Systems Architecture and Internet of Things

Mini project

C. Dilsara Sandun Chandrapala

2439254

Lecturers

University of Wolverhampton

Mr. Darshana Hettiarachchi

CINEC Campus

Development of Internet of Things Project for sensing, controlling, adjusting and performing functional scenario remotely with secure channel.

Table of Contents

Figures

1. Introduction

The Internet of Things (IoT) has completely transformed the way devices interact and communicate, opening the door to creative solutions in a number of areas, including smart homes. The project, A smart home IoT system prototype was selected for design and construction. The project goal is to "develop an Internet of Things project to sense, control, configure, and execute remote action scenarios over a secure channel." The system will integrate contemporary sensing, control, and automation capabilities to provide a seamless and user-friendly experience, supported by global control and secure access. The project will develop an Internet of Things smart home system by simulating the hardware and network environment using Cisco Packet Tracer. The system will have a secure communication path to ensure secure data exchange between pre-configured control modules, microcontroller unit (MCU)-controlled components, and devices. To protect data security and prevent unauthorized access to the system, a secure communication channel must be established. By using Cisco Packet Tracer to simulate the network, the study will show how IoT devices can operate in a coordinated and secure manner.. This document outlines the project development process, including the design, simulation, and evaluation of a smart home Internet of Things system. The project results demonstrate how the Internet of Things can improve the energy efficiency, convenience, and security of smart homes.

You should develop a smart home IoT system (sensing, controlling, adjusting, performing functions) that uses global control using secure access and mcu controlled components as well as predefined control modules.

1. Project Scenario

My firm specializes in providing IoT infrastructure and setup services for both private houses and businesses as an IOT-system service provider. In order to satisfy each client's particular demands, we provide both package-based deals and tailored solutions. Planning, setting up, installing, and maintaining the smart home infrastructure are all included in our service. The design and deployment of an IoT-enabled smart home system for residential property is the main emphasis of the IoT solution we are providing in this project. The customer lives in a two-story home with several rooms in the basement.

1.1 Project's Purpose, Scope, and Objectives

The project's goal is to create and deploy an Internet of Things (IoT) smart home system that provides remote control, efficiency, security, convenience, and real-time monitoring. It entails connecting several IoT devices around the house to provide a safe, intuitive environment for remote administration and automation. Based on predetermined characteristics, the system will allow automation, real-time monitoring, and control of household appliances.

1. A Setup and program (home components) to sense and actuate based on defined variables and add the details to the report

Current designed of Smart home

My building plan states that the design reflects the architecture of the smart home I want to develop. Along with the main gate, the smart home is divided into other areas such as a living room, kitchen, garage, workshop, storage room, and other spaces. The front view has been the primary focus of the concept of this design. I will describe each piece in detail below, along with the building materials that went into making it.

Client's Requirements

Motion Sensor-enabled Windows, Light and Fan Control:

- Windows will be equipped with motion sensors that will help detect activity and control.
- Motion sensor enabled and controlled system for home appliances in designated areas.

Existing Appliances:

- The client has specified that only the existing appliances will be used in the IoT system. No additional appliances will be added at first, but the system should be expandable in the future to add new appliances.

Smoke Detection System with Auto Unlock Door Feature in fire hazards:

- A smoke detection system will be added only specified areas where there is a potential fire risk.
- When smoke detection system triggers, the system should automatically unlock all the doors in the house to evacuate residents.

System Architecture and Function.

Living Room Ground floor and bathroom

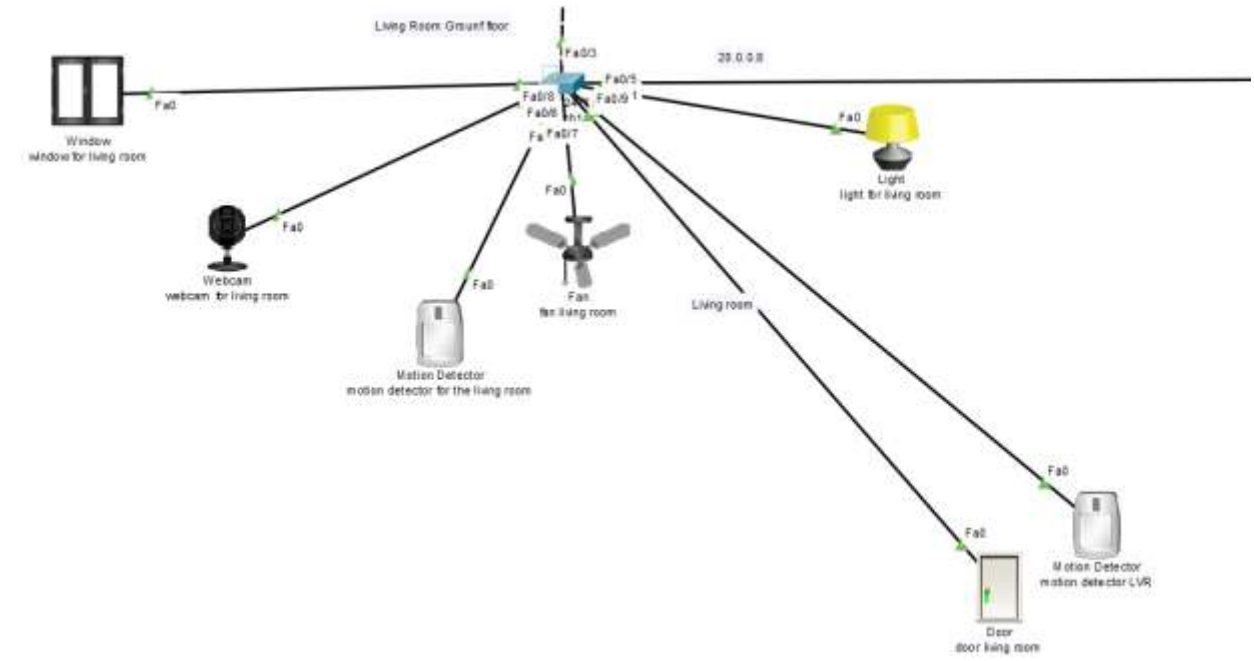


Figure 1

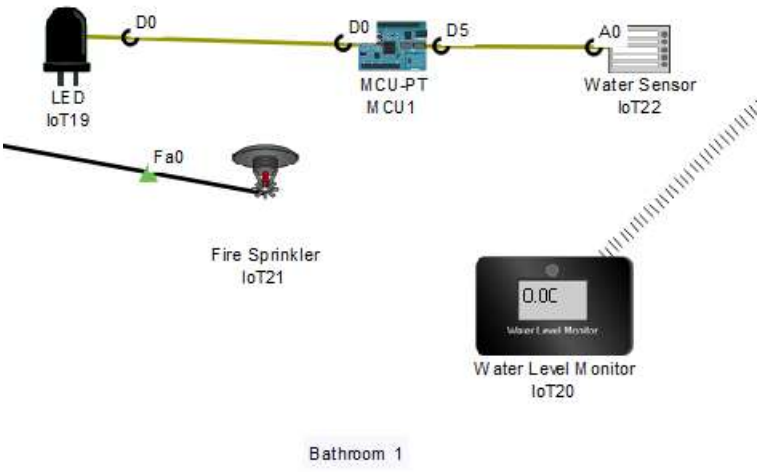


Figure 2

With IoT-enabled components to monitor, control, and automate various tasks, this configuration exemplifies a smart living room setup. The components and their functions are shown below:

1. Central switch

To connect multiple sensor devices in the living space, a centralized switch is installed. These include a camera, window, fan, lamp, door, and motion detectors, all of which are directly connected to the switch. Effective data exchange, routing, and remote access are achieved through this setup. Notably, the gadgets are directly connected to the switch, bypassing the home entrance, allowing for seamless management and communication within the living space.

2. Sensors

Motion Detectors:

In this configuration, two motion detectors are installed. One is placed near the door to watch for movement, and the other is placed near the window to watch for movement. These detectors provide data on motion detection rates and the amount of motion detected. Authorized users can monitor real-time motion detection trends by logging in remotely.

MCU Board and water level monitors and water sensors.

The water sensor measures the water level in the bathroom and is connected to the A0 pin of the MCU. The MCU processes the data to see if a high water level, which could cause flooding or overflow, is above a predetermined threshold. When the water level is above the threshold, an alarm mechanism is triggered; when the water level is normal, the LED light remains off. The MCU can regulate the water drain to lower the water level and stop the overflow if necessary. Using the water sensor, the MCU continuously checks the water levels and provides real-time system updates.

Webcam

The device, which can record live video feeds via motion detection or user instructions, is thoughtfully positioned throughout the living room for security and surveillance reasons.

3. Actuators

The smart light in the living room adjusts its state (on or off) based on motion detection or person-defined schedules. Similarly, the smart ceiling fan operates entirely based on predefined conditions, including room temperature or specific person commands.

To enhance security and automate access to control, the smart door is easily connected to a motion detector and has sensors to detect openings and closings. The device also includes a dummy smart window that can be used to remotely manipulate the airflow or enhance security as needed. Via fast Ethernet connections, the network setup connects each component to the corresponding router. Thanks to the router's specific IP address, the device's capabilities can be accessed safely and reliably.

Functionalities

A camera watches the living room and records video when activated, and the system uses motion detectors to detect movement and trigger automatic reactions. Fans and lighting fixtures can be managed manually or automatically using the remote control. Pre-set modules can be activated, including "night mode" and "welcome mode". To protect against unwanted access and ensure statistical confidentiality, the device uses secure communication protocols.

2. Bed room 1 floor and bath room

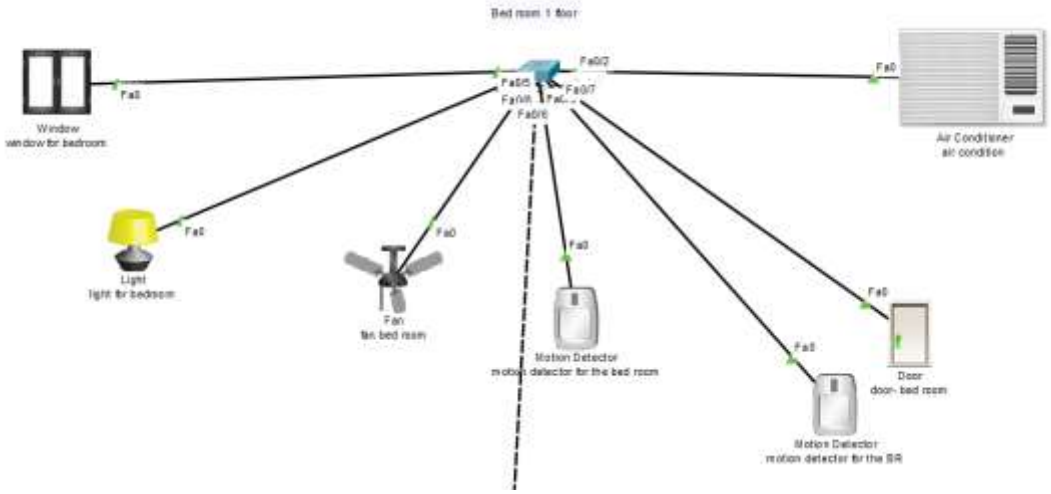


Figure 3

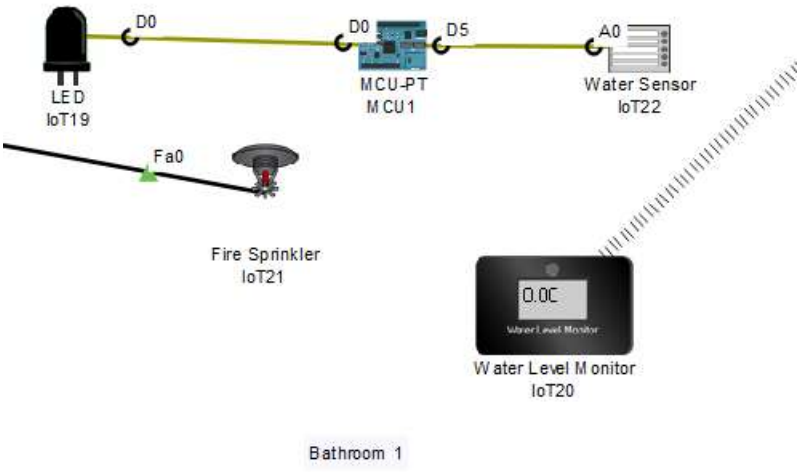


Figure 4

The following section offers tips on how to configure a smart bedroom to increase energy efficiency, comfort, and security. A primary router controls a network of linked IoT devices and accessories. Below are the specifics of each one:

1. Central switch

To connect multiple sensor devices in the living space, a centralized switch is installed. These include a camera, window, fan, lamp, door, and motion detectors, all of which are directly connected to the switch. Effective data exchange, routing, and remote access are achieved through this setup. In particular, the devices are directly connected to the switch, bypassing the home entrance, allowing for seamless management and communication within the living space.

