IoT Project Report

Home Intrusion Detection System

TEAM MEMBERS

TEJAS PARMAR - 151070036

VATSAL MANKODI-151070035

NIKHIL VANKALAYA- 151070040

PRAFULL PARMAR - 151070025

INDEX:

Step 1: Purpose & Requirements Specifications:

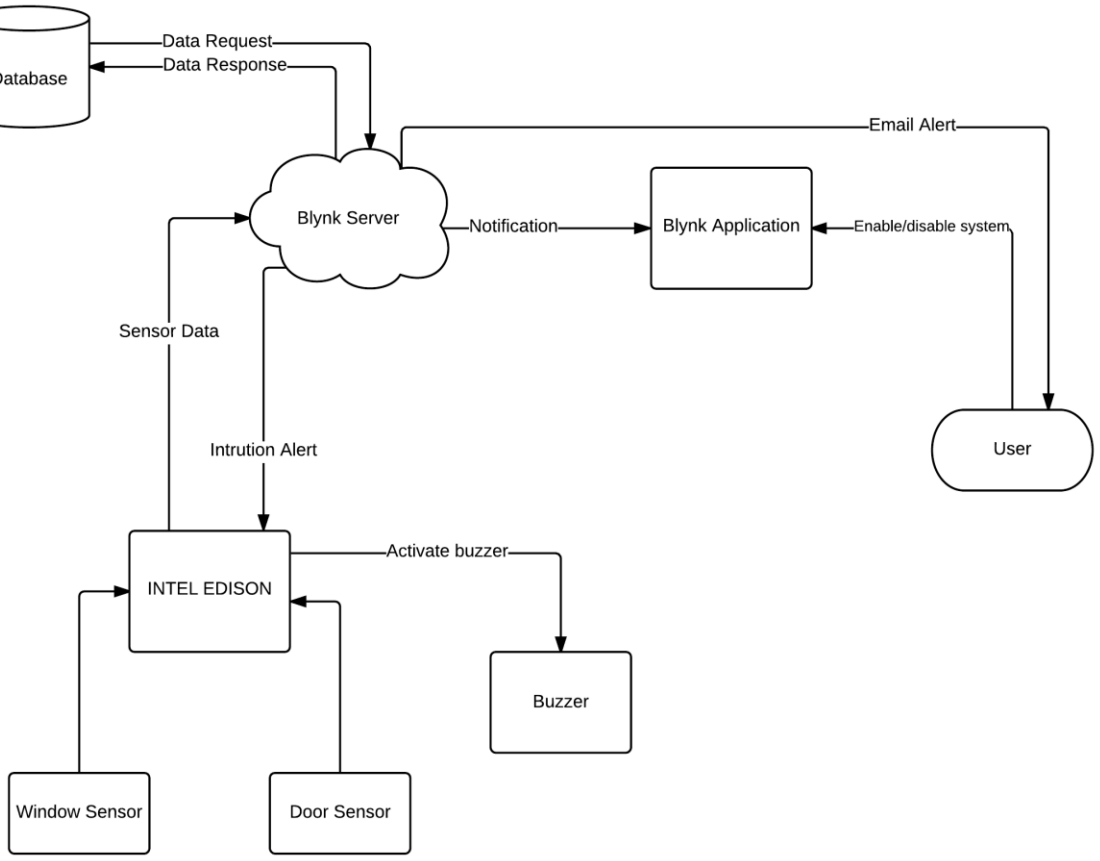
1) Purpose: To design an IoT based solution for an intelligent intrusion detection system with user authentication and remote monitoring capabilities.

2) Behaviour: The user is notified on his mobile application Email whenever the smart system detects an intrusion in any of the doors or windows. The user is then suggested SOS emergency measures to counter the same.

3) System Management Requirements: The system must manage the monitoring and control functions.

4) Data Analysis Requirements: The system must analyse data remotely.

5) Application Deployment Requirement: The application must be deployed on the cloud.



Step 2: Process Specification :-

The second step is process specification. The following diagram shows the Process Specification of the intelligent intrusion detection system IoT system.

The system is connected to a Wi-Fi based network and has the following features:

