Theme no. 2

Smart Home – Security Monitoring

Ana-Maria Lupoaea
Andrei-Răzvan Tablan

1. Applicability domains

The system we propose is a Smart Home system, which incorporates IoT technology to enhance convenience, security, and energy efficiency. The system comprises different components such as smart home devices, communication protocols, a central hub, and a mobile application. |

a. use-cases (minim 4, maxim 8);

- *Lighting Control:* Smart bulbs can be installed in different rooms of the house and controlled through a mobile application. The system can be programmed to turn off the lights automatically when no one is in the room or turn on the lights when someone enters the room.
- *Temperature Control*: Smart thermostats can be installed to control the temperature of the house and optimize energy consumption. The system can be programmed to adjust the temperature based on the time of day or the number of people in the house.
- *Security Monitoring*: IoT cameras can be installed to monitor the house and send alerts to the mobile application when there is any unusual activity. The system can be programmed to automatically turn on the lights or sound an alarm when there is a security breach.
- *Home Entertainment*: Smart speakers can be installed in different rooms of the house, and controlled through the mobile application. The system can be programmed to play music, or stream movies on the TV.
- *Energy Management*: Smart plugs can be installed to monitor the energy consumption of different appliances and provide insights into energy-saving opportunities. The system can be programmed to turn off appliances when they are not in use, or schedule them to turn on during off-peak hours.
- *Smart hot water system*: A system that detects when outside is a sunny day and switches automatically from heating the water with the central gas heater to the solar panels.
- *Water leak detection:* Water damage can be costly and hard to detect. Installing leak detectors in areas prone to water damage, such as bathrooms and basements, can alert occupants to leaks and prevent further damage.

b. one of the use-cases is chosen and the system is defined in detail;

Security monitoring in IoT involves using internet-connected devices, such as sensors and cameras, to identify and respond to security threats in real time. The system analyzes data to detect anomalies in behavior and potential breaches, providing quick detection and response to incidents. There are several ways to integrate IoT into a security monitoring system, including:

- Face-recognition cameras can be used to track who enters and exits the building and send alerts to the owner whenever a new person or one profile configured as being suspicious (wears a mask covering his/hers whole face etc.) is nearby the monitored house. Moreover, the video of the "suspicious" person will be automatically saved in cloud. Some specific faces can be "banned" and trigger a more aggressive reaction, such as a louder siren or even calling the security services.
- The user sets in the security system that no one should be around the house for a particular period. When the movement sensors detect movement, the cameras will automatically start recording and the system will send a message to the owner with the footage in real-time. The user has more options to choose from, such as turning on the lights/playing music/calling the police.
- When more sensors are correlated (pressure sensors in different parts of the yard where no one would have access; motion sensors next to windows or doors that are not particularly used) the security system responds more "aggressively" as follows: the TV and the lights are turned on, the music is turned on, the security services are called.

2. **System definition:**

a. components that enter the system infrastructure;

- Motion sensors
- Pressure sensors
- Cameras with facial recognition
- Receiver
- Smart bulbs
- Smart speakers
- Cloud facility
- Internet gateways
- Mobile application
- Central hub

b. protocols used in communication processes;

- Wi-Fi – it is used for cameras to transmit surveillance footage to a cloud-based server over the internet, mobile applications, central hub;
- Bluetooth - for the smart speakers;
- MQTT (Message Queuing Telemetry Transport) - transmission from sensors to the IoT system;
- Zigbee – used by the smart light bulb.

c. process automation;

There is the complete flow of the use-cases of Security Monitoring System, defined at 1.b.:

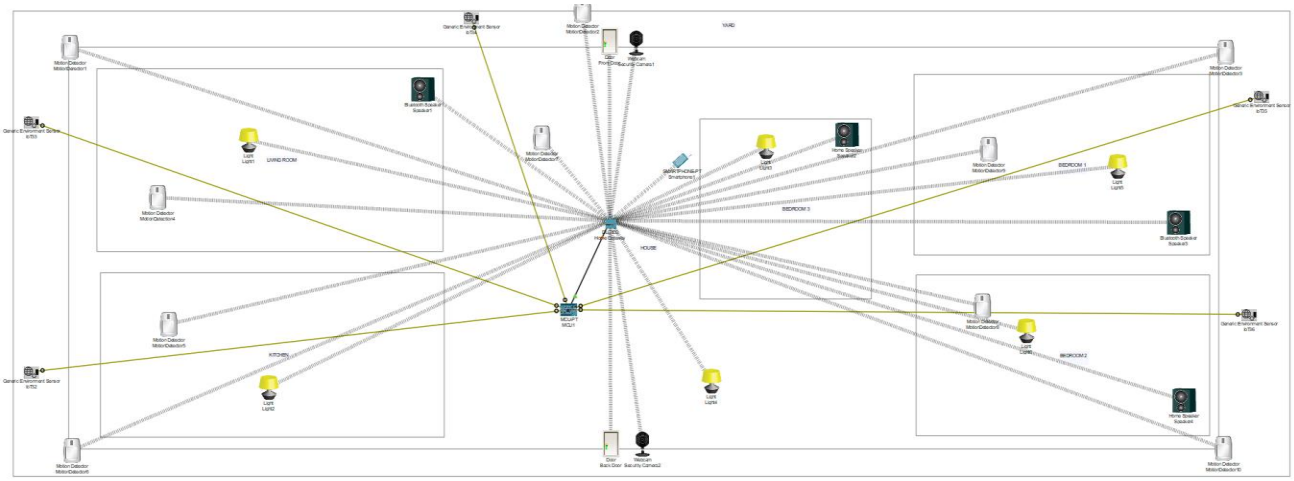
- By using the application, the user can configure some specific details of a person considered to be suspicious. The camera detects people meeting these criteria, and people who have never been seen before around the house, by using computer vision and some advanced machine learning algorithms. Afterwards, it generates an alert, indicating the type (suspicious/unidentified person) and includes additional information, such as the location and time of the event. The user receives the alert on its mobile application, a pop-up with the video in real time and some further actions to take: to turn on the lights, to turn on the TV, play a siren or a specific sound on speakers or call the security services. The command is sent from the client to the server, and afterwards to the central hub which will redirect the command to the other devices like the speakers, the smart bulb via Zigbee or Bluetooth. In addition, the user can add the person involved in the incident to a blacklist, meaning that the next time this specific person is around its house, the security system may have a pre-configured reaction (automatically call the police, without asking for the user's permission)
- The mobile app enables the user to set up the security system to activate the home protection mode once all individuals have left the house and there is no one inside (via motion sensors or by explicitly mentioning that in the app). If the sensors or the cameras detect any movement, the system will process the information in cloud and if the homeowner selects the alerts options in real time, he will be alerted on the mobile application. The flow regarding the alert is the same as above.

- More sensors can be correlated to enhance security, such as pressure sensors deployed in various regions of the yard, those installed at the entry points of the house, motion sensors located around windows of the house, as well as pressure sensors installed on fences. These sensors use the Message Queuing Telemetry Transport (MQTT) protocol to transmit data to the central hub security system, which then alerts the user via a mobile application.

d. estimated costs;

COMPONENT NAME	QUANTITY	DESCRIPTION	UNIT COST	TOTAL
Motion sensors	10	5 outside (at the entrance and at each corner of the house) + 5 (staircase, livingroom, 3 bedrooms)	16.99	169.9
Pressure sensors for door handle	2	2 doors, one in front and one in back	150	300
Pressure sensors for fence	50	in the main spots	23.99	1199.5
Pressure sensors for yard	50	in the main spots(next to the house)	10	500
Cameras with facial recognition + reciver	1	set of 16 cameras	2099.99	2099.99
Smart bulbs	6	Livingroom, 3 bedrooms, 1 kitchen, 1 staircase	4	24
Smart speakers	4	For livingroom, 3 bedrooms	60	240
Mobile application	1	Implemented by us :)	0	0
Central hub	1		23.99	23.99
			TOTAL PRICE $	4557.38

3. **Cisco Packet Tracer:**
    a. **add a print screen of the designed architecture;**