2. Sensors

Motion Detectors:

In this configuration, two motion detectors are installed. One is placed near the door to watch for movement, and the other is placed near the window to watch for movement. These detectors provide data on motion detection rates and the amount of motion detected. Authorized users can monitor real-time motion detection trends by logging in remotely.

MCU Board and water level monitors and water sensors.

The water sensor measures the water level in the bathroom and is connected to the A0 pin of the MCU. The MCU processes the data to see if a high water level, which could cause flooding or overflow, is above a predetermined threshold. When the water level is above the threshold, an alarm mechanism is triggered; when the water level is normal, the LED light remains off. The MCU can regulate the water drain to lower the water level and stop the overflow if necessary. Using the water sensor, the MCU continuously checks the water levels and provides real-time system updates.

3. Actuators

A smart lamp in the house acts to movement or user-defined schedules by changing its state from start to finish. Similar to this, a smart ceiling air conditioner follows predetermined settings, such as the surrounding temperature or specific user commands, to work step-by-step.

A smart door features sensors to monitor entry and exit and may be readily connected to a motion detector to improve security and automate access to control. In addition, the gadget has a fictitious smart window that can be used to remotely adjust the air conditioning or add decorations to the security system as desired. The network configuration links all of the parts to a central router via Fast Ethernet cables. Up to the router's unique IP address, the device's functionality may be reliably and securely accessed.

.

- Also this is connect with Living room main switch.

Functionalities

The system includes motion detection to optimize the performance of lighting and fans. The air conditioner is programmed to turn on when it senses movement, which helps maintain comfort and reduce unnecessary use. Furthermore, the motion detector built into the door enhances security by keeping an eye on door activity. The technology uses very little energy, as it only turns on when movement is detected. In addition, it offers remote and secure control capabilities over a robust, encrypted network, ensuring reliable and secure access to all connected devices.

Working Room first floor

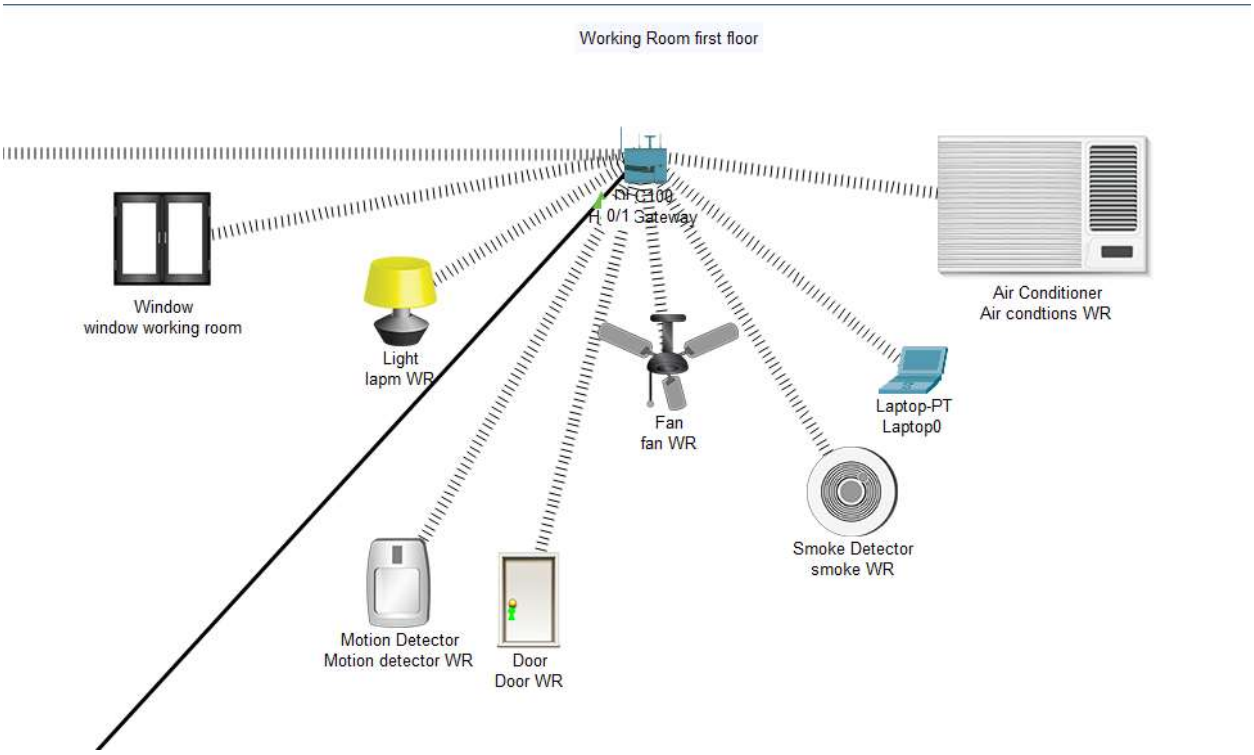


Figure 5

1. Central gateway

A central gateway in a smart workspace is an essential hub that makes it easy for connected sensors and devices to communicate and control each other. It maintains security by monitoring entry points, activating alarm systems, and managing security cameras. It organizes equipment, ensuring smooth operation. To make judgments or send alerts, the gateway collects and analyzes data from sensors including motion, light, temperature, and humidity. Additionally, it enables remote access control, allowing users to monitor activity or manage devices from a web interface or mobile app.

2. Sensors

Motion Detectors: (IoT14 & IoT16)

In this configuration, two motion detectors are installed. One is placed near the door to watch for movement, and the other is placed near the window to watch for movement. These detectors provide data on motion detection rates and the amount of motion detected. Authorized users can monitor real-time motion detection trends by logging in remotely.

Smoke Detector (IoT18):

With features such as emergency alarms, activation of ventilation systems, automatic door control in the event of a fire, and fire safety monitoring, the goal is to detect smoke and monitor air quality.

3. Actuators

The smart light in the working room adjusts its state (on or off) based on motion detection or user-defined schedules. Similarly, the smart ceiling fan operates according to predefined conditions, such as room temperature or specific user commands.

The smart door is equipped with sensors to detect opening and closing and is seamlessly integrated with a motion detector to increase security and automate access control. Additionally, a simulated Smart Window is included in the setup, which can be used to remotely manage ventilation or enhance security as needed. The network configuration connects all components to a home gateway via Bluetooth and home gateway is connected to switch. This router is assigned a unique IP address, enabling secure and reliable access to the system's functionality.

System Integration Activities

Motion detection, door control, emergency procedures, energy management, comfort control, automatic climate control, lighting control, and air quality management are all features of the security system. Smoke detection, emergency lighting, automatic door control, and remote control for status checks and changes via mobile devices are examples of security features.

Kitchen room

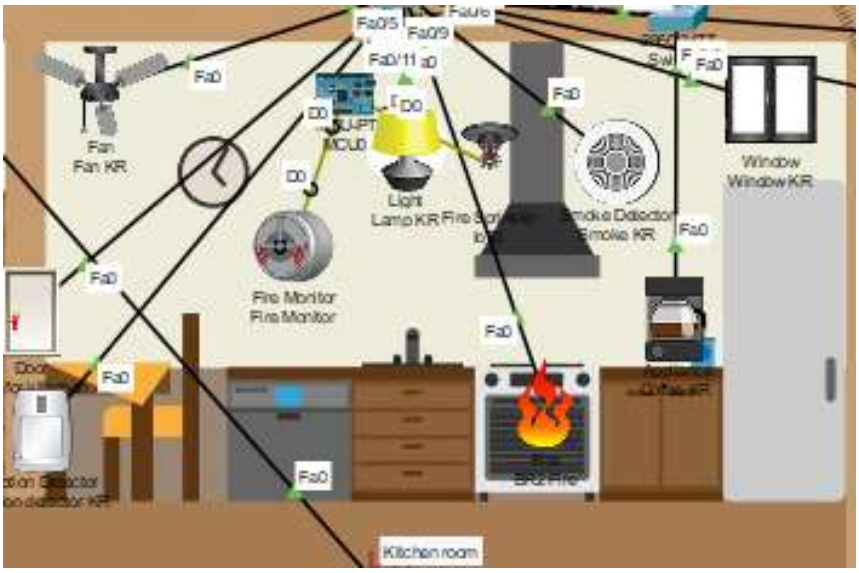


Figure 6

A Cisco 2960 switch acts as the heart of this smart home kitchen. This switch connects directly to each IoT device. The segments, sensor types, and possible uses are divided as follows:

Components and Sensor Types

1. Central switch

To connect multiple sensor devices in the kitchen space and a centralized switch is installed. These include a, window, fan, door, smoke detector, coffee and motion detectors, all of which are directly connected to the switch. Effective data exchange, routing, and remote access are achieved through this setup. Notably, the gadgets are directly connected to the switch, bypassing the home entrance, allowing for seamless management and communication within the garage space.

2. Sensors

Motion Detectors: (IoT14 & IoT16)

In this configuration, two motion detectors are installed. One is placed near the door to watch for movement, and the other is placed near the window to watch for movement. These detectors provide data on motion detection rates and the amount of motion detected. Authorized users can monitor real-time motion detection trends by logging in remotely.

Smoke Detector (IoT18):

With features such as emergency alarms, activation of ventilation systems, automatic door control in the event of a fire, and fire safety monitoring, the goal is to detect smoke and monitor air quality.

3. Actuators

The smart light in the kitchen adjusts its state (on or off) based on motion detection or user-defined schedules. Similarly, the smart ceiling fan operates according to predefined conditions, such as room temperature or specific user commands.

The smart door is equipped with sensors to detect opening and closing and is seamlessly integrated with a motion detector to increase security and automate access control. Additionally, a simulated Smart Window is included in the setup, which can be used to remotely manage ventilation or enhance security as needed. The network configuration connects all components to a switch via Fast Ethernet ports. This router is assigned a unique IP address, enabling secure and reliable access to the system's functionality. Also there are coffee machine for the kitchen.

Potential Functionalities and Scenarios:

A security system that includes door/window sensors, a motion detector, and a smoke detector can alert homeowners to intruders. When someone enters the kitchen, the motion detector can turn on the lights, and when the door is closed, the door sensor can turn off the fan. Through an IoT7 network, the homeowner can turn on the fan and appliances remotely—perhaps with the help of a smartphone app. More complex scenarios, such as a morning routine or a mode that arms the security system and turns off lights and appliances when the house is empty, can be implemented through predefined control modules.

Garage

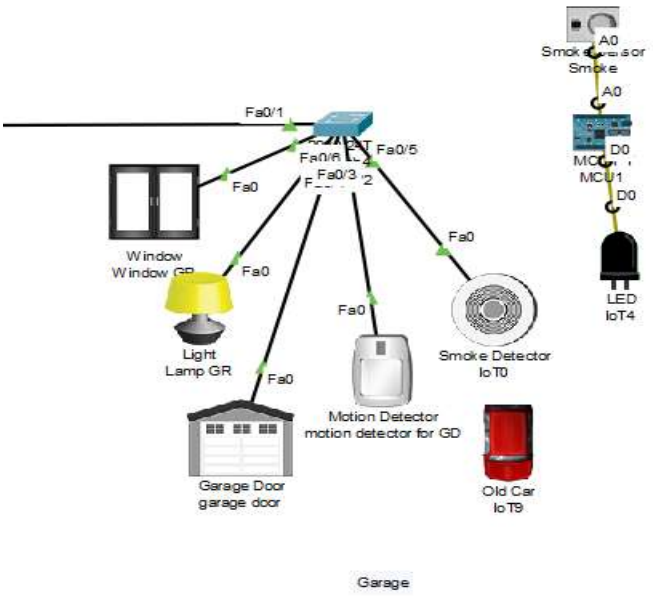


Figure 7

A simple IoT smart home garage with sensors and actuators connected to a central switch is shown in the above mentioned figure. These components are used to monitor and manage various parts of a smart home. The sensors in the system, their responsibilities, and their functional activities are described in detail below.

