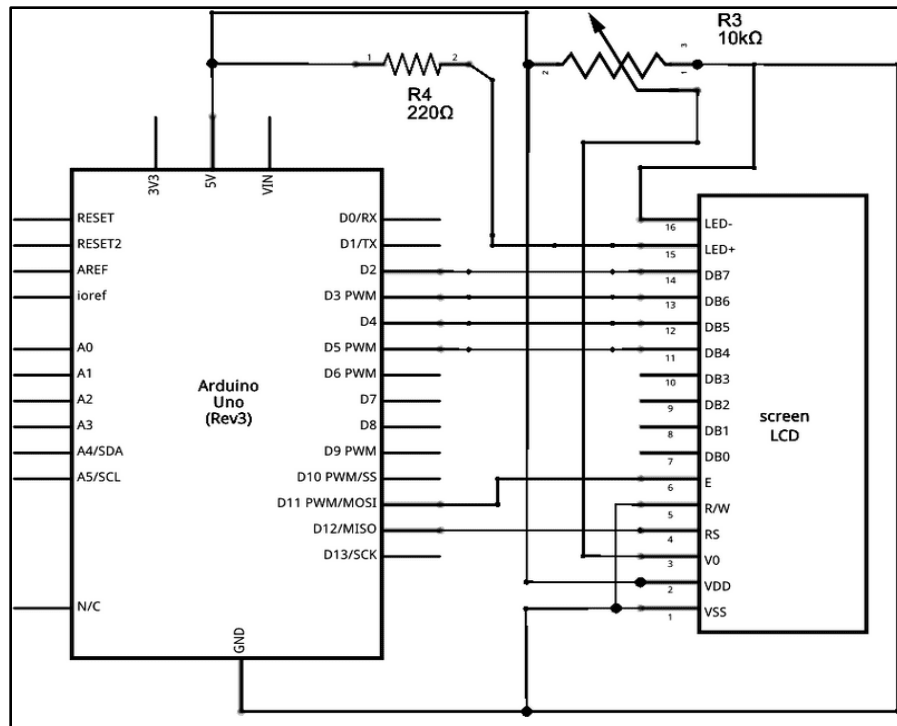


Figure 17 LCD display circuit diagram

Interface with Arduino:

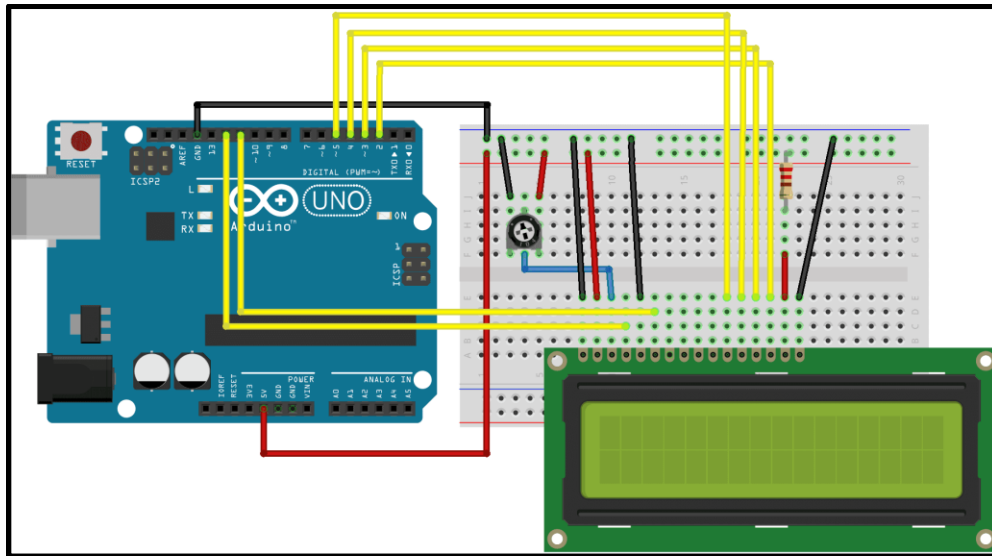


Figure 18 LCD display interface with arduino

Physical Dimensions:

These modules have a 122x44 mm outer dimension with 99x24 mm viewing area on the display. The 162M 16x2 LCD displays are available in STN or FSTN LCD modes with or without an LED backlight.

Details of power ratings:

The recommended voltage range for the VIN pin is 7 to 12V (absolute maximum of 20V); the range for the VCC pin is 4.5 to 5.5V (5V typical).

Code to communicate with the sensors: (RFID, LCD, Buzzer system combined-Hardware 1)

Buzzer:

Working Principle:

The flexible ferromagnetic disk is attracted to the coil when the magnetic field is activated, then returns to rest when the magnetic field is off. By oscillating the signal through the coil, the buzzer produces a fluctuating magnetic field, which vibrates the disk. This movement makes the buzzer sound.

Pin Diagram:

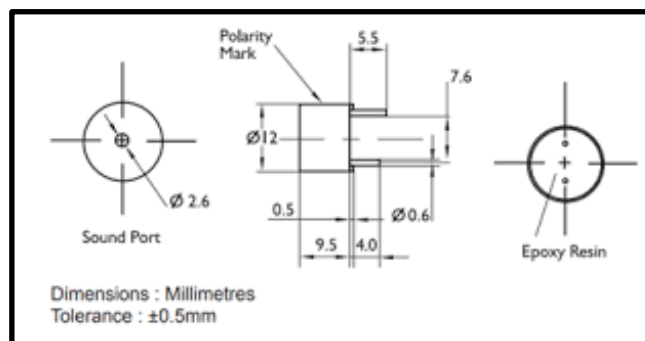


Figure 19 Buzzer Pin diagram

Interface with Arduino:

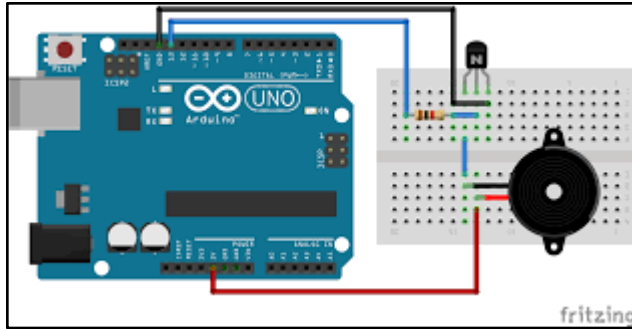


Figure 20 Buzzer Interface with arduino

Physical Dimensions:

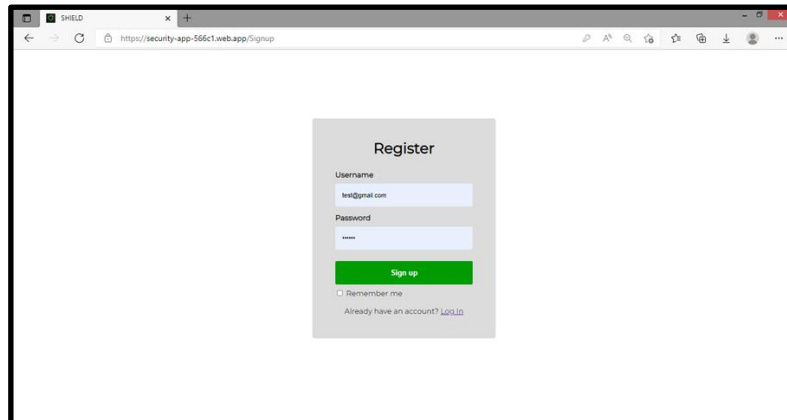
It is about 12mm.