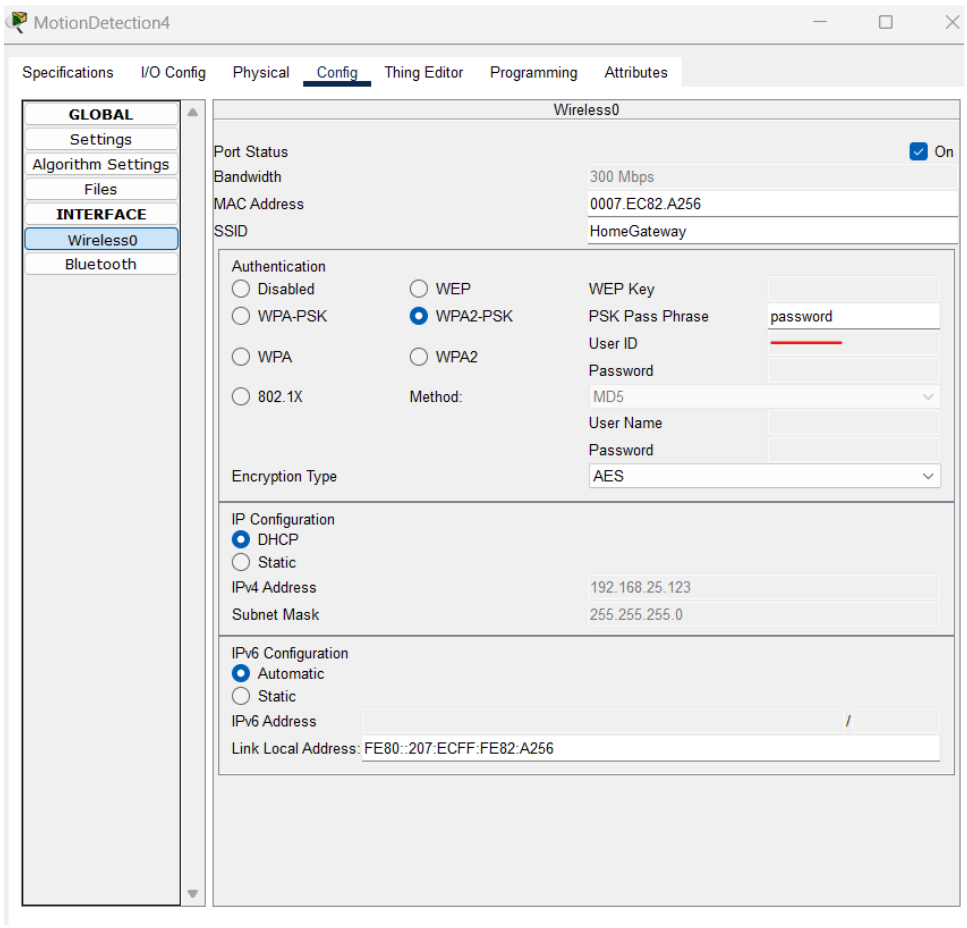
    b. **explain the functionalities implemented in Cisco Packet Tracer;**

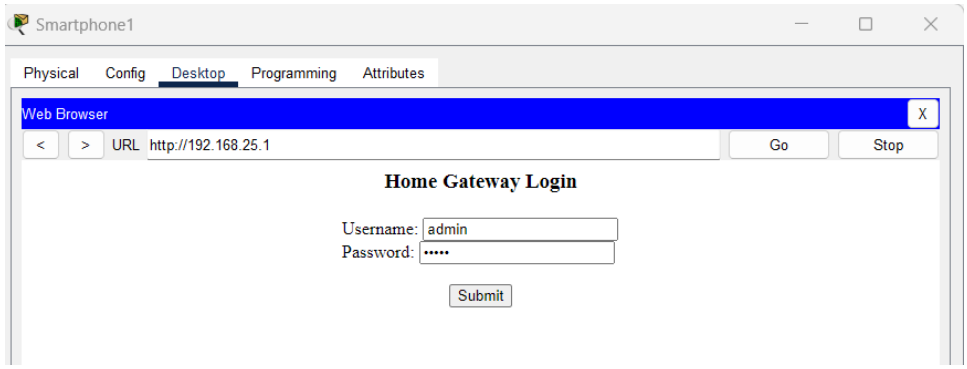
Each square represents a part of the house. The system is designed for a house with three bedrooms, a living room and a kitchen. The IoT components (smart cameras, smart doors, motion sensor, smart lights, smart speakers, pressure sensors as generic sensors) are connected through a central hub. The central hub sends the information via a wireless connection.