1. Central switch

To connect multiple sensor devices in the garage space and a centralized switch is installed. These include a, window, fan, door, smoke detector, car and motion detectors, all of which are directly connected to the switch. Effective data exchange, routing, and remote access are achieved through this setup. Notably, the gadgets are directly connected to the switch, bypassing the home entrance, allowing for seamless management and communication within the kitchen space.

2. Sensors

Motion Detectors:

In this configuration, two motion detectors are installed. One is placed near the door to watch for movement, and the other is placed near the window to watch for movement. These detectors provide data on motion detection rates and the amount of motion detected. Authorized users can monitor real-time motion detection trends by logging in remotely.

Smoke Detector

With features such as emergency alarms, activation of ventilation systems, automatic door control in the event of a fire, and fire safety monitoring, the goal is to detect smoke and monitor air quality.

Window

By detecting whether the window is open or closed, the window sensor provides security by alerting the system in the event that the window is opened unexpectedly. To maximize energy use, it can cooperate with heating or air conditioning systems or set alarms.

Garage Door Sensor

The garage door provides real-time information about the movement and status of the car by keeping an eye on its presence and status. It also improves the security of the garage by detecting illegal vehicle activity and sending alerts or notifications in case of suspicious activity. To regulate access and maximize space efficiency, the gadget also provides information about garage usage trends. It ensures the safety and security of the vehicle.

MCU Board

MC board has used to detect the smoke volume in this smart home. In the programmed used to read the value of the smoke sensor attached to the A0 pin of the MCU. The setup () method ensures real-time monitoring of smoke levels by attaching an interrupt to the A0 pin. The smoke level is evaluated by the process Data () function, which indicates a high smoke hazard and takes appropriate action if it exceeds the threshold. If the level is below the threshold, it reflects normal conditions. The MCU's digital pin D0 controls the LED light, which turns on or off in response to the amount of smoke present. When smoke levels are high, the system sends a diagnostic alarm by logging a message to the console.

Front of house

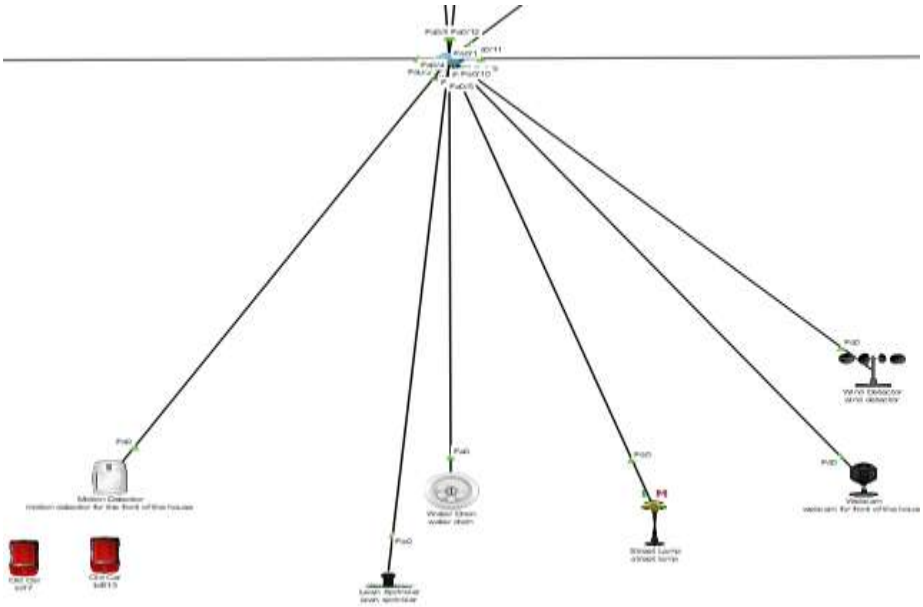


Figure 8

Here is an IoT smart home system centered on the front of the house. For automation, control, and monitoring, it consists of sensors, actuators, and Internet of Things devices connected through a central switch. A description of the purpose and functionality of each device can be found below.

1. Central switch

To connect multiple sensor devices in the garage space and a centralized switch is installed. These include a, lawn sprinkler, motion detector for the front of the house, water drain, street lamp, car, wind detector and webcam for front of the house, all of which are directly connected to the switch. Effective data exchange, routing, and remote access are achieved through this setup. Notably, the gadgets are directly connected to the switch, bypassing the home entrance.

2. Sensors

Car Sensors

The device allows real-time monitoring of driveway or entryway activity by monitoring the presence and status of cars in front of a property. It helps homeowners monitor parking behavior by confirming the presence of parked or moving vehicles. It improves home security by detecting unauthorized vehicle movement and sending notifications for possible intrusions or suspicious activity if a vehicle enters or exits without permission.

Lawn Sprinkler

By automating watering, the smart home system's lawn sprinkler saves water and reduces human labor. Water waste can be minimized by programming it to water at specific times. In addition, it can be connected to environmental sensors to stop watering when the wind is high. This function promotes sustainable water consumption habits in addition to maintaining the health of the lawn. The system would be further enhanced by incorporating soil moisture sensors to adjust watering schedules based on the amount of moisture in the soil.

Water Drain

The "Water Drain" device in my smart home is intended to monitor and manage the water drainage systems in front of the house. Its main purpose is to prevent waterlogging that may occur during heavy rain or flooding, ensuring that water flows properly through the drainage system.

Street Lamp

The street light in your smart home system is intended to illuminate the front of your home to improve safety and visibility at night or in low light. Convenience and energy efficiency are provided by the ability to configure it to turn on automatically when motion is detected or at specific times. You can ensure that the light only turns on when it is needed and avoid wasteful energy use by integrating it with additional sensors such as motion detectors. This technology maximizes energy use while contributing to a safe home environment.

Wind Detector

The wind sensor measures wind direction and speed, providing real-time environmental data to improve outdoor systems such as street lighting and lawn sprinklers. In high winds, it automatically turns off sprinklers to conserve water and ensure efficient use. In addition to helping smart home systems make informed decisions, wind data can be used to activate or change other home appliances, increase energy efficiency, and cut down on unnecessary outdoor system activity.

Web Cam

An essential part of video monitoring in my smart home is the webcam located in the front room. It continuously monitors the property by recording the front area in real time. By integrating the webcam with the motion detection system, proactive security monitoring may be achieved by having the camera begin recording or sending warnings automatically when movement is detected. This function makes sure that any odd behavior is captured right away, allowing you to watch the video remotely and keep track of my property's security condition. By providing a live video stream and improving general situational awareness, the webcam offers an additional degree of security.

Server area and store room

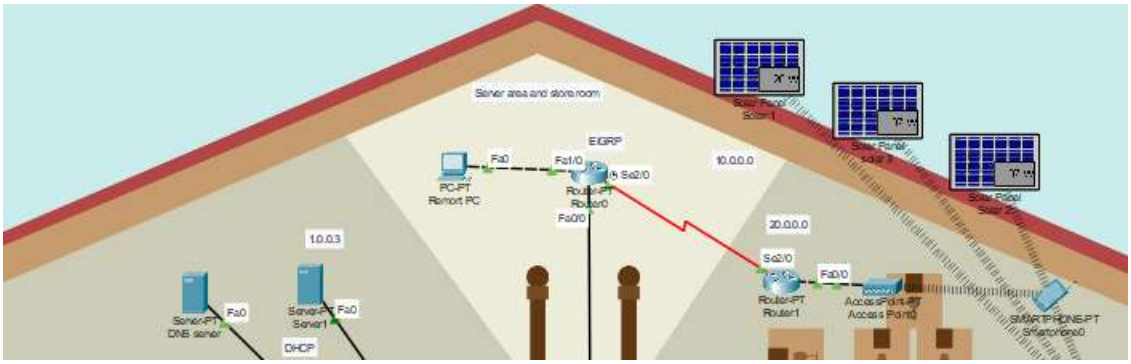


Figure 9

To support smart home architecture, this part of your IoT system acts as the server area and storage room where essential network services and connectivity components are installed. The components are divided as follows:

DNS Server

To facilitate smooth communication between networked devices, this server is in charge of translating domain names into IP addresses. It is assigned the IP address 1.0.0.3 and is connected via the Fa0 interface. Also, this server is working as a backup server; if the main DHCP server fails, all IoT devices can be connected to this server.

DHCP Server:

This server ensures effective and automated IP administration by dynamically allocating IP addresses to networked devices. To distribute IP configurations to connected devices, it is connected via the Fa0 interface. This server is mainly working as an IoT server. All the IoT devices are connected to this server.

Router 1:

EIGRP (Enhanced Interior Gateway Routing Protocol) is configured on Router-PT to facilitate efficient subnet routing. It is responsible for routing traffic between the local network and external devices and is connected to the switch via the Se2/0 serial interface.

Access Point (AccessPoint-PT):

Smartphones and other mobile devices can connect to the network thanks to the wireless connection of the access point. It extends the network coverage wirelessly and is connected to the Fa0 port of the router.

Remote PC

In addition to being a data processing unit that allows for local processing of sensor data, the remote computer also acts as a monitoring station that regulates the smart home's IoT devices, a control center, and an access point for remote users. It is capable of evaluating sensor data,

Full Building plan

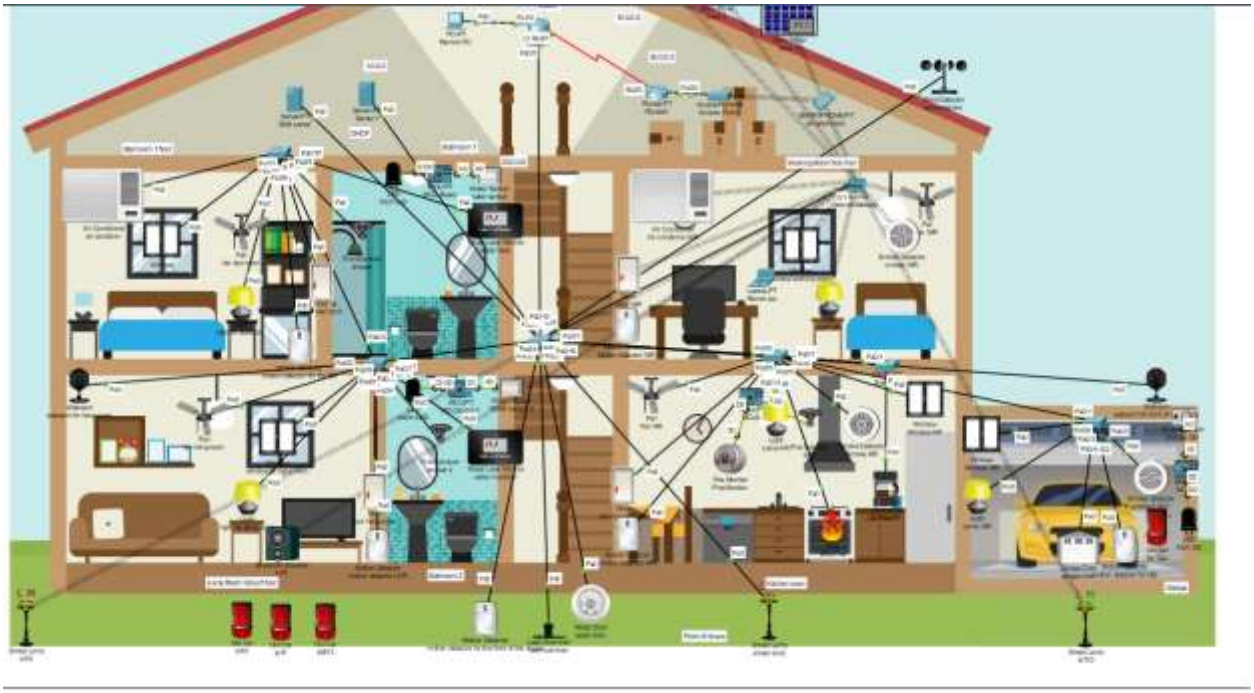


Figure 10

2. Demonstrate how the components interact with the environment by configuring Different actions.

Home automation is building automation for a home, called a smart home or smart house. Home automation systems will control lighting and appliances. It also include home security such as access control and alarm systems when connected with the Internet, home devices are an important constituent of the Internet of Things.