Details of power ratings:

Magnetic buzzers are essentially current-driven devices, typically requiring more than 20mA to operate. The applied voltage can be as low as 1.5V or up to about 12V.

Code to communicate with the sensors: (RFID, LCD, Buzzer system combined-Hardware 1)

Website Details:



A screenshot of a web browser showing the 'Register' page of a security application. The page has a white background with a central grey box containing the registration form. The form includes fields for 'Username' (with 'test@gmail.com' entered) and 'Password' (with masked characters). Below the fields is a green 'Sign up' button. At the bottom of the form, there is a checkbox for 'Remember me' and a link for 'Already have an account? Log In'.

Register

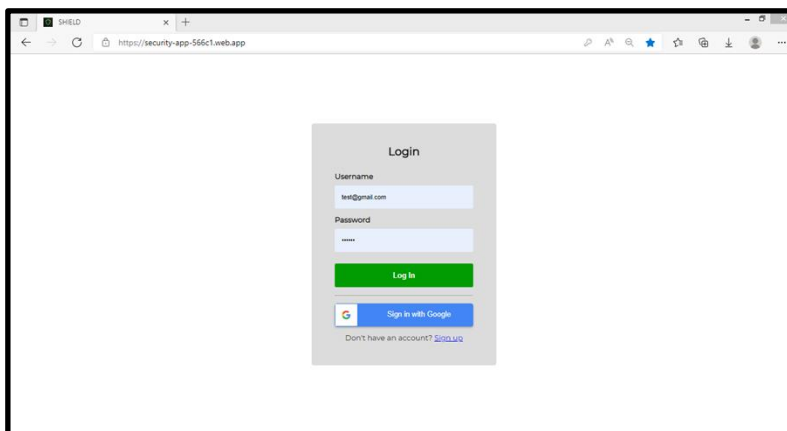
Username
test@gmail.com

Password
.....

Sign up

☐ Remember me

Already have an account? [Log In](#)




A screenshot of a web browser showing the 'Login' page of the same security application. The page features a central grey box with the login form. It includes 'Username' and 'Password' fields, both containing masked text. A green 'Log In' button is positioned below the fields. Below the button is a 'Sign in with Google' button and a link for 'Don't have an account? Register'.

Login

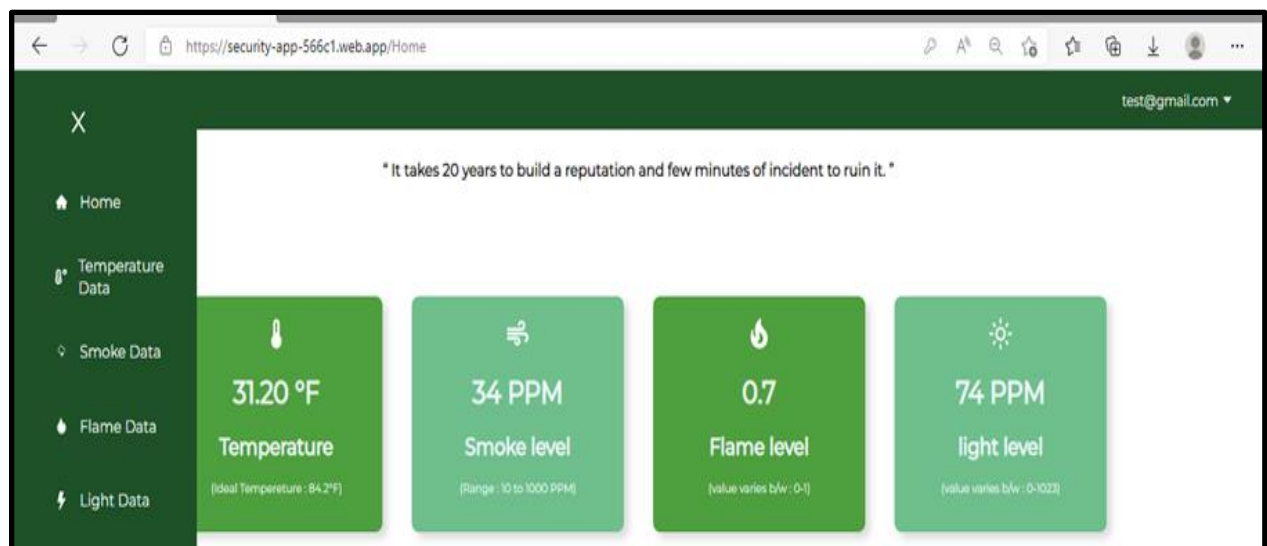
Username
test@gmail.com

Password
.....

Log In

 Sign in with Google

Don't have an account? [Register](#)




urity-app-566c1.web.app

Login

Username

Password

Log In

 Sign in with Google

Don't have an account? [Sign up](#)

urity-app-566c1.web.app

Register

Username

Password

Sign up

☐ Remember me

Already have an account? [Log In](#)

urity-app-566c1.web.app

X

il.com

reputation
t to ruin it."

Home

Temperature
Data

Smoke Data

Flame Data

Light Data

Details Of Communication Protocols:

IoT (Internet of Things) has power to make the complete system automatic. There are various **IOT communication protocols** which are used in communication between devices in the IoT network. **The wireless communication protocol** is a standard set of rules with reference to which various electronic devices communicate with each other wirelessly.

Since there are many wireless communication protocols available to use for your product, it becomes difficult for the product designers to choose the correct one but once the scope of IoT application is decided it would become easier to select the right protocol. Here we are briefly explaining **protocols used in IOT** with their features and applications.

Wi-Fi

Wi-Fi (Wireless Fidelity) is the most popular **IOT communication protocols** for wireless local area network (WLAN) that utilizes the IEEE 802.11 standard through 2.4 GHz UHF and 5 GHz ISM frequencies. Wi-Fi provides Internet access to devices that are within the range of about 20 - 40 meters from the source. It has a data rate up to 600 Mbps maximum, depending on channel frequency used and the number of antennas. In embedded systems, ESP series controllers from Espressif are popular for building IoT based Applications. **ESP32** and **ESP8266** are the most commonly use Wi-Fi modules for embedded applications.