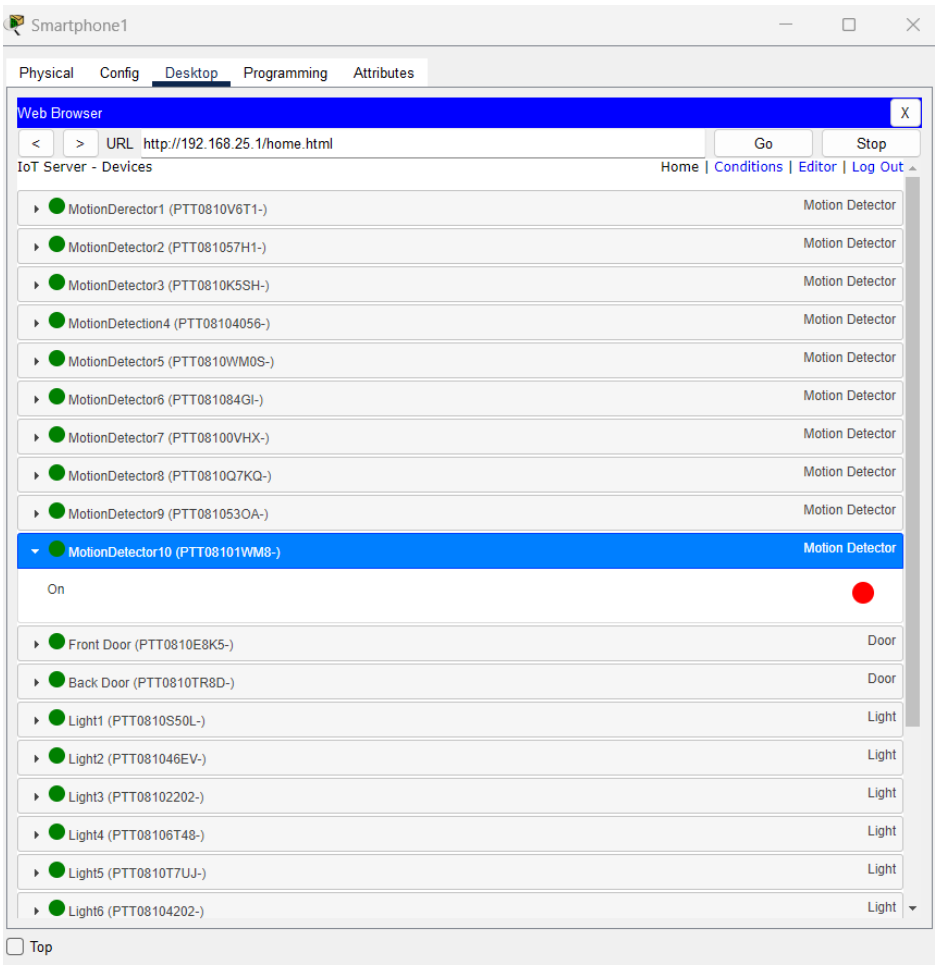
All the IoT elements are using a password to secure the information to the central hub.