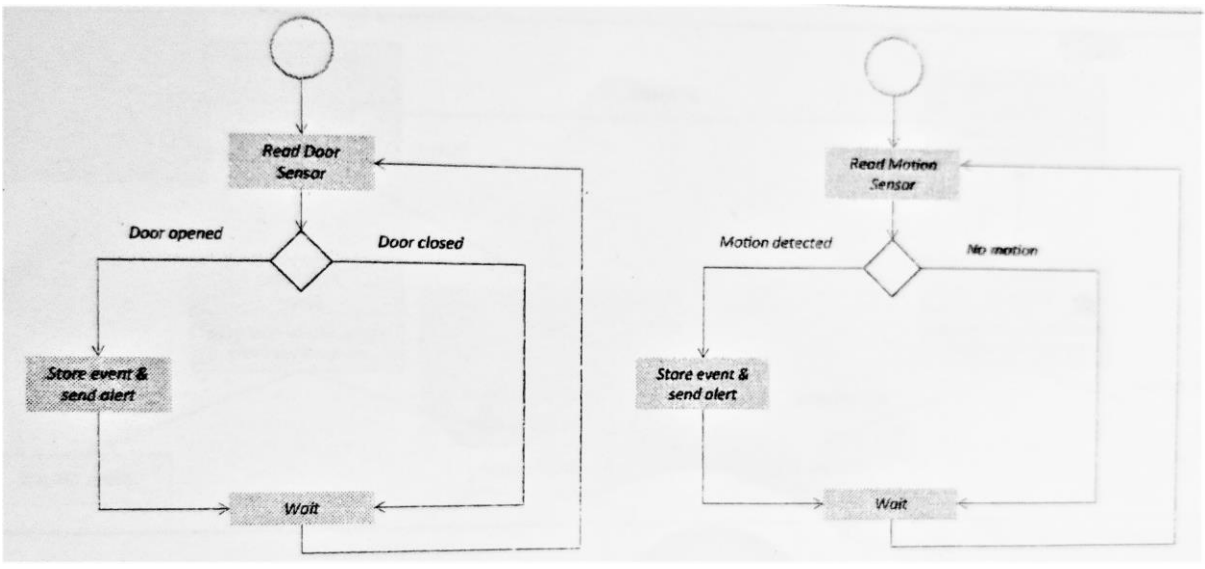
- **Remote monitoring via an application**.
  The home owner has a mobile application which can monitor the lock status of the doors and windows.

- **Application alerts about intrusions.**
  The user is notified on his mobile application whenever the smart system detects an intrusion in any of the doors or windows. The user is then suggested SOS emergency measures to counter the same.

- **Email alerts about intrusions.**
  The user is notified on his Email whenever the smart system detects an intrusion in any of the doors or windows.

- **Voice Alert during a breach.**
  A voice alarm is activated whenever an intrusion is detected by the motion sensors connected to the doors and windows.

Figure 1: Process Specification



Step 3: Domain Model Specification :-

This is the third step in the IoT design methodology. The domain describes the concepts like

the entities, objects and the relationships among them. The entities, objects and the concepts for the Blynk IoT Platform are:

1) Physical Entity: It is the discrete identifiable entity in the physical environment. In the case of this project, there are two physical entities involved- one is the door and other is the window in which the sensors will be placed for monitoring the motion through proximity sensor

2) Virtual Entity: It is the representation of the physical entity in the digital world. So, in the Blynk IoT Platform project there are two virtual entities corresponding to the two physical entities described above.

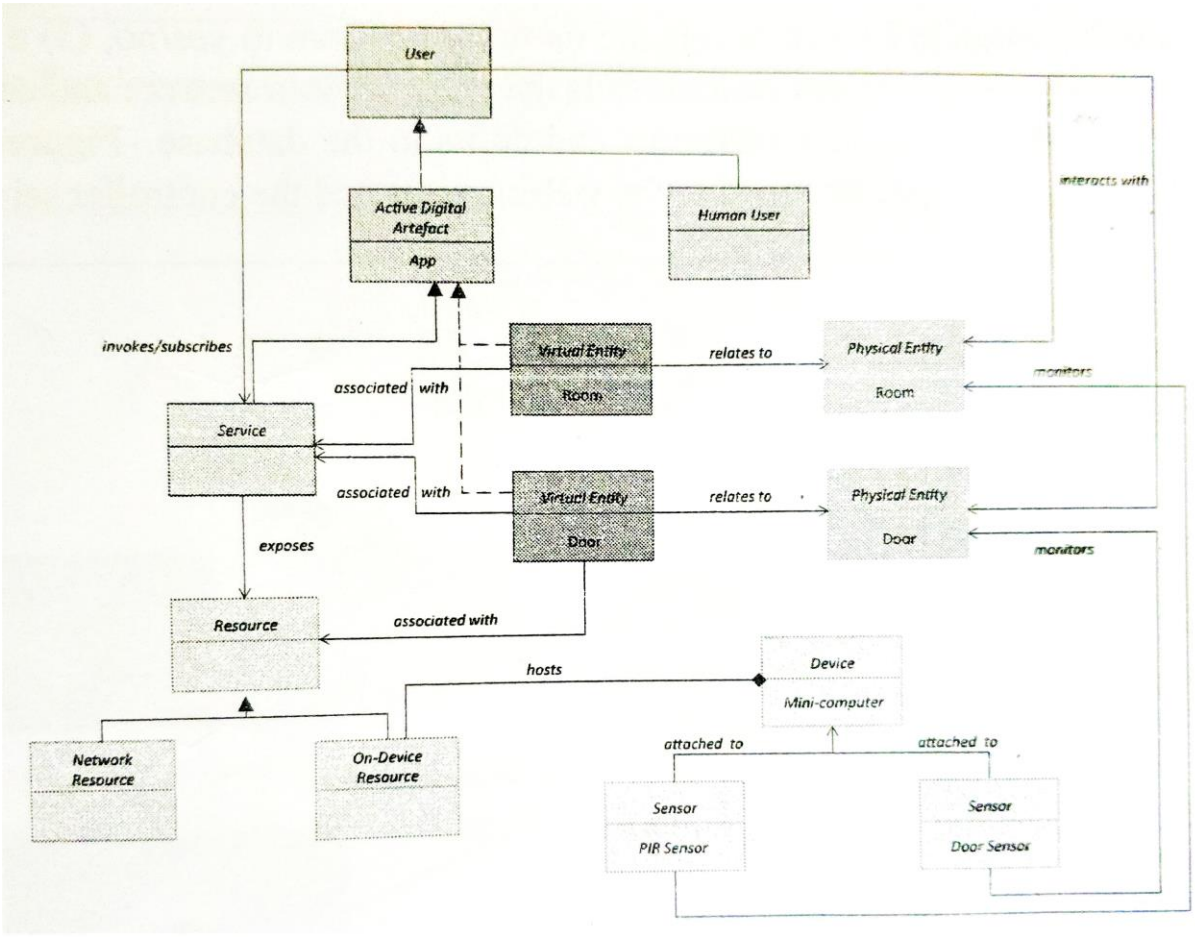
3) Device: It provides a mechanism between physical and virtual entities. Devices are placed near physical entities and gather the information about them and platform actuation on the physical entities. In this project, the devices are the Intel Edison microcontroller that has a proximity sensor and buzzer attached to it.