Objectives

There will be automation in a smart house. Our smart house can improve security and ease of living. It can also save time and energy. We attached an autonomous webcam to the house, which keeps an eye on everything constantly. Additionally, the most the key is that the owner can use his smartphone to enter the residence from anywhere in the globe.

Tools:

- Server
- Access Pointer
- Router
- Smartphone
- IOT Device: webcam, street lamp, fan, light, coffee maker, sensor, etc.
- Motion Detector
- Switch
- Lawn Sprinkler
- Water Drain
- Wind Detector Smart Car
- Air Conditioner
- LED Light
- MCU board
- solar panel
- fire monitor
- laptops
- PC
- Cars

Implementation Details

Taking server, IOT devices, routers, switches, smart phone, wires etc. for Making IOT – Smart Home. In this task I'll connect every router. The routers and switches will then be connected. After that, we'll link every switch, and every switch will connect to every IOT device, home device, server, smartphone, and laptop.

Server configurations

Interface	IP Address	Subnet Mask	Network Address
Fa0 (DNS Server)	**1.0.0.13**	**255.0.0.0**	**1.0.0.0**
Fa0 (DHCP Server)	**1.1.1.3**	**255.0.0.0**	**1.1.1.0**
Fa1/0 (Router1)	**192.168.1.1**	**255.255.255.0**	**192.168.1.0**
Se2/0 (Router1)	**10.0.0.1**	**255.255.0.0**	**10.0.0.0**
Se2/0 (Router2)	**10.0.0.2**	**255.255.0.0**	**10.0.0.0**
Fa0/0 (Router2)	**20.0.0.1**	**255.255.0.0**	**20.0.0.0**
Fa0 (Access Point)	**20.0.0.8**	**255.255.0.0**	**20.0.0.0**

Now we will configure router 1 for giving dynamic ip address by using DHCP protocol.

```
ip dhcp pool 10network
 network 1.0.0.0 255.0.0.0
 default-router 1.1.1.1
 dns-server 1.1.1.2
ip dhcp pool 20network
 network 10.0.0.0 255.0.0.0
 default-router 20.0.0.1
 dns-server 10.0.0.2
ip dhcp pool PC-Network
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 1.1.1.2
```

Figure 11

Now we will configure router 2 for giving dynamic ip address by using DHCP protocol.

```
.
ip dhcp pool 30network
 network 10.0.0.0 255.0.0.0
 default-router 10.0.0.1
 dns-server 10.0.0.2
!
```

Figure 12

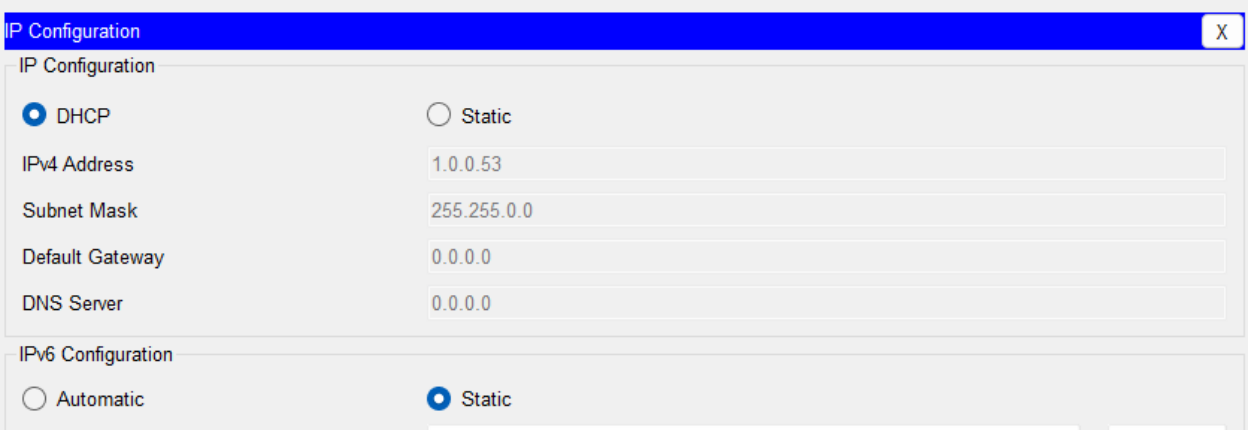


Figure 13

Configure the EIGRP protocol

Now we will configure routing protocol EIGRP in router 1 and 2 so that owner of the house can access my home from anywhere in the world over the internet by using his smart phone.

```
.
router eigrp 1
 network 1.0.0.0
 network 10.0.0.0
 network 192.168.1.0
 auto-summary
!
```

Figure 14

```
!
router eigrp 1
 network 10.0.0.0
 network 20.0.0.0
 auto-summary
!
```

Figure 15

Router 1 interfaces

```
Wellcome Router 1

User Access Verification

Password:
Password:

Router1>en
Password:
Router1#sh
Router1#show ip
Router1#show ip in
Router1#show ip interface br
Router1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        1.1.1.1         YES NVRAM  up                    up
FastEthernet1/0        192.168.1.1     YES NVRAM  up                    up
Serial2/0              10.0.0.1        YES NVRAM  up                    up
Serial3/0              unassigned      YES NVRAM  administratively down down
FastEthernet4/0        unassigned      YES NVRAM  administratively down down
FastEthernet5/0        unassigned      YES NVRAM  administratively down down
FastEthernet6/0        unassigned      YES unset  up                    down
Router1#Router1#
```

Figure 16

Router 2 interfaces

```
Well come to router 2

User Access Verification

Password:
Password:

Router>en
Password:
Router#sh
Router#show ip
Router#show ip int
Router#show ip interface br
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        20.0.0.1        YES manual up                    up
FastEthernet1/0        unassigned      YES manual up                    down
Serial2/0              10.0.0.2        YES manual up                    up
Serial3/0              unassigned      YES unset  administratively down down
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
Router#
```

Figure 17

Smart phone accessing the server by using EIGRP routing protocol in figure 15.

Figure 18

For the Routing, I have use Rip method.

```
router eigrp 1
 network 1.0.0.0
 network 10.0.0.0
 network 192.168.1.0
 auto-summary
!
```

Figure 19

Connectivity of device

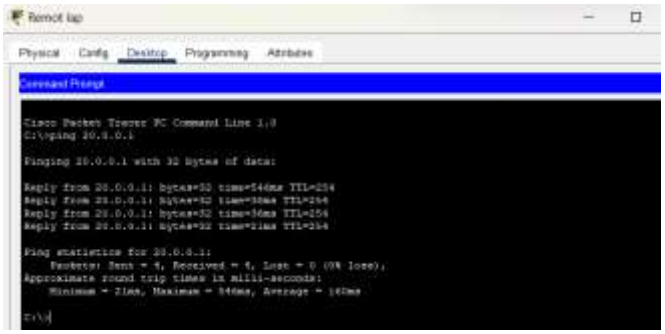


Figure 20-lap top Router2

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=38ms TTL=255
Reply from 10.0.0.1: bytes=32 time=37ms TTL=255
Reply from 10.0.0.1: bytes=32 time=45ms TTL=255
Reply from 10.0.0.1: bytes=32 time=27ms TTL=255

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 45ms, Average = 36ms

C:\>
```

Figure 21-laptop to router 2

```
C:\>ping 1.1.1.3

Pinging 1.1.1.3 with 32 bytes of data:

Reply from 1.1.1.3: bytes=32 time=71ms TTL=128
Reply from 1.1.1.3: bytes=32 time=31ms TTL=128
Reply from 1.1.1.3: bytes=32 time=42ms TTL=128
Reply from 1.1.1.3: bytes=32 time=46ms TTL=128

Ping statistics for 1.1.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 71ms, Average = 47ms