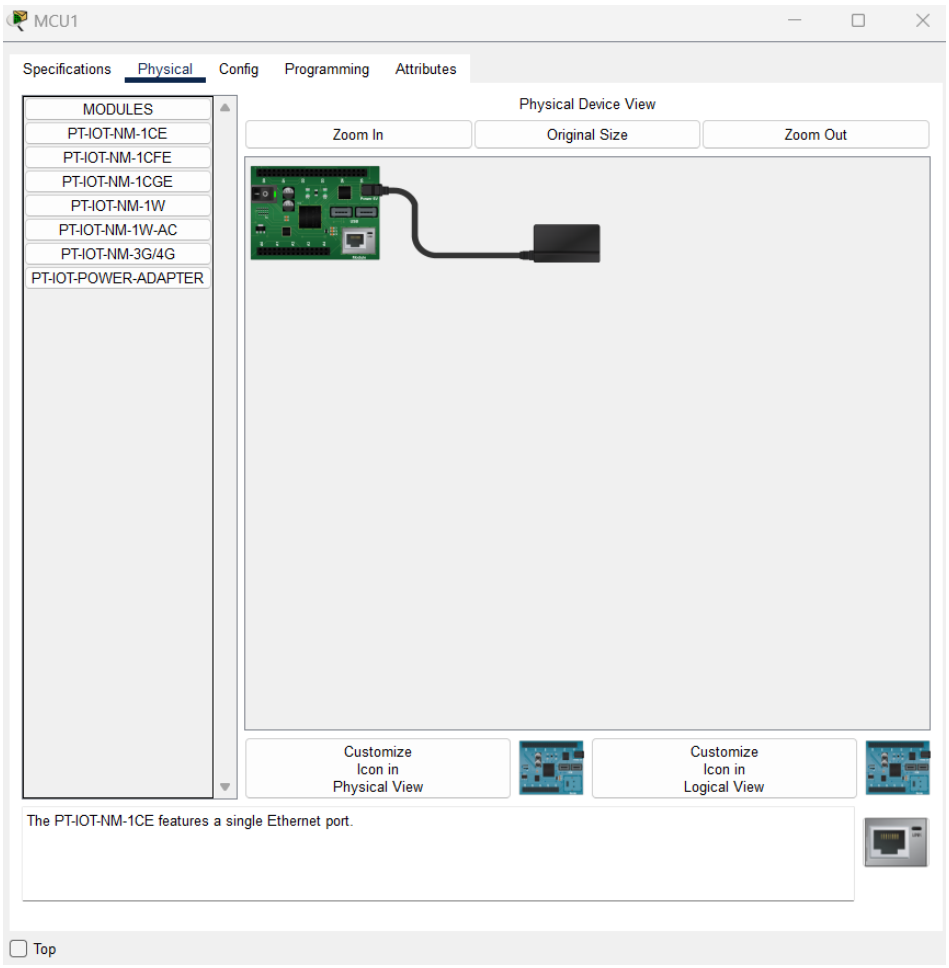
Using the smartphone, the user can configure the central hub and see the connected IoT elements.

The pressure sensors are connected through an MCU which has been modified to have an Ethernet port. The MCU is connected to the central hub.


MotionDetection4
Specifications
I/O Config
Physical
Config
Thing Editor
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
Files
INTERFACE
Wireless0
Bluetooth
Wireless0
Port Status
On
Bandwidth
300 Mbps
MAC Address
0007.EC82.A256
SSID
HomeGateway
Authentication
Disabled
WEP
WPA-PSK
WPA2-PSK
WPA
WPA2
802.1X
Method:
MD5
WEP Key
PSK Pass Phrase
password
User ID
Password
User Name
Password
Encryption Type
AES
IP Configuration
DHCP
Static
IPv4 Address
192.168.25.123
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address:
FE80::207:ECFF:FE82:A256