4) Resource: They are the software components that can either be on-device or network resources. In the Blynk IoT platform system, the on-device resource are the operating systems (Yocto Embedded Linux on Intel Edison) that runs on the mini-computers.

5) Service: It provides an interface for interacting with the physical entity. In the Blynk IoT platform system, there are two services:

a) A service that send the values of the proximity sensor to the Blynk server , which in turn sends an intrusion alert to the user through the Blynk app and also sends an email to the user.

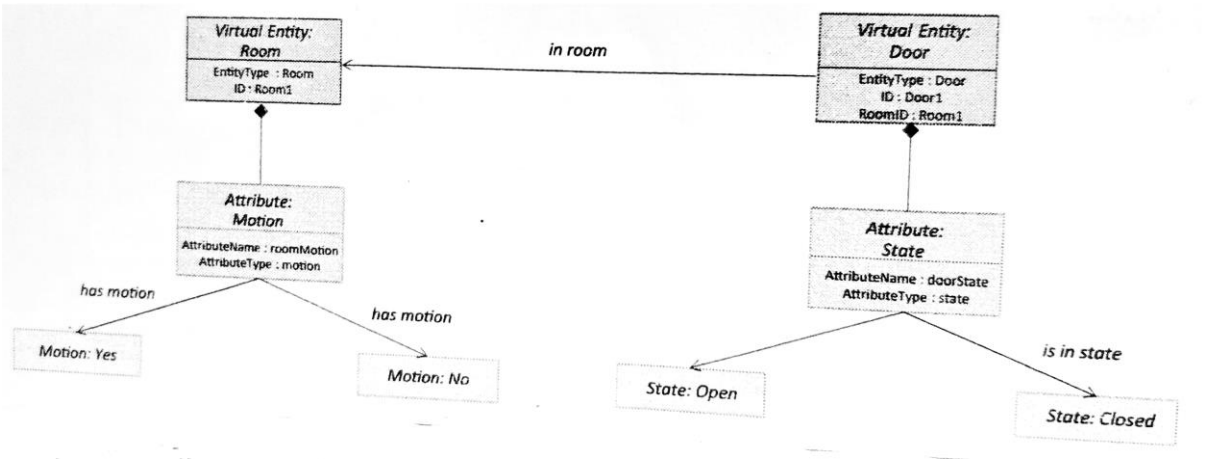
b) A service that activates the voice alert module when an intrusion occurs.


User
Active Digital Artefact
App
Human User
interacts with
invokes/subscribes
Virtual Entity
Room
relates to
Physical Entity
Room
monitors
associated with
Service
associated with
Virtual Entity
Door
relates to
Physical Entity
Door
monitors
exposes
Resource
associated with
hosts
Device
Mini-computer
Network Resource
On-Device Resource
attached to
attached to
Sensor
PIR Sensor
Sensor
Door Sensor

Step 4: Information Model Specification :-

This is the fourth step of the IoT design methodology. Information model defines the structure of all the information in the system, for example the entities, attributes, relations, etc. It does not describe how the information is represented. The virtual entities are listed which are defined in the Domain Model Specification and more details about those entities are added. In our project, the two virtual entities i.e the door and the window in which the PIR sensor is placed for motion detection.