In terms of using the Wi-Fi protocol for IOT, there are some pros & cons to be considered. The infrastructure or device cost for Wi-Fi is low & deployment is easy but the power consumption is high and the Wi-Fi range is quite moderate. So, the Wi-Fi may not be the best choice for all types of IOT applications but it can be used for applications like Home Automation.

There are many development boards available that allow people to build IOT applications using Wi-Fi. The most popular ones are the Raspberry Pi and Node MCU. These boards allow people to build IOT prototypes and also can be used for small real-time applications. Likewise, is the Marvell Avastar 88W8997 SoC, which follows the Wi-Fi's IEEE 802.11n standard. The chip has applications like wearables, wireless audio & smart home.

Bluetooth

Bluetooth is a technology used for exchanging data wirelessly over short distances and preferred over various **IOT network protocols**.

It uses short-wavelength UHF radio waves of frequency ranging from 2.4 to 2.485 GHz in the ISM band. The Bluetooth technology has 3 different versions based on its applications:

Bluetooth: The Bluetooth that is used in devices for communication has many applications in IOT/M2M devices nowadays. It is a technology using which two devices can communicate and share data wirelessly. It operates at 2.4GHz ISM band and the data is split in packets before sending and then is shared using any one of the designated 79 channels operating at 1 MHz of bandwidth.

BLE (Bluetooth 4.0, Bluetooth Low Energy): The BLE has a single main difference from Bluetooth that it consumes low power. With that, it makes the product of low cost & more long-lasting than Bluetooth.

iBeacon: It is a simplified communication technique used by Apple and is completely based on Bluetooth technology. The Bluetooth 4.0 transmits an ID called UUID for each user and makes it each to communicate between iPhone users.

Bluetooth has many applications, such as in telephones, tablets, media players, robotics systems, etc. The range of Bluetooth technology is between 50 – 150 meters and the data are being shared at a maximum data rate of 1 Mbps.

After launching the BLE protocol, there have been many new applications developed using Bluetooth in the field of IOT. They fall under the category of low-cost consumer products and Smart-Building applications.

Zigbee

ZigBee is another **IOT wireless protocols** has features similar to the Bluetooth technology. But it follows the IEEE 802.15.4 standard and is a high-level communication protocol.

It has some advantages similar to Bluetooth i.e., low-power consumption, robustness, high security, and high scalability.

Zigbee offers a range of about 10 – 100 meters maximum and data rate to transfer data between communicated devices is around 250 Kbps. It has a large number of applications in technologies like M2M & IOT.

Having limitations in regards to data rate, range, and power consumption, Zigbee is only appropriate for Small-Scale Wireless applications.

Though having some limitations, **it provides a 128-bit AES encryption and is giving a big hand in making secure communication for home automation & small Industrial applications.** Zigbee too has its DIY module named **XBee & XBee Pro** which can be interfaced with Arduino or Raspberry Pi boards to make simple projects or application prototypes.

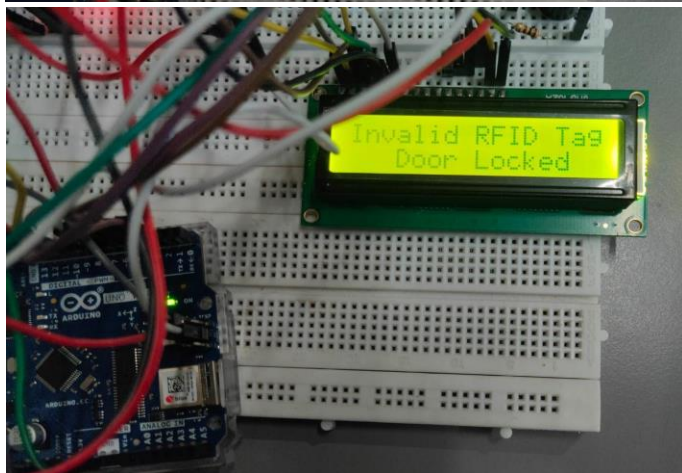
Table for Comparison:

Table 2

Parameters	Bluetooth (Low Energy)	Wi-fi	Zigbee
IEEE	IEEE 802.15.1	IEEE 802.11n	IEEE 802.15.4
Data Rate	1-3 Mbps	1gbps or more	20kbps,40kbps,250kbps
Frequency band	2.4GHz	2.4GHz and 5GHz	2.4GHz
Range	10 meters	190 m	100m
Risk of Data Collision	High		Medium
Maximum Nodes	8	2007	>65,000
Power Efficient	Acceptable to Good	Varies	Excellent
Applications	To replace wiring in handheld devices	The main connectivity resource for home, work, retail and more.	Mesh capability creates greeter signal reliability
Advantages	<ul style="list-style-type: none"> • Convenience • Cost Effective • Connection with various Windows, Android and iOS devices. 	<ul style="list-style-type: none"> • Widely used wireless connectivity • Connectivity to Android and iOS devices. 	Reliable, Low Power, cost effective, “Assemble and Forget”
Drawbacks	Short Range	Not always reliable, Consumer high Power	Not mainstream for connection to smartphones etc.
Markets	Mainly for Portables. Widely adopted in consumer Markets, retails	Ubiquitous, widely adopted in nearly every market. Replaces cables in work areas or homes.	Better known in Industrial markets, smart homes, smart lighting.
Security	medium	Low	Very High

Hardware/ Circuit 1:

Office Security System (Secure Door System Using RFID):



Code For communicating with 1st Hardware:

```
#include <SPI.h>
#include <MFRC522.h>
#include <LiquidCrystal.h>
#define BUZZER 7
#define SS_PIN 10
#define RST_PIN 9
MFRC522 mfrc522(SS_PIN, RST_PIN); // Create MFRC522 instance.
const int rs = 12, en = 11, d4 = 5, d5 = 4, d6 = 3, d7 = 2;
LiquidCrystal lcd(rs, en, d4, d5, d6, d7);

void setup()
{
  Serial.begin(9600); // Initiate a serial communication
  SPI.begin();        // Initiate SPI bus
  mfrc522.PCD_Init(); // Initiate MFRC522
  Serial.println("Approximate your card to the reader...");
  Serial.println();
  // set up the LCD's number of columns and rows:
  lcd.begin(16, 2);
  //lcd.begin();
  //lcd.backlight();
  lcd.clear();
  lcd.setCursor(0,0); // column, row
  lcd.print(" Scan Your RFID ");
  lcd.setCursor(0,1); // column, row
  lcd.print("  Door Locked  ");
  pinMode(BUZZER, OUTPUT);
  noTone(BUZZER);
}

void loop()
{
  lcd.clear();
  lcd.setCursor(0,0); // column, row
  lcd.print(" Scan Your RFID ");
  lcd.setCursor(0,1); // column, row
  lcd.print("  Door Locked  ");
  // Look for new cards
  if ( ! mfrc522.PICC_IsNewCardPresent())
```

```

{
    return;
}
// Select one of the cards
if ( ! mfrc522.PICC_ReadCardSerial())
{
    return;
}
//Show UID on serial monitor
Serial.print("UID tag :");
String content= "";
byte letter;
for (byte i = 0; i < mfrc522.uid.size; i++)
{
    Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
    Serial.print(mfrc522.uid.uidByte[i], HEX);
    content.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
    content.concat(String(mfrc522.uid.uidByte[i], HEX));
}
Serial.println();
Serial.print("Message : ");
content.toUpperCase();

if (content.substring(1) == "D9 B4 E5 B3" || content.substring(1) == "63 4E D3
16" ) //change here the UID of the card/cards that you want to give access
{
    Serial.println("Access Granted ");
    Serial.println();
    lcd.setCursor(0,0);
    lcd.print(" Access Granted ");
    delay(500);
    lcd.setCursor(0,1); // column, row
    lcd.print(" Door Un-Locked ");
    tone(BUZZER, 2000);
    delay(100);
    noTone(BUZZER);
    delay(50);
    tone(BUZZER, 2000);
    delay(100);
    noTone(BUZZER);
}

else {