C:\>
```

Figure 22-laptop to IOT server

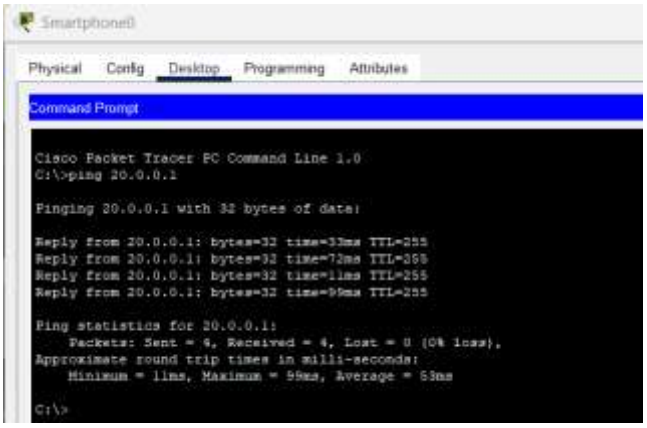


Figure 23-Smart phone to router

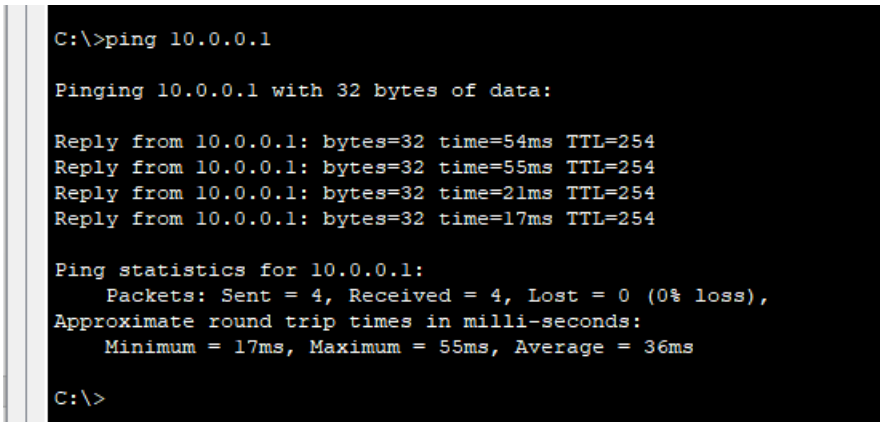


Figure 24-smart phone to router 2

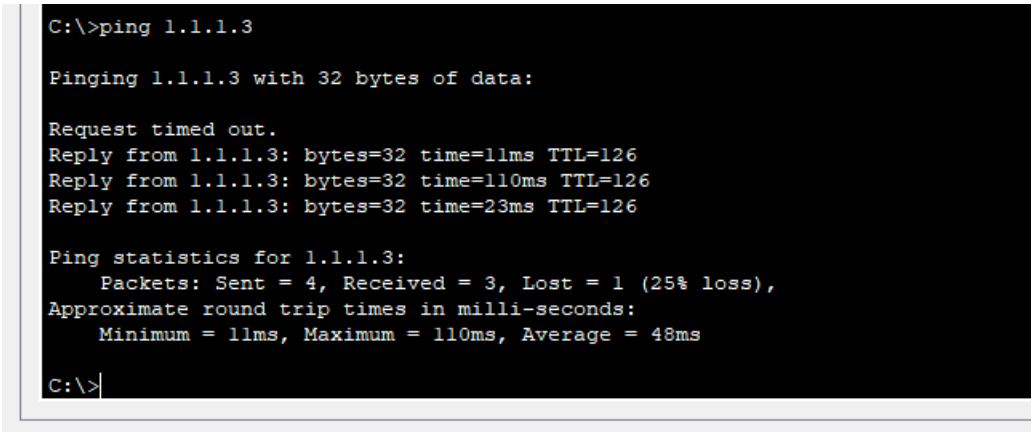


Figure 25-smart phone to IOT server

Password and IOT device connection

Now we will register an account in the server for connecting all the IoT devices/home devices by giving a user name & password.

Figure 26

Smart phone accessing the home by sign in to the server

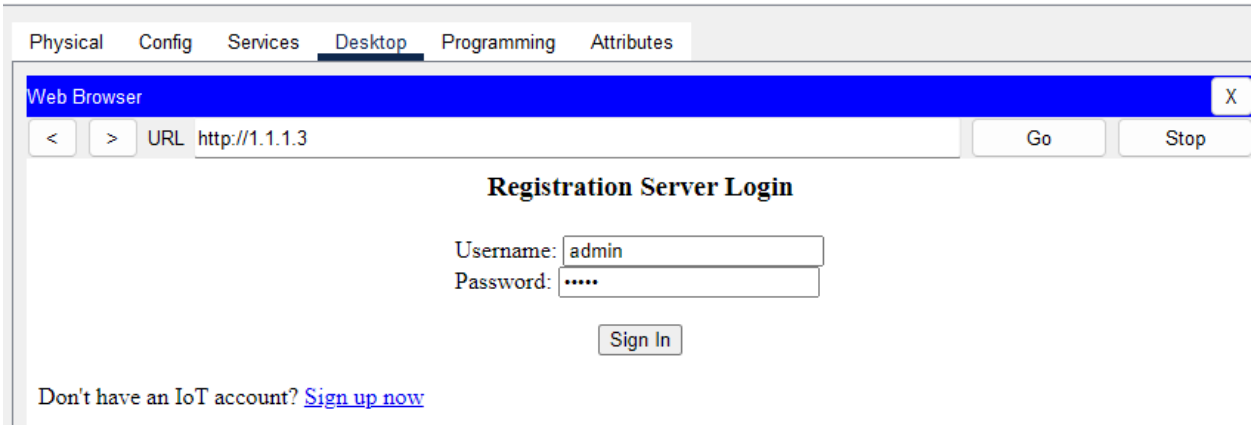


Figure 27

After sign in to the server by using smart phone.

Figure 28

This figure shows all the IoT sensors and devices connected to the IoT network. In addition, there are several IoT devices that can be accessed and monitored. It is also possible to view and control everything from a smartphone.

IOT Device connect to the main server

Bedroom

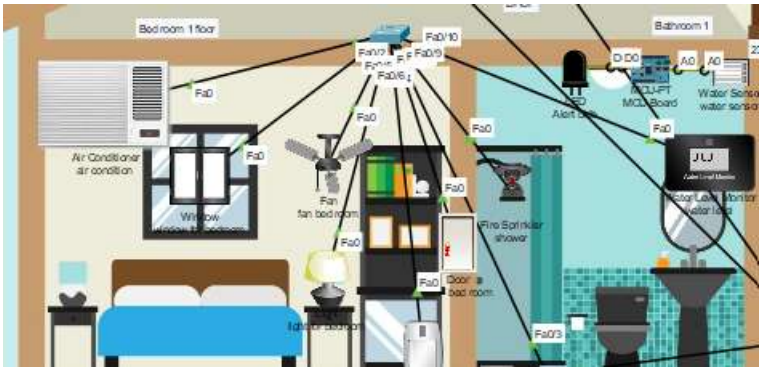


Figure 29

This section illustrates a smart bedroom setup that is intended to improve energy efficiency, comfort, and security. A central router controls a network of interconnected IoT devices and components. The specifics of each component are as follows:

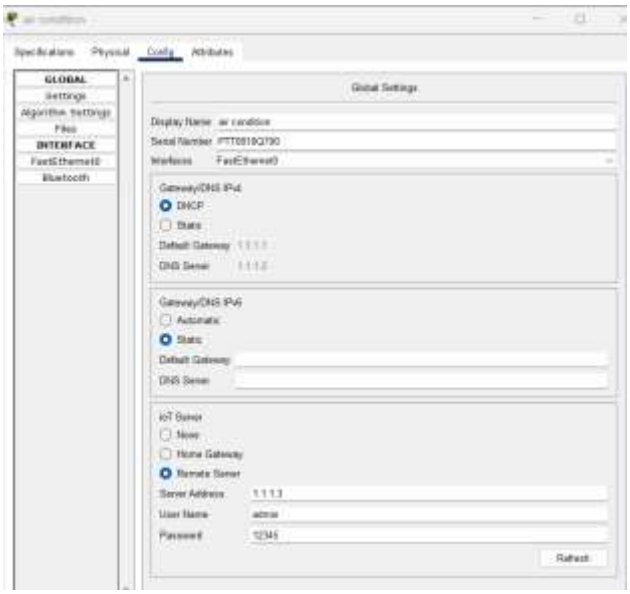


Figure 30-widow bedroom

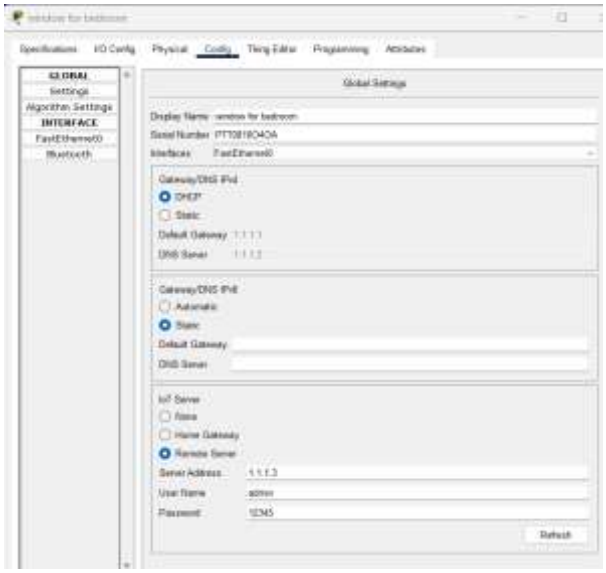


Figure 22-window bedroom

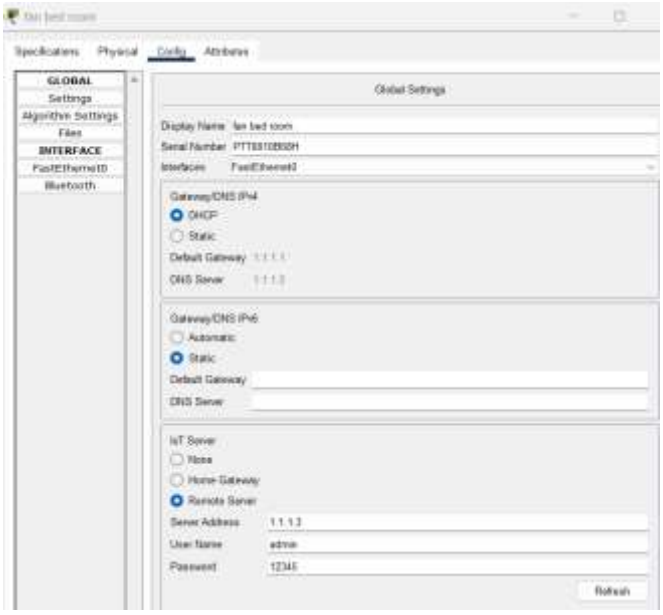


Figure 23- fan bedroom

As shown, all IoT devices are connected to this central server. These images are used as an example. Everything is installed and connected to the distribution.

At the first point all the IOT device will stay in turn off.

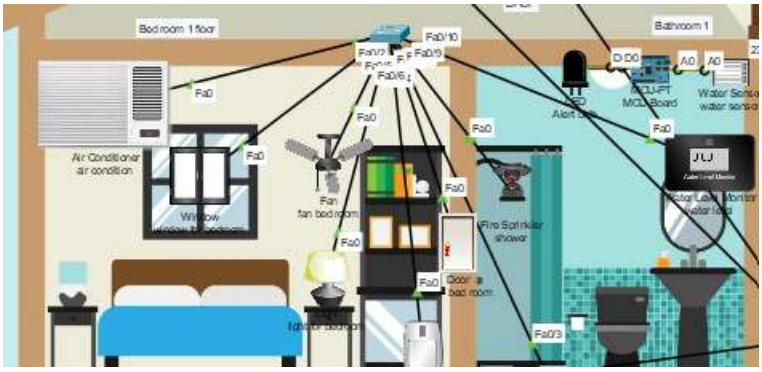


Figure 24

When there is movement in front of the living room door, the door opens automatically. After entering the room, the light, fan, and window turn on.

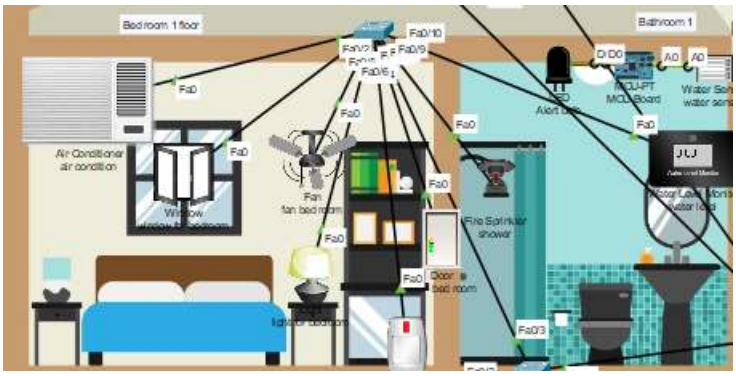
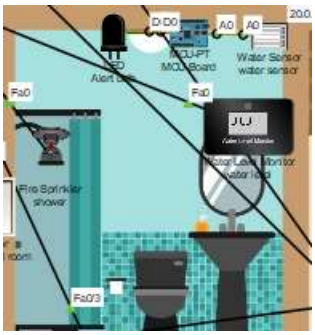
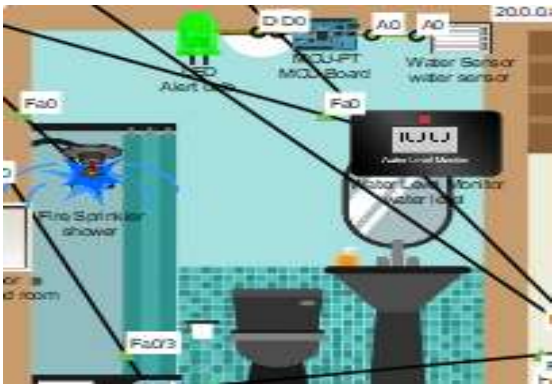


Figure 31

At the first point all the IOT device will stay in turn off in bathroom



If someone forgets to turn off the shower while using the bathroom, a motorized level monitor will detect if the water level has exceeded the appropriate level, and a bulb will light up via the MCU board.



Sensor conditions

Edit Remove	Yes	Motion BD	motion detector for the BR On is true	Set window for bedroom On to true Set light for bedroom Status to On Set door- bed room Lock to Unlock Set air condition On to false Set fan bed room Status to High
Edit Remove	Yes	No Motion BD	motion detector for the BR On is false	Set window for bedroom On to false Set door- bed room Lock to Lock Set light for bedroom Status to Off Set air condition On to true Set fan bed room Status to Off

MCU Board configuration.

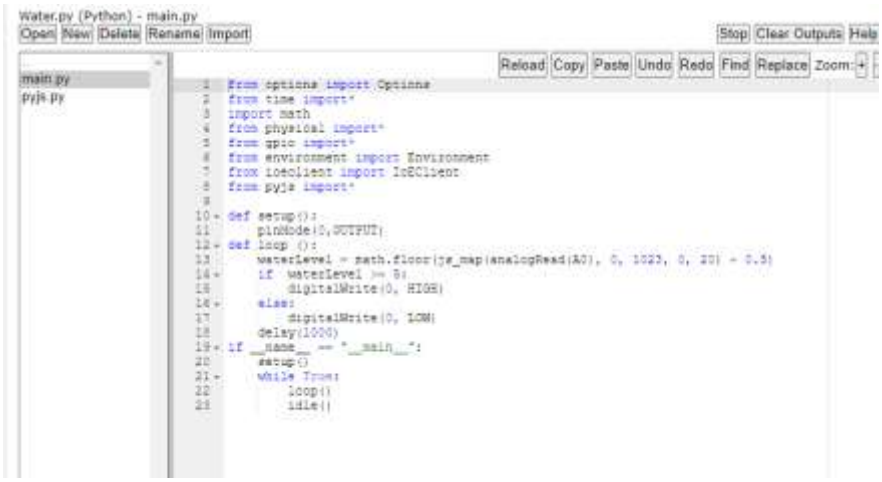


Figure 32

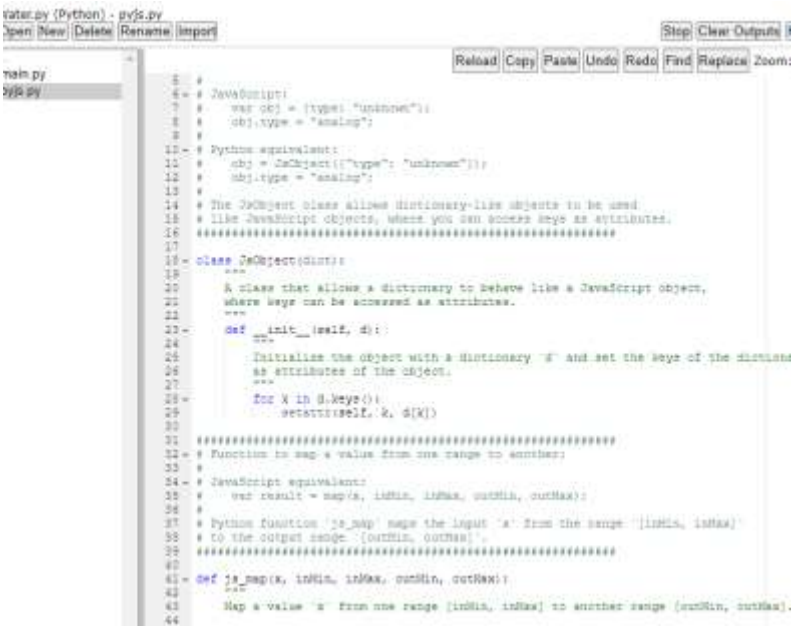
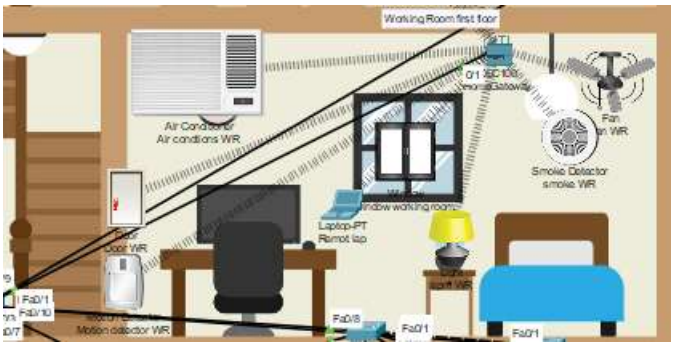


Figure 33

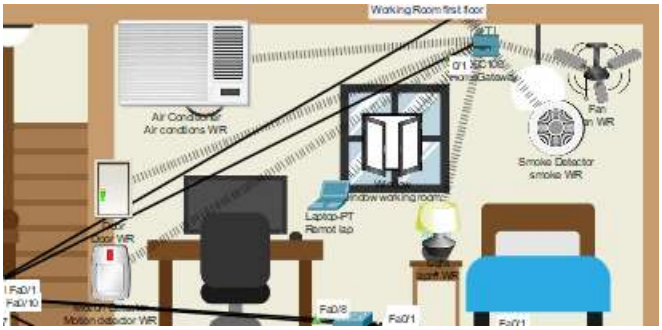
The Python script shows how to set up and run an MCU board that monitors water levels and controls an output device using a water level sensor. It communicates with the input and output pins of the MCU using libraries such as GPIO, math, and PyJS. GPIO pin 0 is configured as an output pin with the pinMode(0, OUTPUT) pin setting. AnalogRead(A0) is used to read the water level from the sensor's analog input (A0). The control logic is configured to turn the connected device on or off depending on the water level, and the js_map function translates the sensor value into a meaningful range. Before moving on to the next iteration, the software pauses for 1000 milliseconds.

Working Room first floor

At the first point all the IOT device will stay in turn off.



When there is movement in front of the living room door, the door opens automatically. After entering the room, the light, fan, and window turn on.

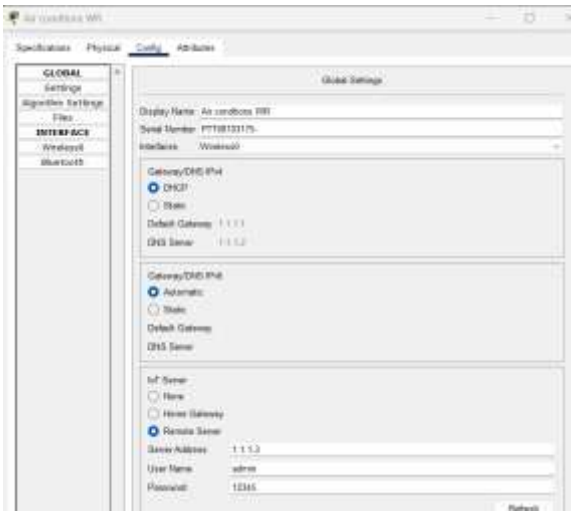


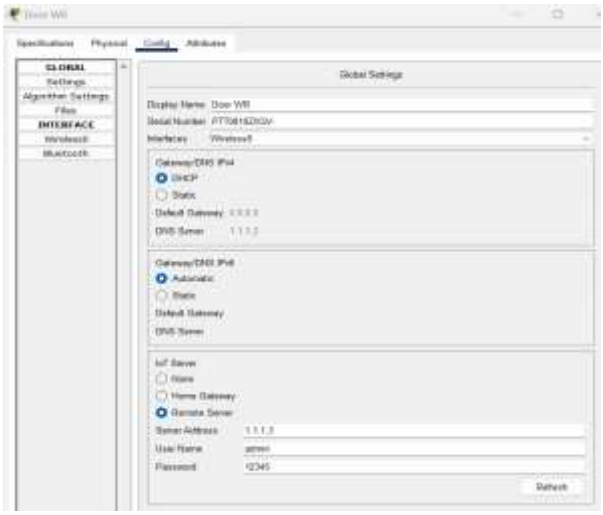
Sensor condition

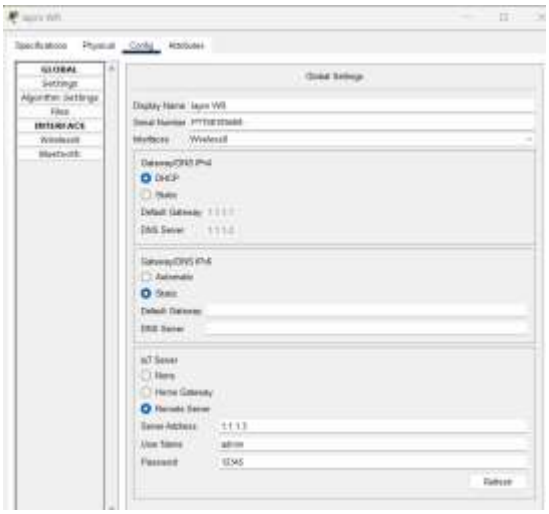
Edit Remove	Yes	Motion WR	Motion detector WR On is true	Set window working room On to true Set Air condtions WR On to false Set fan WR Status to High Set lapm WR Status to On Set Door WR Lock to Unlock
Edit Remove	Yes	No motion WR	Motion detector WR On is false	Set window working room On to false Set lapm WR Status to Off Set Door WR Lock to Lock Set Air condtions WR On to true Set fan WR Status to Off

Figure 34

IOT device connection to IOT server.







In this, lap top can be access the IOT server.

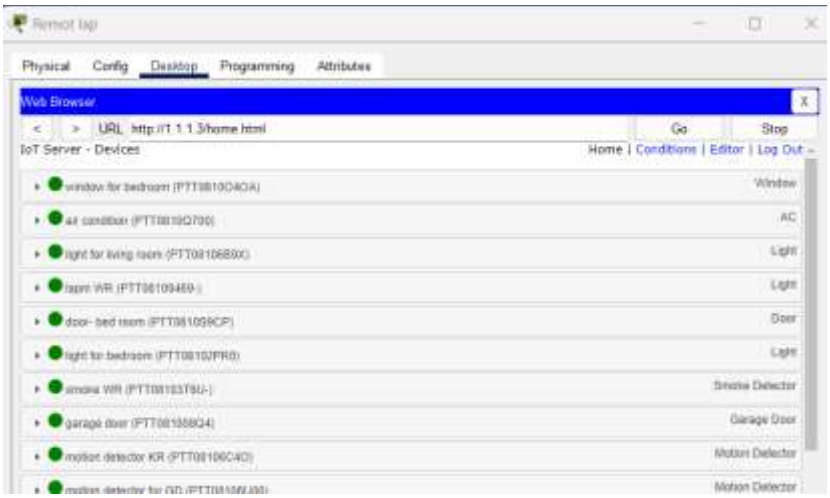


Figure 35