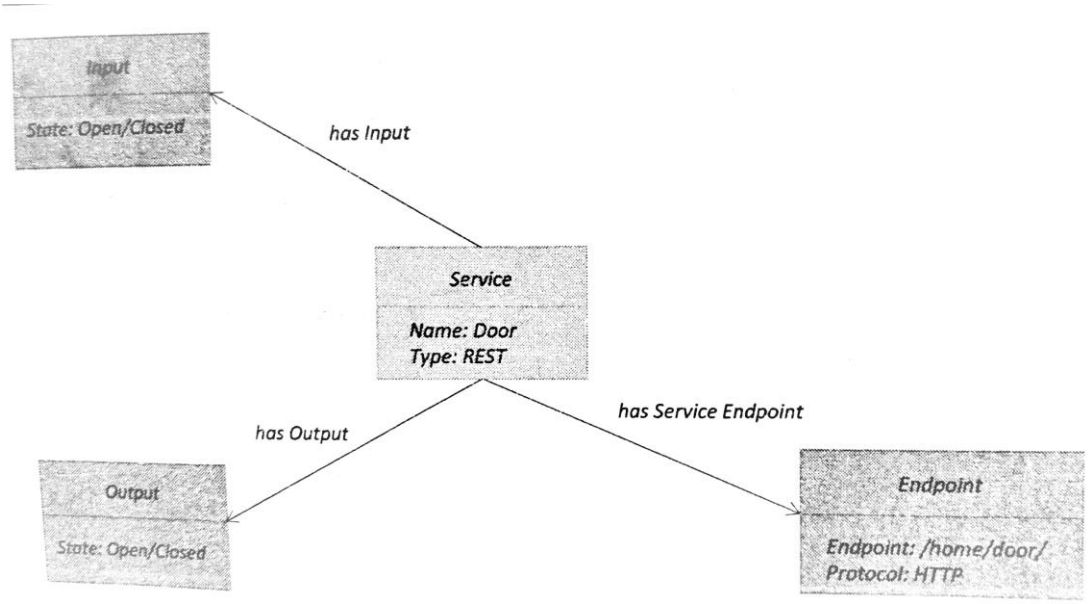
Figure 3: Information Model Specification

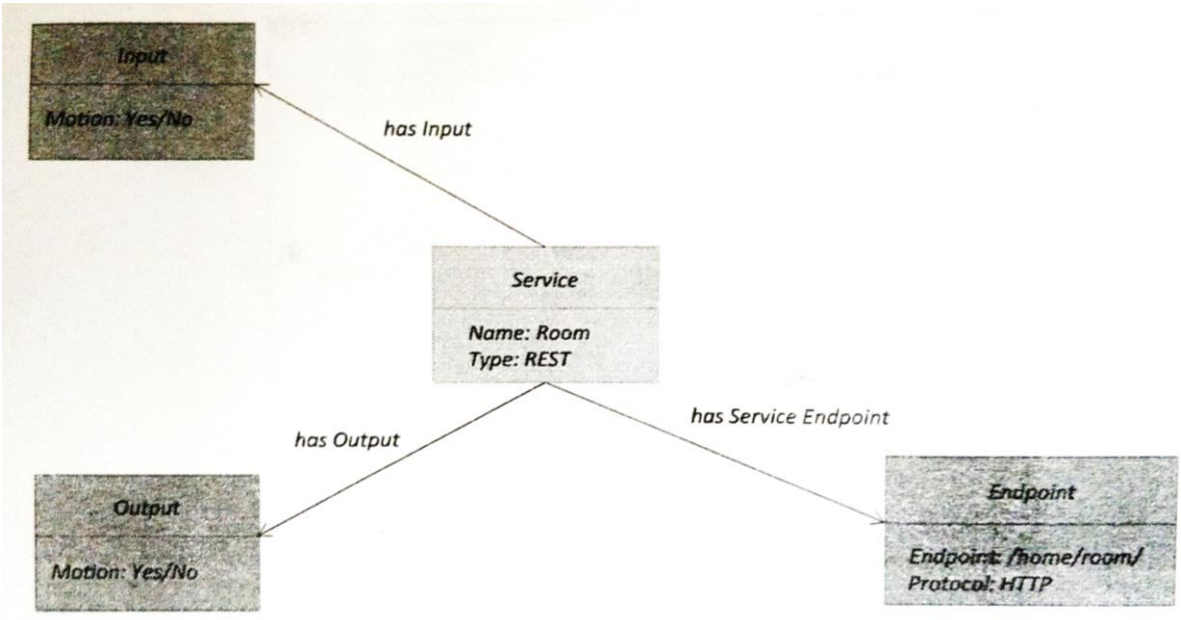


Step 5: Service Specification :-

This is the fifth step in IoT design methodology. Service specifications define the service in IoT system, service types, service inputs-outputs, service endpoints, service schedules, service preconditions and service efforts.The services provided by the Smart intrusion detection system are:-

- Remote monitoring via an application.
- Application alerts about intrusions.
- Email alerts about intrusions.
- Voice Alert during a breach.