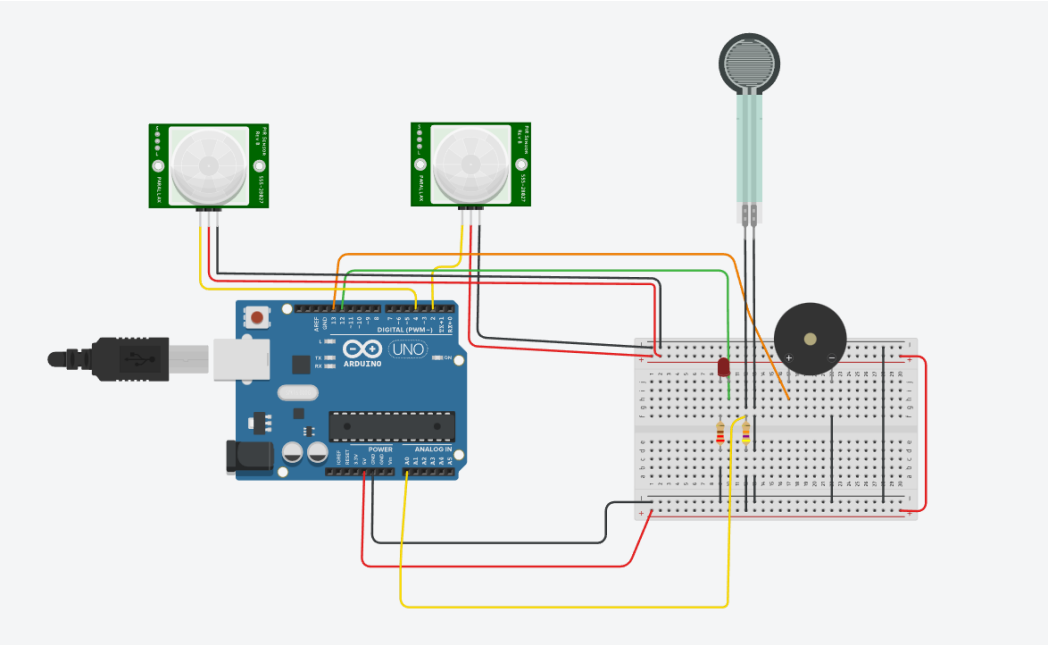

Smartphone1
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.25.1
Go
Stop
Home Gateway Login
Username:
admin
Password:
Submit