In this specially all devise are connected to central gateway. A central gateway in a smart workspace is an essential hub that makes it easy for connected sensors and devices to communicate and control each other. It maintains security by monitoring entry points, activating alarm systems, and managing security cameras. It organizes equipment, ensuring smooth operation. To make judgments or send alerts, the gateway collects and analyzes data from sensors including motion, light, temperature, and humidity. Additionally, it enables remote access control, allowing users to monitor activity or manage devices from a web interface or mobile app.

Living room

Initially all things are off

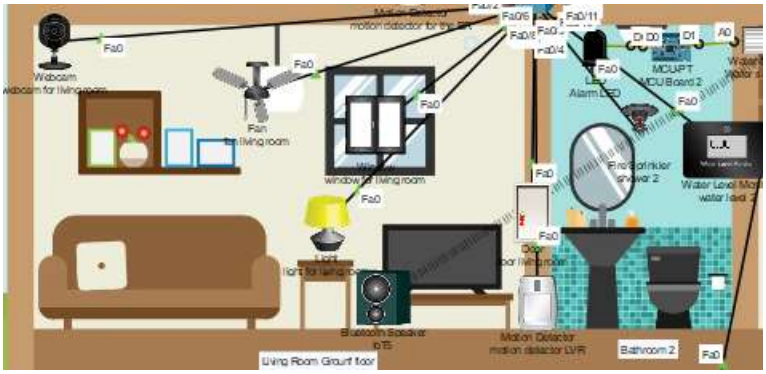


Figure 36-

When the motion happens in front of the door of the living room, the door itself is open automatically. After entering the room, the light, fan, webcam, and window will run. If it is needed, then the user can control the light and fan by his smartphone. When we are out of the room, the lamp, fan, window, and webcam will then turn off themselves.

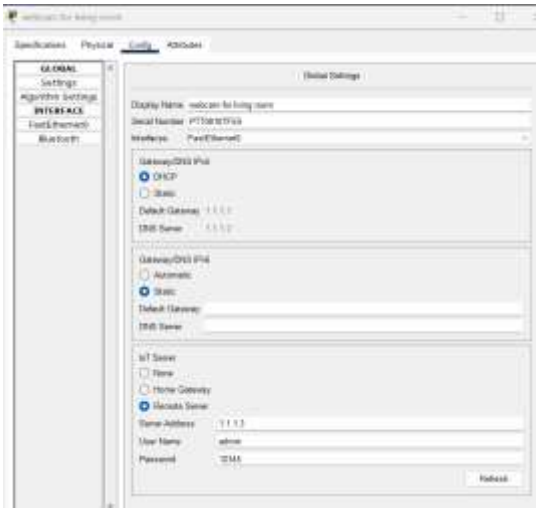
Figure 37- living room fan, light, webcam is running and window is open

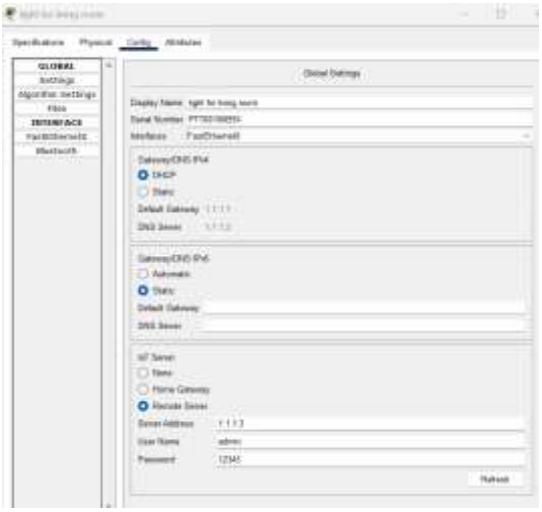
Sensor condition

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Motion LR	motion detector LVR On is true	Set window for living room On to true Set webcam for living room On to true Set fan living room Status to High Set door living room Lock to Unlock Set light for living room Status to On
Edit Remove	Yes	No Motion LR	motion detector LVR On is false	Set door living room Lock to Lock Set webcam for living room On to false Set light for living room Status to Off Set fan living room Status to Off Set window for living room On to false

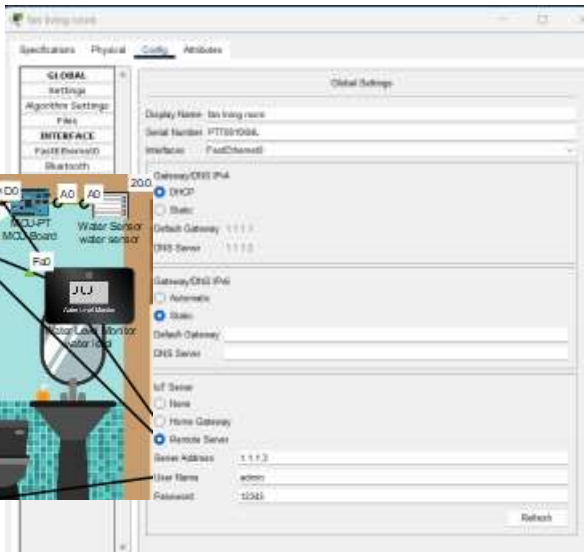
Figure 38

Sensor connection to IOT server





At the first point all the IOT device will stay in turn off in bathroom



If someone forgets to turn off the shower while using the bathroom, a motorized level monitor will detect if the water level has exceeded the appropriate level, and a bulb will light up via the MCU board.

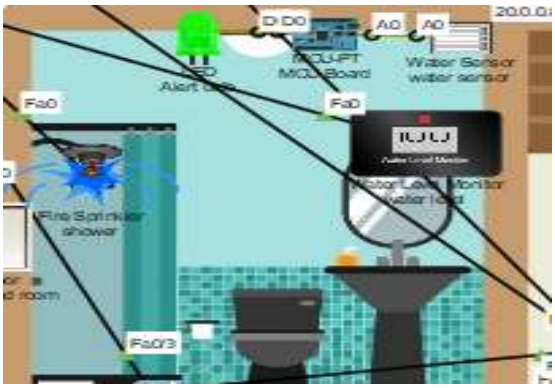


Figure 39

Kitchen

As other rooms kitchen door will open itself. And after entering the kitchen Coffee maker and other IOT device will turn on as well.

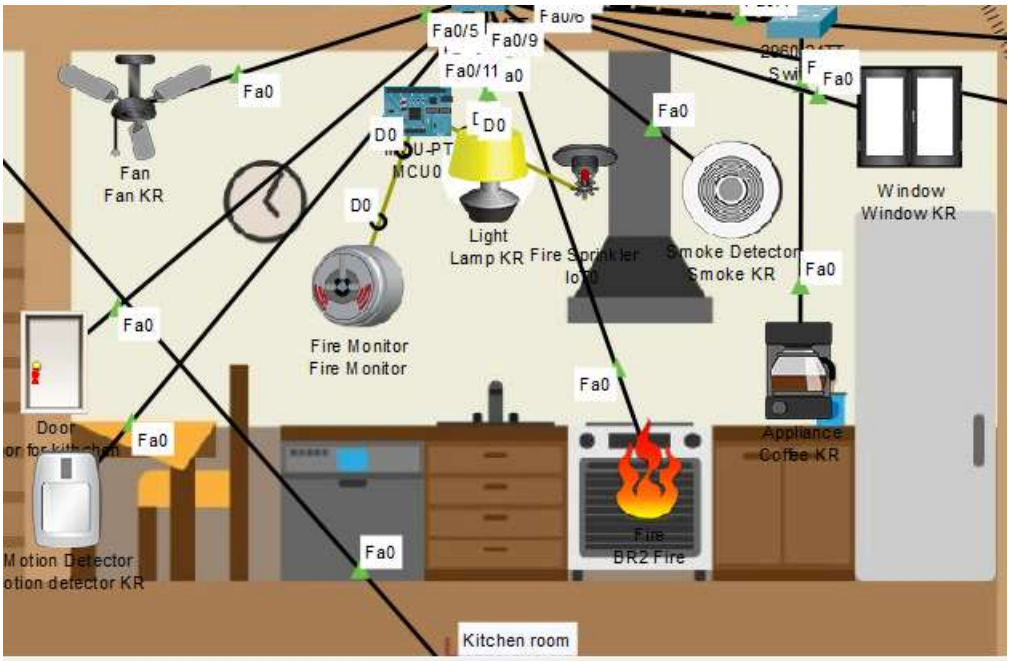


Figure 40

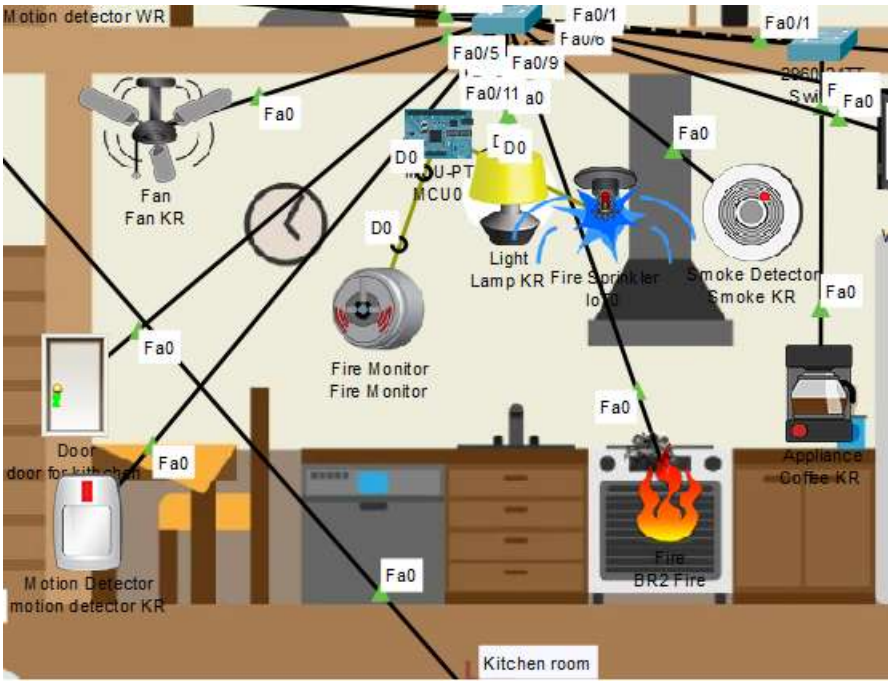


Figure 41

MCU Board configuration in kitchen

Figure 42

When a fire is detected in the kitchen, the Python code uses the GPIO capability to handle the fire detection and initiate essential actions such as turning on the lights and spraying water. Let me correct your description and explain the code:

GPIO pin 0 is connected to a fire sensor, which detects a flame or fire. If no fire is detected, the lights and sprinklers are turned off. When a fire is detected, they are turned on. The handleSensorData method is called when GPIO pin 0 changes, which are monitored by the add_event_detect function. Every second, the software checks the sensor input while running endlessly. Some of the key features include instant sprinkler activation, visual alerts for real-time status updates, IoT-based remote control and monitoring, and automated fire safety actions.

To enhance automation and safety, more appliances and sensors have been added to the smart kitchen. Motion detection and a fire monitor in the kitchen trigger the system to immediately start a water sprinkler if a fire or flame is detected. The water sprinkler system automatically reacts and extinguishes the fire as it develops. Other appliances respond simultaneously, and the corresponding indicator lights will show the current status. This feature, which enables users to remotely monitor and operate their appliances, illustrates the modern Internet of Things (IoT) capabilities in the smart home.

Garage

If the car stays In front of the door of the garage, the garage door will open itself. Also In an IoT system, the microcontroller unit (MCU) board is responsible for monitoring the amount of smoke detected by a smoke sensor and managing the LED lighting in response to the sensor data. The GetSensorData () function retrieves the analog value from the smoke sensor and converts it to a percentage scale. The smoke sensor is connected to the analog input pin of the MCU. The setup () method ensures real-time monitoring of smoke levels by connecting an interrupt to the A0 pin. The smoke level is evaluated by the process Data () function, which indicates a high smoke hazard and takes appropriate action if it exceeds a threshold. When smoke levels are high, the system logs a message to the console and the MCU's digital pin D0 controls the LED lighting.

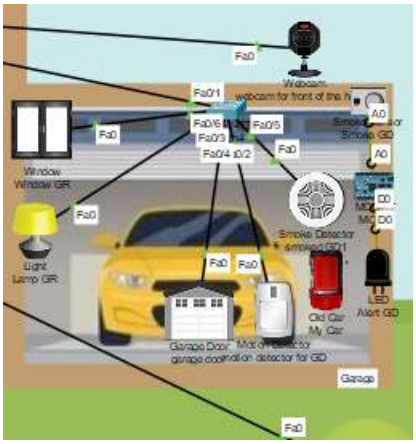


Figure 43

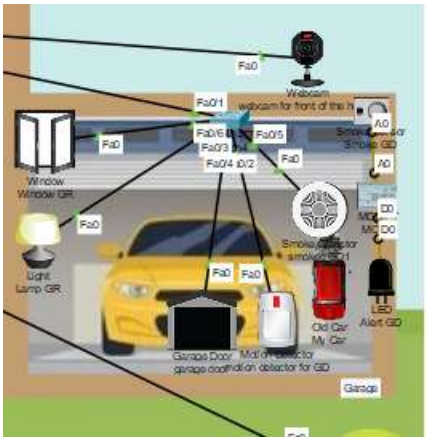


Figure 44

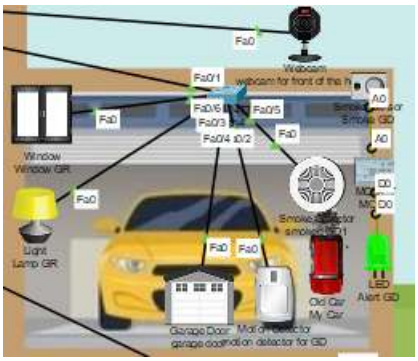


Figure 45