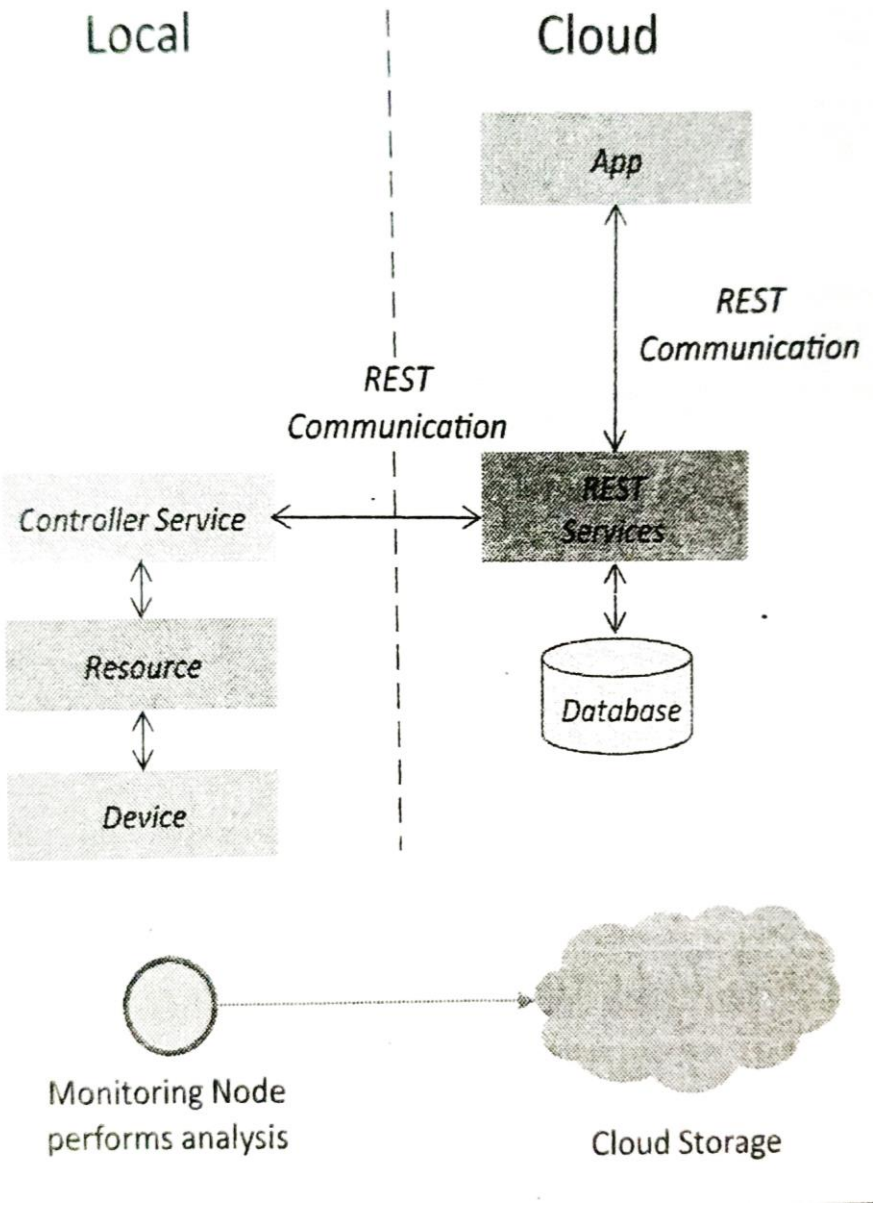




Step 6: IoT Level Specification :-

The actual IoT Level that are used here are Level-2 Specifications.

The analysis of the motion using the PIR sensor is done at monitoring node which is the edison board band the sensor data is sent to the cloud which is the Blynk cloud in this case .Thus the IOT Level-2 Specification is used.



Step 7: Functional View Specification :-

This is the seventh step in IoT design methodology. The Functional View defines the functions of the IoT systems grouped into various functional groups. Each functional group provides functionalities for interacting with the instances of the concepts defined in Domain Model

Specification. The FG included in this part are:

1) Device: In our project, the devices are the single board minicomputer (Intel Edison) which acts as a sensor and actuator node and a wifi-router.

2) Communication: The FG handles the communications of the IoT system. It Includes protocols like IPv4 (network layer), TCP(transport layer), HTTP(application layer) and Blynk protocols.

3) Services: In our project, there are two services, Monitor Service and Storage Service

4) Management: The management FG includes all functionalities that are needed to configure and manage the system.

5) Application: The application FG includes the interface that would be used by the users to access the control of the appliance and monitor the motion. In this example, we have used a Blynk application.

Step 8: Operational View Specification :-

This is the eighth step in the IoT design methodology. In this step various options like service

hosting, service options, device options, application hosting options, etc. are defined. The

operational view specifications include:

1) Device: Computing devices (Intel Edison),PIR sensor, Voice module, WiFi Router.

2) Communication Protocols : IPv4 (network layer), TCP(transport layer), HTTP(application layer), Blynk Protocols.

3) Services:

a) Controller Service: Hosted on device, implemented on Intel Edison and run as a native service.

b) Monitor Service: Network services to send the data to the Blynk database and from there using network service to upload it on the web application.

4) Application: Blynk Application.