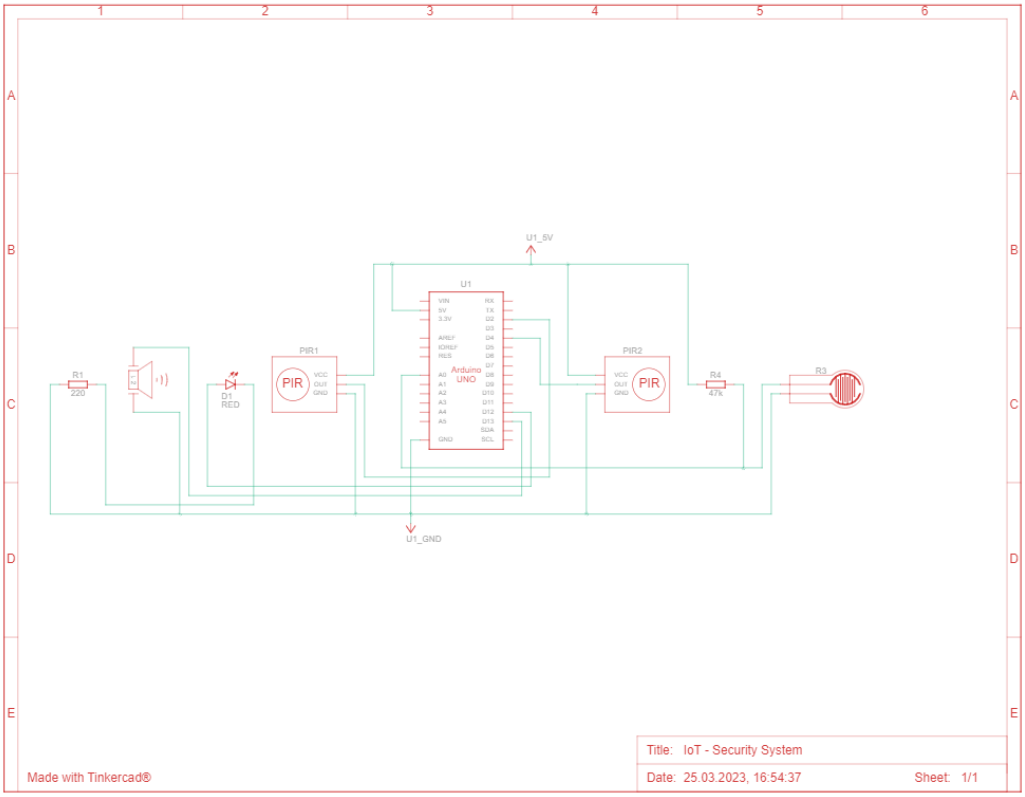

Smartphone1
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.25.1/home.html
Go
Stop
IoT Server - Devices
Home | Conditions | Editor | Log Out
MotionDerector1 (PTT0810V6T1-)
Motion Detector
MotionDetector2 (PTT081057H1-)
Motion Detector
MotionDetector3 (PTT0810K5SH-)
Motion Detector
MotionDetection4 (PTT08104056-)
Motion Detector
MotionDetector5 (PTT0810WM0S-)
Motion Detector
MotionDetector6 (PTT081084GI-)
Motion Detector
MotionDetector7 (PTT08100VHX-)
Motion Detector
MotionDetector8 (PTT0810Q7KQ-)
Motion Detector
MotionDetector9 (PTT081053OA-)
Motion Detector
MotionDetector10 (PTT08101WM8-)
Motion Detector
On
Front Door (PTT0810E8K5-)
Door
Back Door (PTT0810TR8D-)
Door
Light1 (PTT0810S50L-)
Light
Light2 (PTT081046EV-)
Light
Light3 (PTT08102202-)
Light
Light4 (PTT08106T48-)
Light
Light5 (PTT0810T7UJ-)
Light
Light6 (PTT08104202-)
Light
Top


MCU1
Specifications
Physical
Config
Programming
Attributes
MODULES
PT-IOT-NM-1CE
PT-IOT-NM-1CFE
PT-IOT-NM-1CGE
PT-IOT-NM-1W
PT-IOT-NM-1W-AC
PT-IOT-NM-3G/4G
PT-IOT-POWER-ADAPTER
Physical Device View
Zoom In
Original Size
Zoom Out
Customize Icon in Physical View
Customize Icon in Logical View
The PT-IOT-NM-1CE features a single Ethernet port.
Top

4. **TinkerCad:**

a. **add a print screen of the designed architecture;**





Name	Quantity	Component
U1	1	Arduino Uno R3
PIR1	1	24.71243767132131 , -144.12048086799518 , -206.51977675894608 PIR Sensor
D1	1	Red LED
PIEZO1	1	Piezo
R1	1	220 Ω Resistor
PIR2	1	18.1874848703755 , -170.78532315529208 , -170.78532315529208 PIR Sensor
R3	1	Force Sensor
R4	1	47 kΩ Resistor

b. explain the functionalities implemented in TinkerCad.

Our system contains an Arduino Uno R3 microcontroller board, a breadboard, a resistor, 2 motion sensors – one considered to be inside the house, and the other one, outside, a force sensor, a red led and a piezo buzzer, used for making a sound. If the outside motion sensor detects a movement, while the one from the inside does not detects anything (no one is inside the house) and the force sensor exceeds a certain limit, the light will turn on and the piezo buzzer will make a sound, otherwise nothing happens.

```
int pinSensorOutside = 2;
int pinSensorInside = 4;
int pinLed = 12;
int pinBuzzer = 13;
int pirSensorOutside = 0;
int pirSensorInside = 0;
int forcesense = 0;

void setup()
{
  Serial.begin(9600);
  pinMode(pinSensorOutside, INPUT);
  pinMode(pinSensorInside, INPUT);
  pinMode(A0, INPUT);
  pinMode(pinLed, OUTPUT);
  pinMode(pinBuzzer, OUTPUT);
}

void loop()
{
  pirSensorOutside = digitalRead(pinSensorOutside);
  pirSensorInside = digitalRead(pinSensorInside);
  forcesense = analogRead(A0);
  Serial.println(forcesense);
  if (pirSensorOutside == HIGH && pirSensorInside == LOW && forcesense>50)
  {

     digitalWrite(pinLed, HIGH);
     tone(pinBuzzer, 1000, 500);
  }
  else {
      digitalWrite(pinLed, LOW);
  }
  delay(10);
}
```