```
Starting Smart home (JavaScript)...
High    Smoke   Danger!!!
High    Smoke   Danger!!!
High    Smoke   Danger!!!
High    Smoke   Danger!!!
```

Figure 46

Sensor condition

Edit Remove	Yes	Motion GR	motion detector for GD On is true	Set garage door On to true Set Window GR On to true Set Lamp GR Status to On
Edit Remove	Yes	No Motion GR	motion detector for GD On is false	Set Lamp GR Status to Off Set garage door On to false Set Window GR On to false

Figure 47

MCU Board configuration

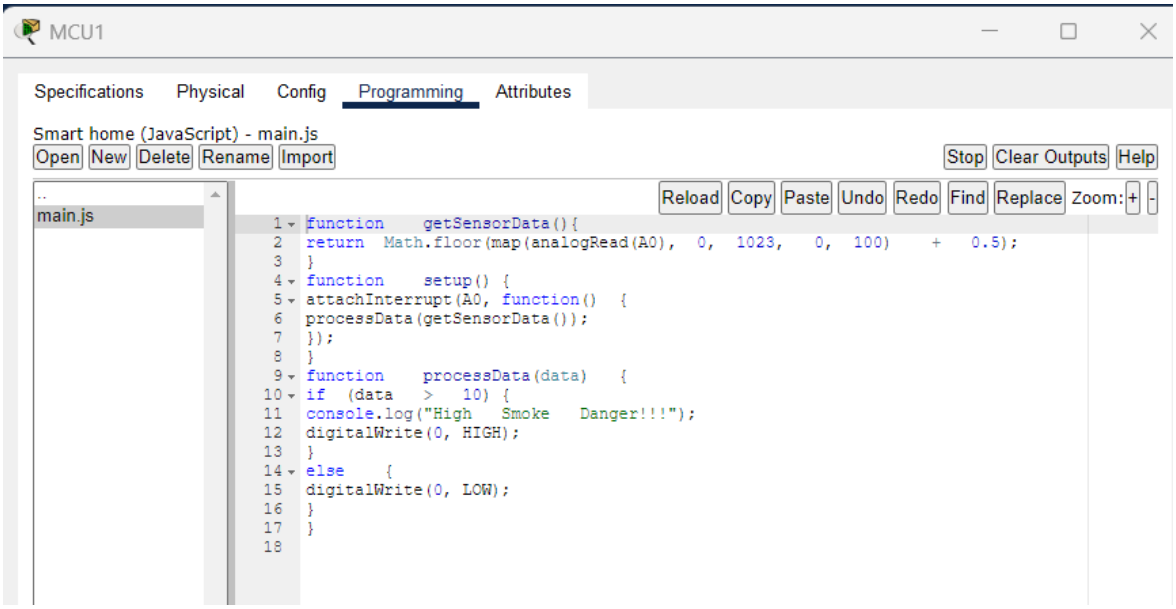


Figure 48-MCU Board garage

Front of the House

Initially all things are off.

Figure 49

When a motion is detected by the motion detector, then the webcam, street light, and wind detector will be turned on. The automatic water drain will be opened when the water sprinkler is turned on and drain the excess water.

Figure 50- Front of the house after turned on

Solar panel area

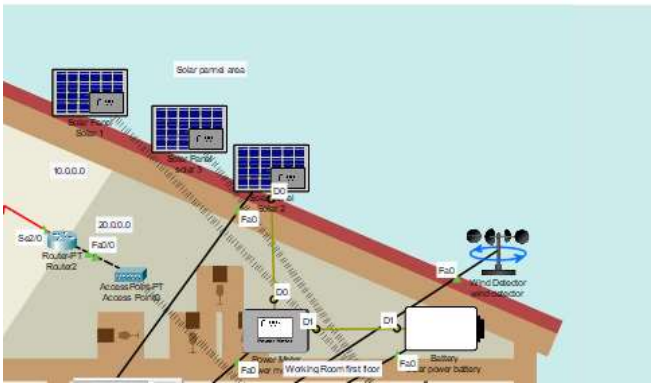


Figure 51-solar panel area

To maximize exposure to sunlight, solar panels absorb solar energy and convert it into electrical power. When there is less demand for energy, the energy can be stored in a battery and used to power appliances or other devices. To maximize energy management, a wind sensor detects the direction and speed of the wind. The solar panel area is monitored and managed by an Internet of Things device that serves as a control center. Routers and access points are used to integrate the solar panel area with the network, enabling remote control and monitoring.

When exposed to sunlight, the solar panels generate electricity, which can be stored in a battery or used to power appliances. Environmental information from the wind sensor, such as strong wind conditions, can be used to adjust how the solar panel system operates. The IoT hub collects data from the solar panels, batteries, and the wind sensor to provide real-time updates on energy output, storage levels, and weather conditions.

The solar panel area encourages weather adaptation, smart energy management, remote monitoring, and sustainable energy use. In the event of severe weather, the wind sensor helps protect the system from any damage.

Overall Logics / Conditions

When a motion detector in a house senses someone in front of it, it automatically turns on a camera, turns on the water faucet, and closes all the windows. When it senses a lawn sprinkler in front of the house, the water faucet also turns on or off.

When a wind detector detects high winds, all the windows automatically close. When a person enters the room, the motion detector in the living room opens or closes the door. The motion detector in the bedroom opens or closes the door in response to detecting a person in the bedroom. The fans, lights, windows, and camera are all activated by motion detection in the bedroom.

The garage door opens or closes in response to a motion detector that senses a car or person in front. In addition, the motion detector on the kitchen door senses when someone is there and opens or closes the door accordingly.

Finally, a motion detector in a house senses when someone is in front of it and initiates automatic processes such as turning off the sprinklers, turning on a camera, and closing all the windows. In addition, the motion detector opens or closes the garage door when it senses a vehicle or person in front of it.

Conditions

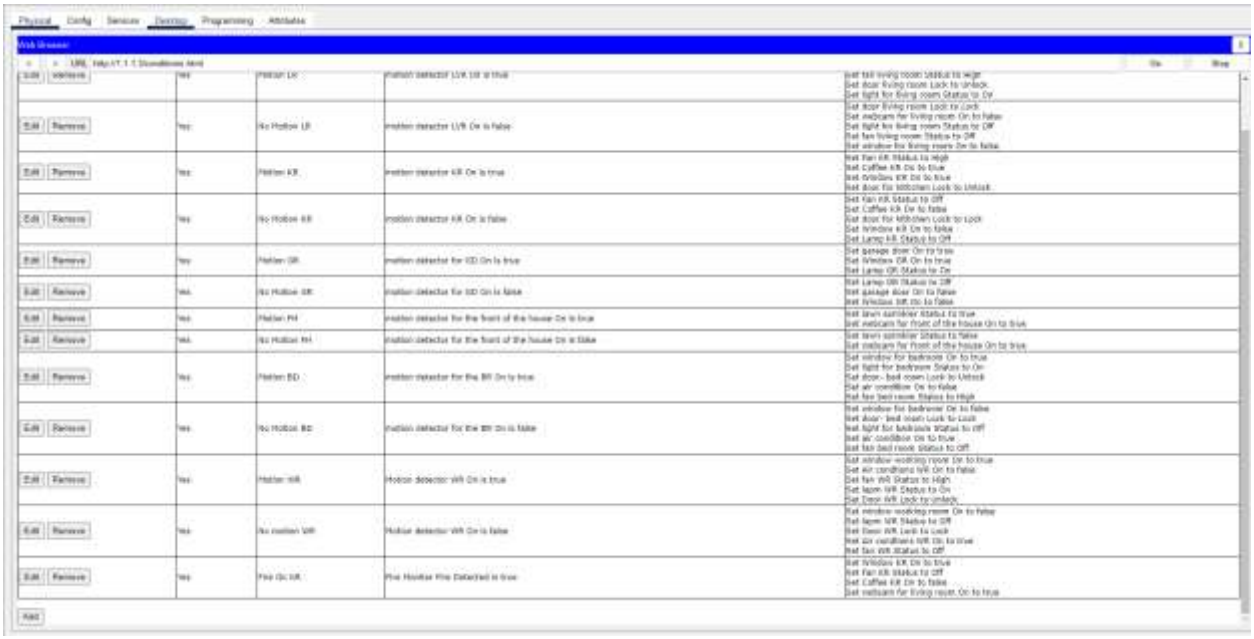


Figure 52

Connection

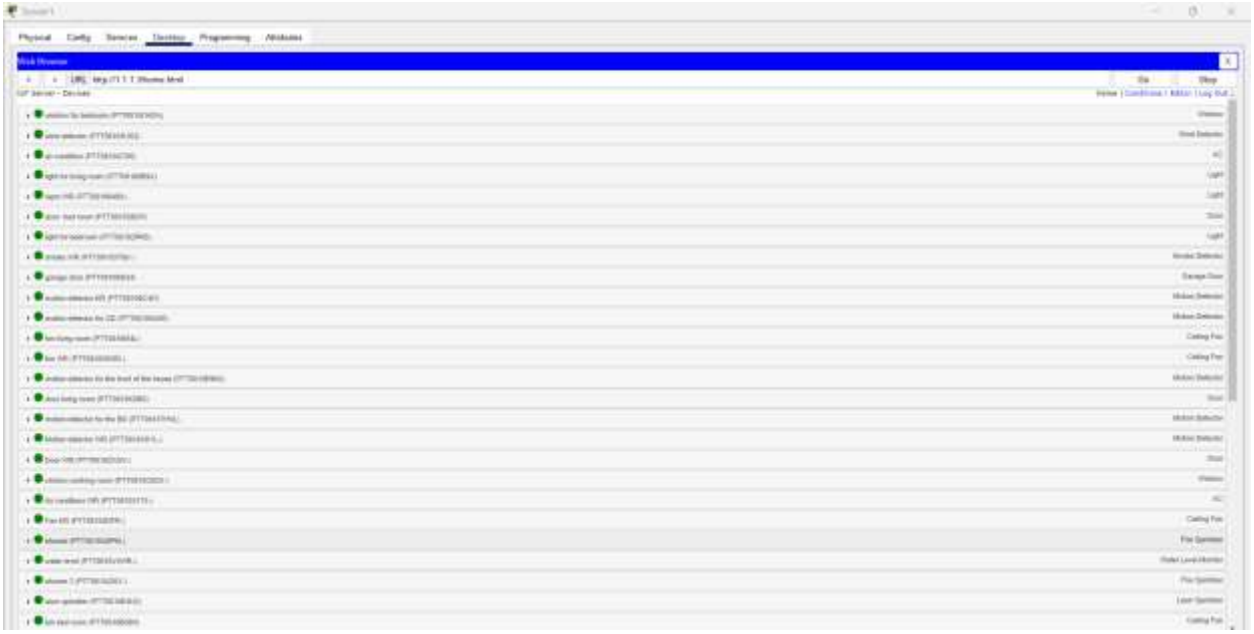


Figure 53

3. Demonstrate the security protocols and configurations

By implementing security rules in my smart home, my smart home system is protected from breaches and unwanted access by ensuring that all its sensors, controls, and devices are operating securely. The configurations used and other suggestions for improving security are described below:

1. Configured Security Protocols

1.1 Console Password

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line aux 0
Router(config-line)#password IOTsmartkey
Router(config-line)#login
Router(config-line)#exi
Router(config)#
Router(config)#
```