Step 9:Device and Component Specification

● Intel Edison: The Intel Edison is used as a remote sensor node which collects data from the PIR sensors attached to the doors and windows. It then sends this data to the Blynk Server which then sends relevant feedbacks and notification alerts to the users using the Blynk application and email service.

● Motion Sensor: The motion sensors are attached to 3 different entities which are the door,window and the valuables in the home.

Platform used for the project is Blynk platform.There are three major components in the platform:

- **Blynk App** - allows to you create amazing interfaces for your projects using various widgets we provide.
- **Blynk Server** - responsible for all the communications between the smartphone and hardware. You can use our Blynk Cloud or run your private Blynk server locally. It's open-source, could easily handle thousands of devices and can even be launched on a Raspberry Pi.
- **Blynk Libraries** - for all the popular hardware platforms - enable communication with the server and process all the incoming and outcoming commands.

In the entire project, there are three independent processes going on. They are;

● Sensor data acquisition and transport from Edison to Blynk Server.

● Parsing and logging the data in a database on the Blynk Server..

● Selecting and displaying the data on the GUI on the Blynk application as values or a graph.

The reason I say they are independent is that they are asynchronous and the procedures for any step is not dependent on any other steps. All the steps only change database values.

Working:

- The smart intrusion detection systems consists of proximity sensors which are are placed in the doors and windows of the home.
- Sensors are also placed near the valuables in the home.
- The Proximity sensors helps in detecting the motion .
- The user is alerted of the intrusion using the Blynk Application Notification .
- Email is also sent to the user using the Blynk Server whenever an intrusion occurs.
- The sensor data is sent to the Blynk Server using HTTP and Blynk protocols for analysis and the data is stored in the database, if an intrusion is detected then the user is notified of intrusion.
- The Blynk Server sends an intrusion alert to the edison board an the buzzer alarm connected to the edison board is activated.
- The user can enable/disable the system using the application.

Components Specification:

HARDWARE:

- Intel Edison Breakout Board
- Resistors
- Proximity(PIR) sensor
- Bread Board
- Connecting wires

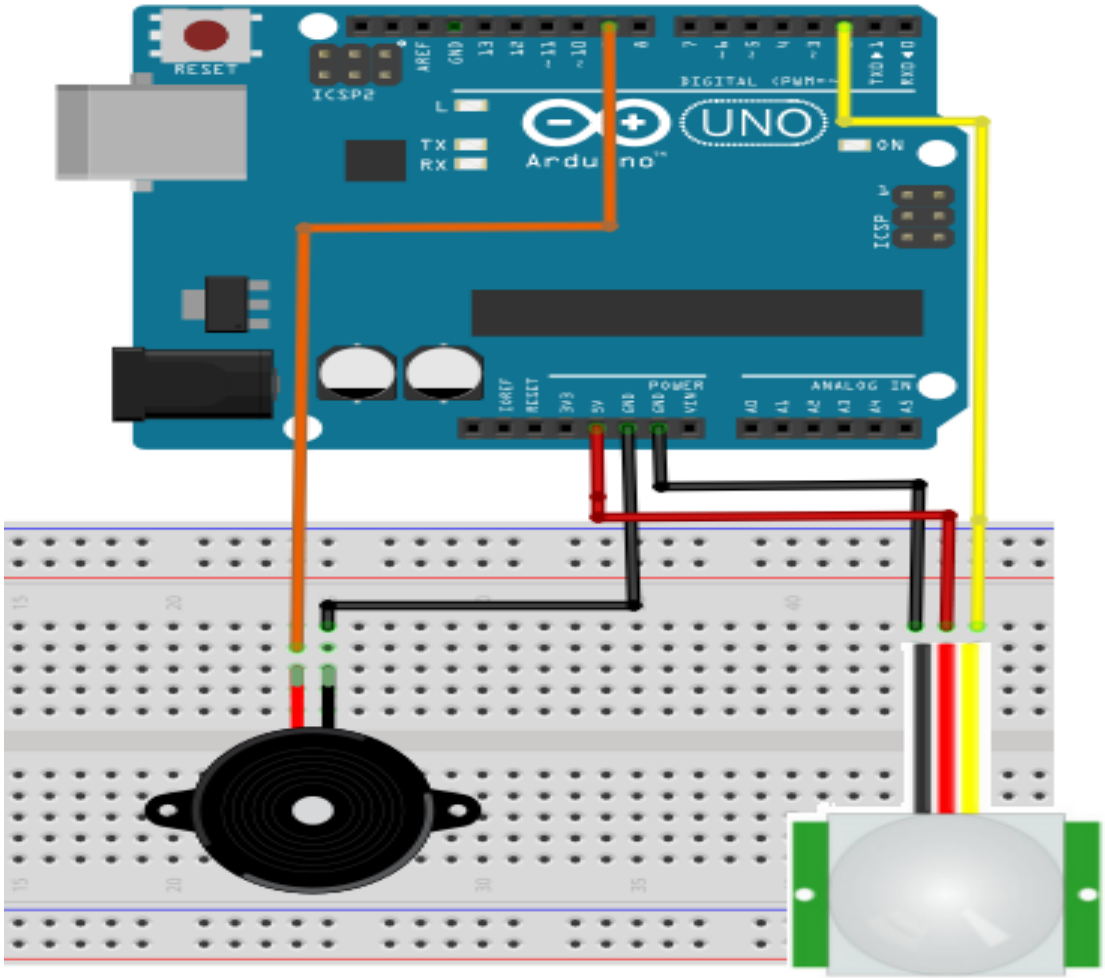
SOFTWARE & PLATFORMS:

- IDE: Arduino IDE
- Blynk Mobile App

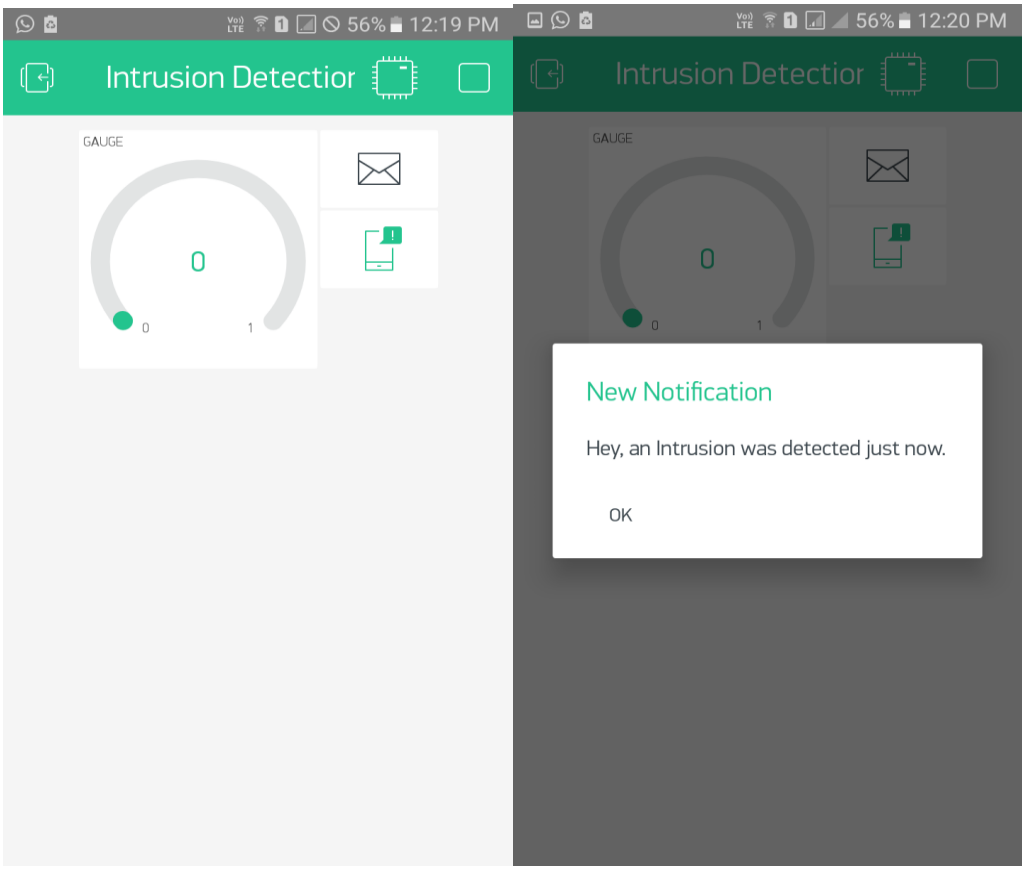
Step 10: Application Interface

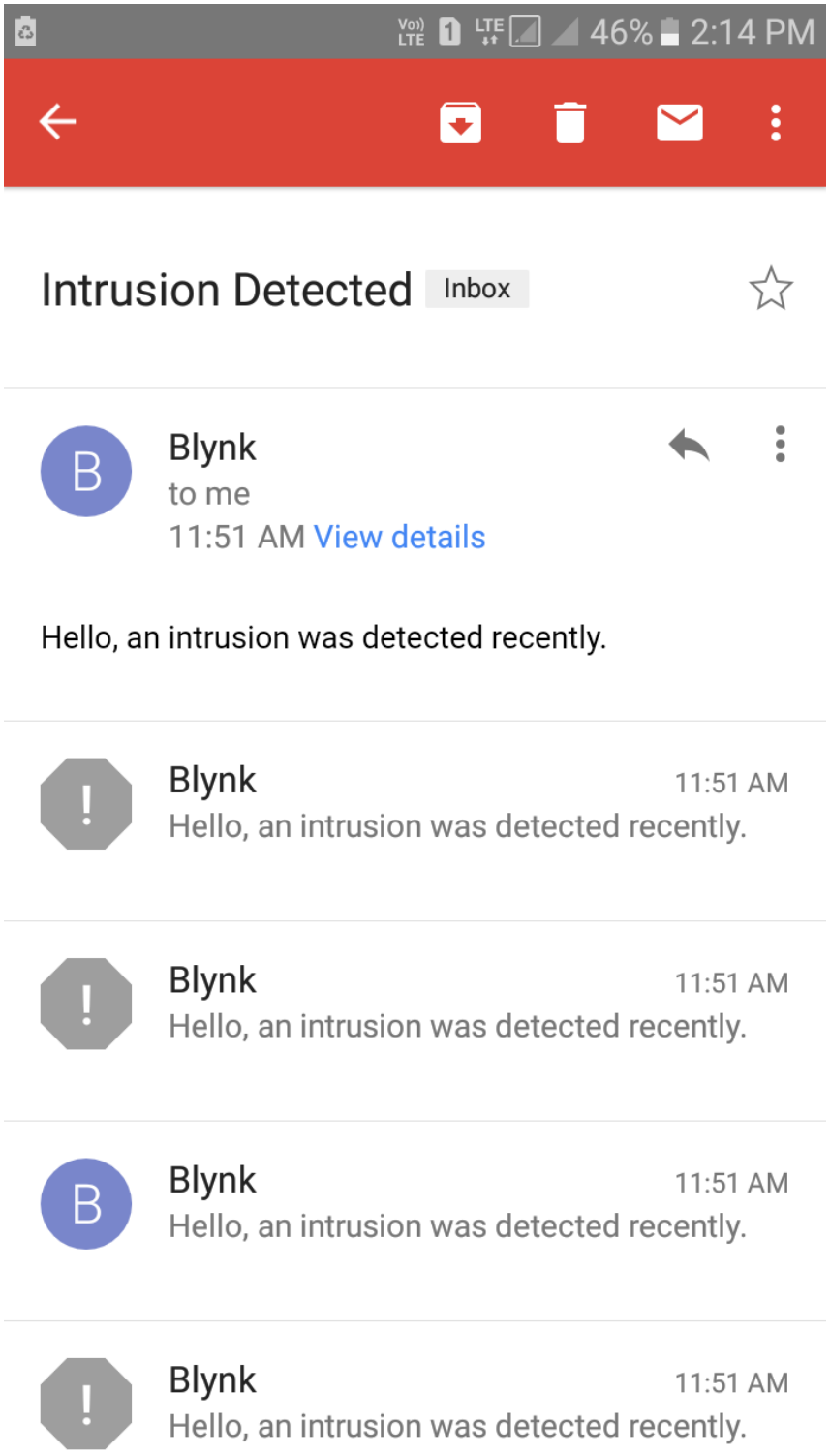
A Blynk application is used to visualise the data obtained from the sensors. These data items can be used to analyse the house conditions and form strong inferences. Blynk app is connected to Blynk database from where it retrieves the data stored in the tables and creates a line graph from the data.

Circuit Diagram:



Mobile Application:




46% 2:14 PM
Intrusion Detected
Inbox
B
Blynk
to me
11:51 AM View details
Hello, an intrusion was detected recently.
Blynk 11:51 AM
Hello, an intrusion was detected recently.
Blynk 11:51 AM
Hello, an intrusion was detected recently.
B
Blynk 11:51 AM
Hello, an intrusion was detected recently.
Blynk 11:51 AM
Hello, an intrusion was detected recently.

PROGRAM:

```
#define BLYNK_PRINT Serial


#include <WiFi.h>
#include <BlynkSimpleIntelEdisonWiFi.h>

const int motionSensor = 12;
int voiceOn=8;

// You should get Auth Token in the Blynk App.
// Go to the Project Settings (nut icon).
char auth[] = "7971a80ce5db4fde8f7039c526ad37fd";

// Your WiFi credentials.
// Set password to "" for open networks.