```

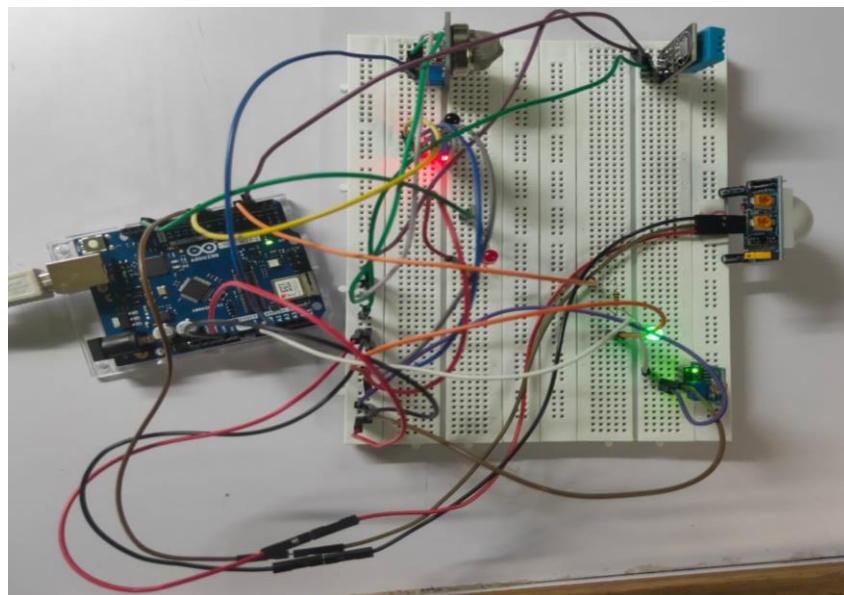
```

    lcd.setCursor(0,0); // column, row
    lcd.print("Invalid RFID Tag");
    lcd.setCursor(0,1);
    lcd.print(" Access Denied ");
    Serial.println(" Access denied");
    tone(BUZZER, 1500);
    delay(500);
    noTone(BUZZER);
    delay(100);
    tone(BUZZER, 1500);
    delay(500);
    noTone(BUZZER);
    delay(100);
    tone(BUZZER, 1500);
    delay(500);
    noTone(BUZZER);
    lcd.setCursor(0,1); // column, row
    lcd.print("  Door Locked  ");
  }
  delay(4000);
}

```

Hardware/ Circuit 2:

Office Security System (Fire Detection, Motion Detection, Automatic Lighting, Temperature and Humidity)



Code For communicating with 2nd Hardware:

```
int val = 0 ;
int LED = 13; // Use the onboard Uno LED
int isFlamePin = 7; // This is our input pin
int isFlame = HIGH;
#include "DHT.h"
#define DHTPIN 2
#define MQ2pin (1)
float sensorValue;
int sensor = 8;

#define DHTTYPE DHT11
DHT dht(DHTPIN, DHTTYPE);
void setup()
{
    Serial.begin(9600); // sensor buart rate
    pinMode(3,OUTPUT); // LED PIN
    pinMode(LED, OUTPUT); // put onboard LED as output
    pinMode(isFlamePin, INPUT); //flame sensor should be input as it is giving data
    pinMode(sensor, INPUT);
    dht.begin();
}
void loop()
{
    sensorValue = analogRead(MQ2pin);
    int PIRSensor = digitalRead(sensor); // read sensor value
    if (PIRSensor == HIGH) {

        Serial.println("Motion detected");
    }
    else{
        Serial.println("Motion stopped!");
    }

    float h = dht.readHumidity();
    // Read temperature as Celsius (the default)
    float t = dht.readTemperature();
    // Read temperature as Fahrenheit (isFahrenheit = true)
    float f = dht.readTemperature(true);

    // Check if any reads failed and exit early (to try again).
    if (isnan(h) || isnan(t) || isnan(f)) {
```

```

    Serial.println(F("Failed to read from DHT sensor!"));
    return;
}

isFlame = digitalRead(isFlamePin);
val = analogRead(A0); // LDR Sensor output pin connected

int newval = val/10;

analogWrite(3 , newval);
if (isFlame== LOW) //if it is low
{
    Serial.println("FLAME, FLAME, FLAME"); //Print Flame Flame
    digitalWrite(LED, HIGH); //LED on
}
else //if not
{
    Serial.println("no flame"); //print no flame
    //off the LED

    digitalWrite(LED, LOW);
}
Serial.print("Smoke sensor value :");
Serial.println(sensorValue);
if(sensorValue > 200)
{
    Serial.print(" | Smoke detected!");
}

Serial.println("");

Serial.print(F("Humidity: "));
Serial.println(h);
Serial.print(F("% Temperature: "));
Serial.println(t);
Serial.print(F("°C "));
Serial.println(f);
delay(1000);
}

```


Conclusion:

This Office/corporate security system is made of cost-effective materials with and can be used to protect the entire office building with reasonably low cost. This system can be adjusted without problems at any home or workplace space. The office security system was tested several times, effectively and accurately measured a variety of useful features in everyday life for most of the sensors. Lastly, this office security system can also be used via Bluetooth without major changes in its design but still are able to control a variety of office objects. Hence, this system is scalable and flexible; we have designed an Office security system using Arduino and with the help of IOT devices and sensors, which is practical, portable, cost-effective and highly efficient as well. Such systems are much needed for security purposes so the provided system can be considered useful and effective in view of the above features it offers.