//char ssid[] = "Tej's Hotspot";
//char pass[] = "yeja5279";
char ssid[] = "PDP";
char pass[] = "73031452000";
bool alert=false;

String Title = "Intrusion Detected";
String Body = "Hello, an intrusion was detected recently.";

void setup()
{
  // Debug console
  Serial.begin(9600);

  //Blynk.begin(auth, ssid, pass);
  // Or specify server using one of those commands:
  Blynk.begin(auth, ssid, pass, "blynk-cloud.com", 8442);
  //Blynk.begin(auth, ssid, pass, "172.18.39.36", 8442);

     pinMode(voiceOn,OUTPUT);
}

void loop()
{
  int a = digitalRead(motionSensor);
  if(a==1){

    Blynk.email("tejasparmar99@gmail.com", Title, Body);
    Blynk.notify("Hey, an Intrusion was detected just now.");
    digitalWrite(voiceOn, HIGH);


    }
    else{
     digitalWrite(voiceOn, LOW);

    }
```

```
  Serial.print(a);
  Blynk.virtualWrite(V0,a);

  Blynk.run();
}
```

CONCLUSION:

Thus we have successfully completed a working prototype of a home intrusion detection system using Blynk IoT Platform.

Future Scope:

- A Snapshot of the intruder can be taken
- The security authorities can be notified
- A Light sensor can be used
- A measure of the intrusion threat can be calculated