Project Time line:

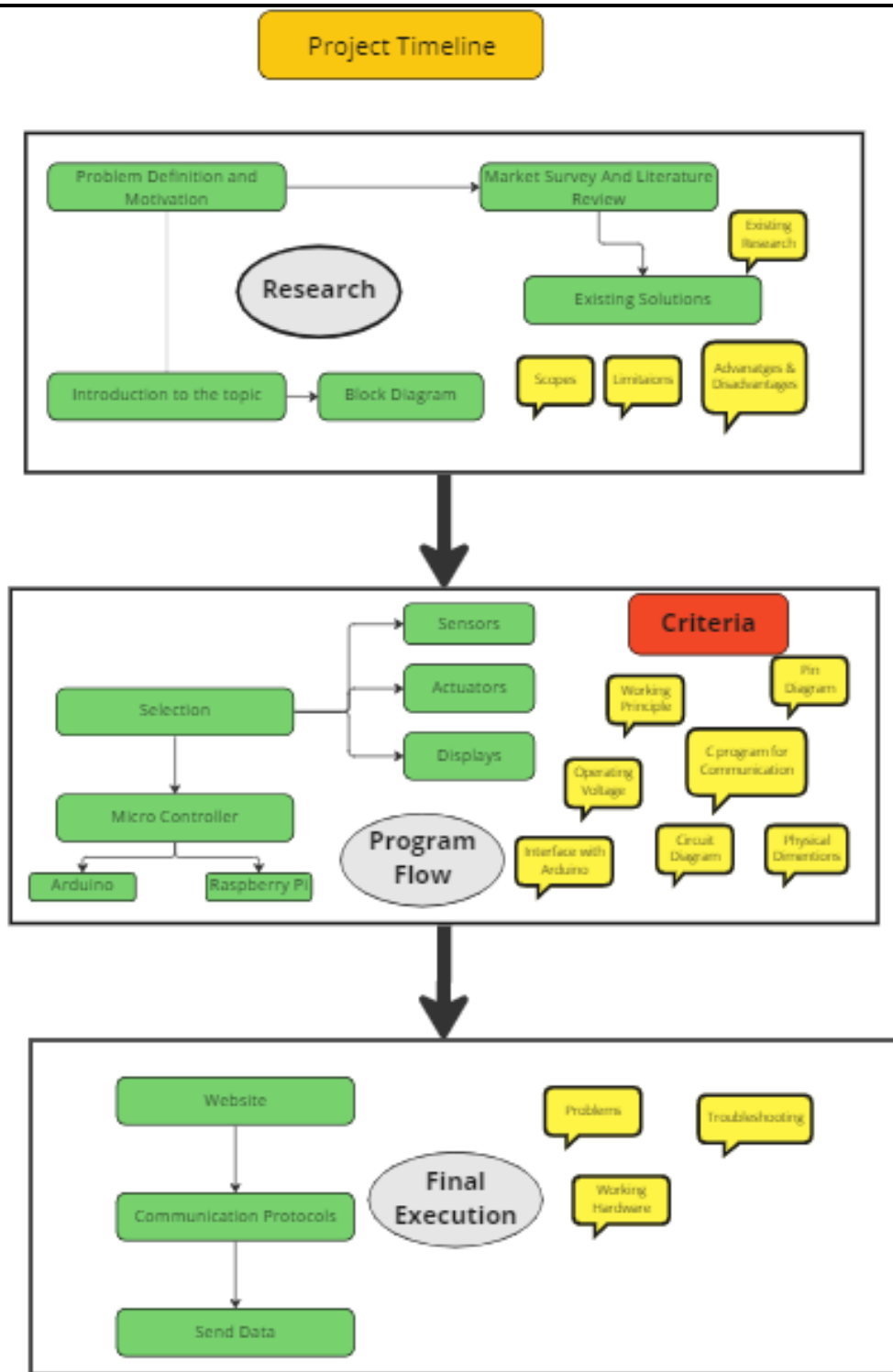


Figure 21 Project Timeline

References:

- Soumya, S., Chavali, M., Gupta, S., & Rao, N. (2016). Internet of Things based Home Automation System. IEEE, 848-850.
- Mohd Nor Azmi, M., Vellasami, L., Zainal, A., Mohammed, F., Mohd Daud, N., Vejasegaran, R., . Ku Azir, K. P. (2016). Home Automation System with Android Application. 299-302.
- Govinda K and Sai Krishna Prasad K and Sai ram susheel 2014 Intrusion detection system for smart home using laser rays International Journal for Scientific Research & Development (IJSRD) 2 176-78
- Karri V and Daniel Lim J S 2005 Method and Device to Communicate via SMS after a Security Intrusion 1st International Conf. on Sensing Technology Palmerston North New Zealand 21-23 Jayashri B and Arvind S 2013 Design and Implementation of Security for Smart Home based on GSM technology International Journal of Smart Home 7 201-08
- Lee C T, Shen T C, Lee W D and Weng K W 2016 A novel electronic lock using optical Morse code based on the Internet of Things Proceedings of the IEEE International Conference on Advanced Materials for Science and Engineering eds. Meen, Prior & Lam
- Anitha A, Paul G and Kumari S 2016 A Cyber defence using Artificial Intelligence International Journal of Pharmacy and Technology 8 25352-57
- Anitha A, Kalra S and Shrivastav 2016 A Cyber defence using artificial home automation system using IoT International Journal of Pharmacy and Technology 8 25358-64
- - R. -, "IR Sensor Working Principal & Applications," *Robocraze*, 20-Jun-2022. [Online]. Available: <https://robocraze.com/blogs/post/ir-sensor-working>. [Accessed: 31-Nov-2022].
- Admin, "LDR sensor with Arduino tutorial: What is Arduino Light Sensor in details," *Techatronic*, 04-Apr-2022. [Online]. Available: <https://techatronic.com/ldr-sensor-with-arduino-tutorial/>. [Accessed: 02-Nov-2022].
- "Arduino with pir motion sensor," *Arduino Project Hub*. [Online]. Available: <https://create.arduino.cc/projecthub/biharilifehacker/arduino-with-pir-motion-sensor-fd540a>. [Accessed: 02-Nov-2022].
- "Intel® Edison Development Platform." [Online]. Available: https://www.intel.com/content/dam/support/us/en/documents/edison/sb/edison_pb_331179002.pdf. [Accessed: 31-Nov-2022].

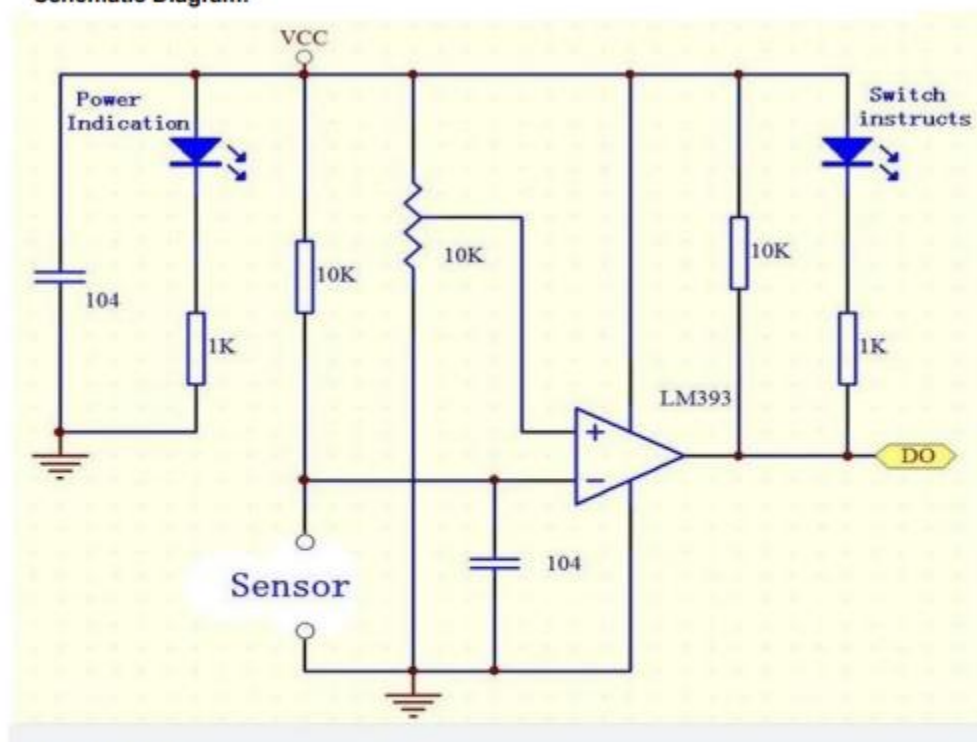
- L. Ada, “Pir motion sensor,” *Adafruit Learning System*. [Online]. Available: <https://learn.adafruit.com/pir-passive-infrared-proximity-motion-sensor/>. [Accessed: 02-Nov-2022].
- “Security access using RFID reader,” *Arduino Project Hub*. [Online]. Available: <https://create.arduino.cc/projecthub/Aritro/security-access-using-rfid-reader-f7c746>. [Accessed: 01-Nov-2022].
- “Radio interference and how it impacts IOT Systems,” *Novotech Technologies*, 28-Oct-2020. [Online]. Available: <https://novotech.com/learn/m2m-blog/blog/2020/10/28/radio-interference-and-how-it-impacts-iot-systems/#:~:text=A%20second%20solution%20is%20to,uses%20the%205%20GHz%20band>. [Accessed: 04-Nov-2022].

Appendix A:

Flame Sensor:

<https://4.imimg.com/data4/AV/UT/MY-23669504/flame-sensor-module-arduino.pdf>

Schematic Diagram:

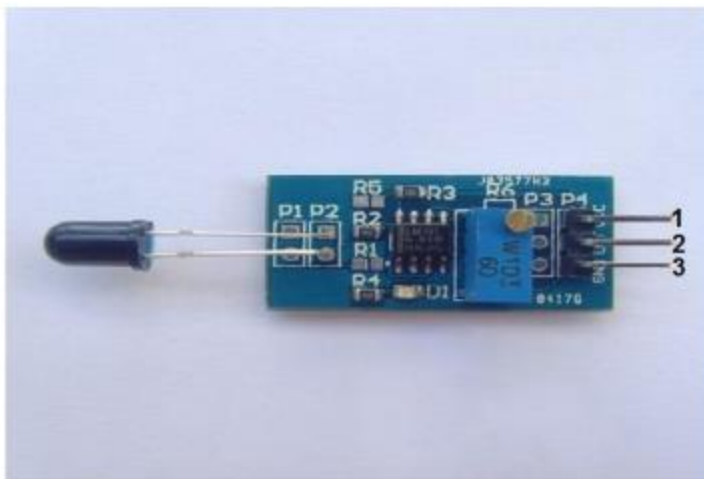


How to test:

1. Connect your Arduino microcontroller to the computer.
2. Connect the VCC pin of your module to the 5V pin of your Arduino.
3. Connect the GND pin of your module to the GND pin of your Arduino.
4. Connect the Output pin of your module to the A0 pin of your Arduino.
5. Enter this program to your Arduino Integrated Development Environment (IDE):

Specifications:

- On-board LM393 voltage comparator chip and infrared sensing probe.
- Support 5V/3.3V voltage input.
- On-board signal output indication, output effective signal is high level, and the same time the indicator light up, output signal can directly connect with microcontroller IO.
- Signal detection sensitivity can be adjusted.
- Reserved a line voltage compare circuit (P3 is leaded out).
- PCB size: 30(mm) x15(mm).

**Pin Configuration:**

1. VCC
2. Output
3. Ground

Temperature & Humidity Sensor (DHT11)

<https://www.mouser.com/datasheet/2/758/DHT11-Technical-Data-Sheet-Translated-Version-1143054.pdf>

2. Technical Specifications:

Overview:

Item	Measurement Range	Humidity Accuracy	Temperature Accuracy	Resolution	Package
DHT11	20-90%RH 0-50 °C	± 5%RH	± 2 °C	1	4 Pin Single Row

Detailed Specifications:

Parameters	Conditions	Minimum	Typical	Maximum
Humidity				
Resolution		1%RH	1%RH	1%RH
			8 Bit	
Repeatability			± 1%RH	
Accuracy	25°C		± 4%RH	
	0-50°C			± 5%RH
Interchangeability	Fully Interchangeable			
Measurement Range	0°C	30%RH		90%RH
	25°C	20%RH		90%RH
	50°C	20%RH		80%RH
Response Time (Seconds)	1/e(93%)25 °C, 1m/s Air	6 S	10 S	15 S
Hysteresis			± 1%RH	
Long-Term Stability	Typical		± 1%RH/year	
Temperature				
Resolution		1°C	1°C	1°C
		8 Bit	8 Bit	8 Bit
Repeatability			± 1°C	
Accuracy		± 1°C		± 2°C
Measurement Range		0°C		50°C
Response Time (Seconds)	1/e(93%)	6 S		10 S

3. Typical Application (Figure 1)

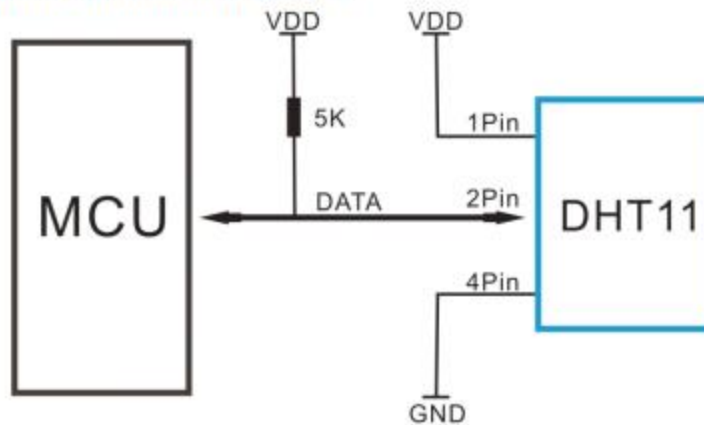


Figure 1 Typical Application

Note: 3Pin – Null; MCU = Micro-computer Unite or single chip Computer

When the connecting cable is shorter than 20 metres, a 5K pull-up resistor is recommended; when the connecting cable is longer than 20 metres, choose a appropriate pull-up resistor as needed.

6. Electrical Characteristics

VDD=5V, T = 25℃ (unless otherwise stated)

	Conditions	Minimum	Typical	Maximum
Power Supply	DC	3V	5V	5.5V
Current Supply	Measuring	0.5mA		2.5mA
	Average	0.2mA		1mA
	Standby	100uA		150uA
Sampling period	Second	1		

Note: Sampling period at intervals should be no less than 1 second.

Smoke Sensor

<https://5.imimg.com/data5/BG/QX/MY-1833510/mq2-gas-sensor-module.pdf>

SPECIFICATIONS

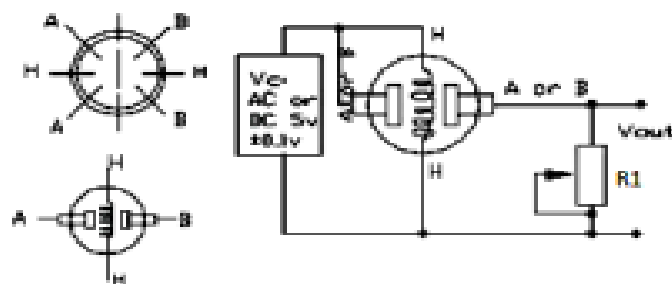
- Power Supply: 4.5V to 5V DC
- High sensitivity to Propane, Smoke, LPG and Butane
- Wide range high sensitivity to Combustible gases
- Long life and low cost
- Analog and Digital output available
- Onboard visual indicator (LED) for indicating alarm
- Compact design and easily mountable
- Simple 4 PIN header interface
- Drive circuit is simple.
- Sensor Type : Semiconductor
- Concentration : 300-10000ppm (Combustible gas)
- Supply voltage =5v

APPLICATIONS

- Safety of home
- Control of air quality
- Measurement of gas level

Working Principle

The MQ2 has an electrochemical sensor, which changes its resistance for different concentrations of varied gasses. The sensor is connected in series with a variable resistor to form a voltage divider circuit (Fig 1), and the variable resistor is used to change sensitivity. When one of the above gaseous elements comes in contact with the sensor after heating, the sensor's resistance change. The change in the resistance changes the voltage across the sensor, and this voltage can be read by a microcontroller. The voltage value can be used to find the resistance of the sensor by knowing the reference voltage and the other resistor's resistance. The sensor has different sensitivity for different types of gasses.

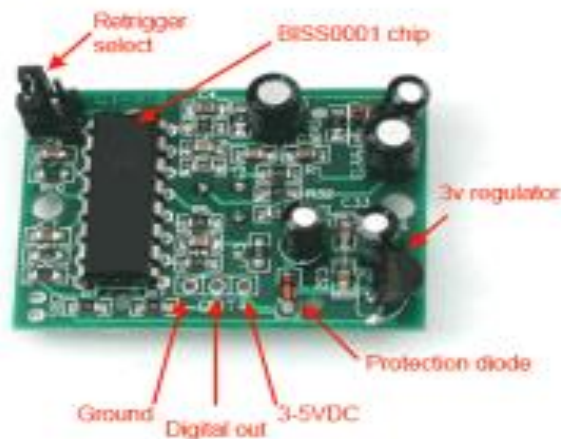


PIR Motion Sensor

<https://cdn-learn.adafruit.com/downloads/pdf/pir-passive-infrared-proximity-motion-sensor.pdf>

Along with the pyroelectric sensor is a bunch of supporting circuitry, resistors and capacitors. It seems that most small hobbyist sensors use the [BISS0001](https://adafruit.it/cir/) ("Micro Power PIR Motion Detector IC") (<https://adafruit.it/cir/>), undoubtedly a very inexpensive chip. This chip takes the output of the sensor and does some minor processing on it to emit a digital output pulse from the analog sensor.

Our older PIRs looked like this:



Our new PIRs have more adjustable settings and have a header installed in the 3-pin ground/out/power pads

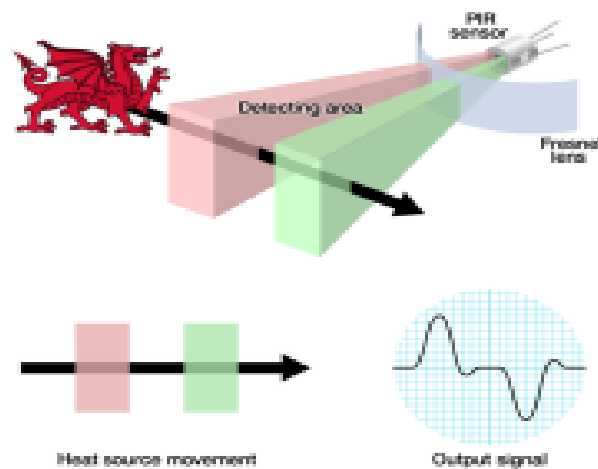


For many basic projects or products that need to detect when a person has left or entered the area, or has approached, PIR sensors are great. They are low power and

How PIRs Work

PIR sensors are more complicated than many of the other sensors explained in these tutorials (like photocells, FSRs and tilt switches) because there are multiple variables that affect the sensors input and output. To begin explaining how a basic sensor works, we'll use this rather nice diagram

The PIR sensor itself has two slots in it, each slot is made of a special material that is sensitive to IR. The lens used here is not really doing much and so we see that the two slots can 'see' out past some distance (basically the sensitivity of the sensor). When the sensor is idle, both slots detect the same amount of IR, the ambient amount radiated from the room or walls or outdoors. When a warm body like a human or animal passes by, it first intercepts one half of the PIR sensor, which causes a positive differential change between the two halves. When the warm body leaves the sensing area, the reverse happens, whereby the sensor generates a negative differential change. These change pulses are what is detected.

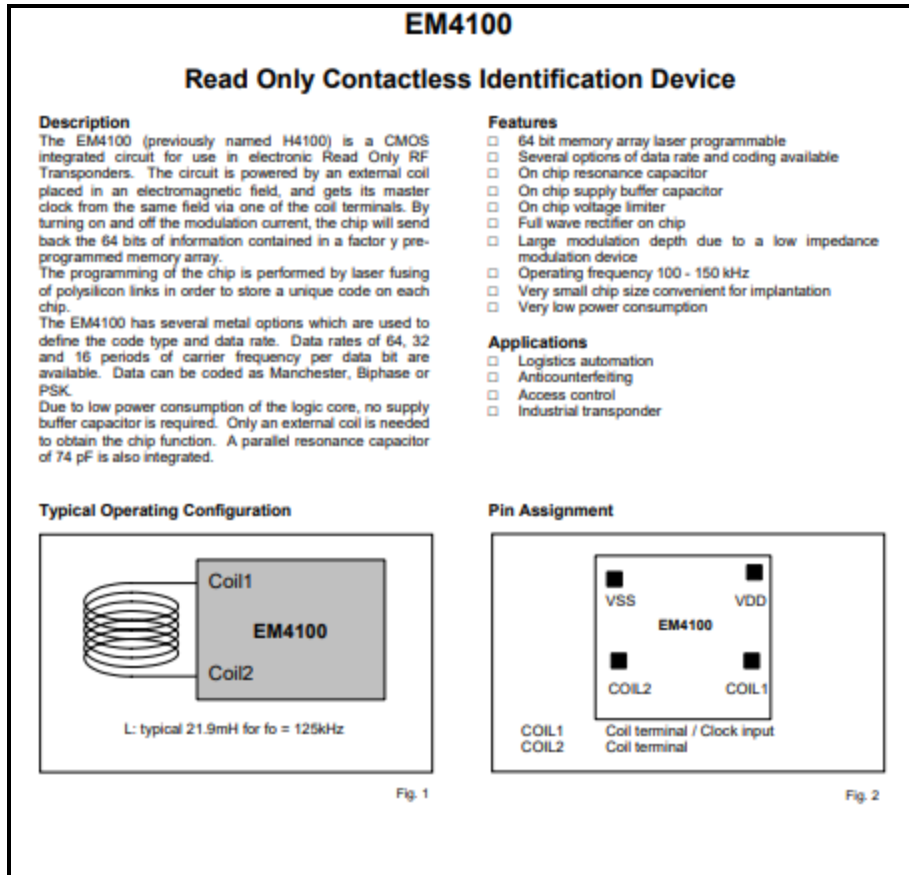


The PIR Sensor

The IR sensor itself is housed in a hermetically sealed metal can to improve noise/temperature/humidity immunity. There is a window made of IR-transmissive material (typically coated silicon since that is very easy to come by) that protects the sensing element. Behind the window are the two balanced sensors.

RFID:

<https://download.mikroe.com/documents/accessories/rfid/125khz/rfid-card-125khz-em4100-datasheet.pdf>



Appendix B:

C	Python	Java	C++
Machine independent and portable	Object oriented programming	Neutral architecture	Compiler based
Case sensitive	GUI Support	Platform independent	Portability
Rich set of operators	Embeddable	Robust	Portability
Easily extendable	Integrated	Multithreaded	Structure and pointers allocations
Low memory usage	Dynamic memory allocation	Secure	Garbage removed dynamically
Statically typed	Interpreted language	Distributed	Procedural programming

Appendix C

Examples of trouble-shooting and debugging:

- ❖ One of the most complex and tedious tasks was to setup the RFID sensor. Before giving the access to a specific card or a tag we need to get the Unique ID of the particular card or tag. The above process took us a lot of time as our code showed some errors but later realized that the Arduino rev2 has a different way of connection with the sensor as compared to the normal Arduino UNO. Thus, this was one of the examples of trouble-shooting and debugging
- ❖ The other one was with the PIR sensor which we used to detect the motion of a person sitting on a desk to calculate total time but the sensor needed to be adjusted for the sensitivity and also the time delay for which it should be working.
- ❖ We also faced difficulty adjusting the light intensity value which is measured through light sensor as the output of this sensor was connected to the led in order to change the intensity of the led with the change in the value of LDR light sensor. This was solved using proper calibration technique.

Appendix D

All the parts/Sensors of our system will be mostly be placed in indoor conditions but it may defer to some extent based on the designs and architecture of different offices.

Firstly, we plan to integrate the whole system of Secure Door with Authorized Entry within a box where in the front part a provision would be kept for scanning the RFID and wherever the sensor would be kept- the top of it would be kept open such that it can easily sense from the outer environment. Also, we would place at a certain height so that changes of damage reduce. Along with this as all the parts would be placed inside the box except the RFID scanner so they would be protected from external environment. At last, for the power supply a plug would be pinned from the backside of the box which would be connected to the charging/power socket. If in any case there is any disruption being caused in the sensors or any other device then the lid of box can be easily opened and issue can be fixed accordingly.

Appendix E

Problem 1:

Although it's not very common, wireless corporate security systems can suffer from interference. Some types of electrical equipment could cause problems, and large metal objects can block the signal. It is also possible that an attacker could jam a wireless corporate alarm if they had the right equipment.

- One solution is to only use IoT systems in cellular bands where the RF environment is well planned and coordinated. Cellular systems don't experience interference – when they do, it's because someone used an unauthorized device that "leaks" RF into a licensed band. Such occurrences, while on the rise, are not as commonplace. However, such systems are more expensive than those deployed in the unlicensed bands.
- A second solution is to use IoT systems that are well-separated in frequency. For instance, don't build or use a system that relies on Wi-Fi and Bluetooth systems operating at 2.4 GHz. Instead, use a Wi-Fi system that only uses the 5 GHz band. While this doesn't mitigate interference from outside your network, it at least minimizes self-interference.
- It is anticipated that the use of 5G will greatly benefit IoT for many different reasons. There will be plenty of licensed spectrum to use for IoT products and applications from an interference standpoint. More than ever before, it should be relatively easy to avoid RF interference while allowing many devices to operate simultaneously and collision-free.

Problem 2:

All the detection devices in this system usually run-on batteries. That can be a lot of batteries in a large office. The sensors will need to be periodically checked and the batteries replaced as needed.

Prioritizing power optimization during development is crucial for ensuring the device performs as intended. Hence below Mentioned are some effective ways through which we can effectively perform power optimization:

- Implement a Sleep Mode for IoT devices
- Consider energy harvesting techniques
- Avoid excessive Push Notifications
- Choose when and how the IoT device transfers information
- Understand how features affect battery life
- Select the most appropriate Wireless Protocol
- Ponder power consumption with care

Problem 3:

It could be possible for a Cyber attacker to hack a wireless system and block the signals. Some cheaper wireless systems do not encrypt the wireless signal between the sensors and the control panel.

- One of the solutions could be that we can deploy a Next-Generation Firewall because a traditional firewall lacks important security features. A next-generation firewall (NGFW) is an integrated network platform that combines a traditional firewall with other security functionalities such as intrusion prevention system (IPS), malware protection, content filtering, SSL/SSH interception, QoS management, and virtual private network (VPN). An NGFW has all the capabilities of a traditional firewall as well, making it powerful in detecting and protecting against cyberattacks.
- The other solution could be that we can add multi-factor authentication or 2 Factor Authentication (2FA) which is an added layer of security beyond a mere password. With two-factor authentication, every time someone tries to log in to your IoT device, they have to provide additional proof of identity. This proof can come in the form of a one-time pin (OTP) or a verification code sent to your phone or email address that confirms that the person logging in is indeed you.