Figure 54-console password

Here is main purpose is Secures physical access to the device through the console port. When a user physically connects to the device (via console connection) and physically tampers with the device without authorization, the console password must be entered before using the command line interface (CLI).

1.2 Auxiliary Password

```
!
line aux 0
 password IOTsmartkey
 login
!
```

Figure 55-Auxiliary password

Here main purpose is Secures access through auxiliary ports (commonly used for dial-up or out-of-band access). In case the main network is inaccessible, the password must be entered while connecting to the auxiliary port. Helpful as a fallback access option.

3. Telnet Password

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password IOTsmartkey
Router(config-line)#login
Router(config-line)#exit
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Figure 56-Telnet password

Here is main purpose is Enables remote access to the device over the network using Telnet.

Telnet allows users to remotely access a device over a network. The system prompts for a configured password before granting access.

Note: Telnet is less secure than SSH because it transmits data in plain text. Use Telnet only if encryption is not required.

4. Enable Password

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#Enable Password
% Incomplete command.
Router(config)#enable password IOTsmartkey
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 57-enable password

Here is main purpose is Protects access to privileged EXEC mode (where sensitive configurations can be made). To access privileged EXEC mode, users must enter the active password after logging in to the device. The active secret is more secure than the active password because the password is encrypted.

Note: In this smart home, I don't have encrypted this password, if wish to encrypt this password, we can use below command to encrypt this password.

Enable Secret

```
Router (config) #enable secret IOTsmartkey1
```

```
Router1(config)#enable secret IOTsmartkey1
Router1(config)#exit
Router1#
%SYS-5-CONFIG_I: Configured from console by console

Router1#
```

- Special note - We cannot configure same password for both enable password and enable secret.

When we configured both enable password types on the same router, then the enable password will be deactivated. Most recommended password is enable secret.

Enable secret will be encrypted as level 5 password by default.

How to encrypt other passwords:

```
Router (config) #service password-encryption
```

```
Router1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#service password-encryption
Router1(config)#exit
Router1#
%SYS-5-CONFIG_I: Configured from console by console

Router1#
```

Verification

```
Press RETURN to get started.




Wellcome Router 1

User Access Verification

Password:

Router>en
Password:
Router#
```

Figure 58-password verification

Router 2

```
Well come to router 2

Router>
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line con 0
Router(config-line)#password cisco123
Router(config-line)#login
Router(config-line)#exit
Router(config)#line aux 0
Router(config-line)#password IOTsmartkey
Router(config-line)#password cisco123
Router(config-line)#login
Router(config-line)#exit
Router(config)#
Router(config)#line vty 0 4
Router(config-line)#password cisco123
Router(config-line)#login
Router(config-line)#exit
Router(config)#enable password cisco123
Router(config)#
```

Figure 59-router 2

As mentioned above, all configurations created on the first router are applied to the 2nd router.

```
Well come to router 2

User Access Verification

Password:
Password:
Password:

Router2>en
Password:
Router2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#enable secret ciscoworld
Router2(config)#service password-encryption
Router2(config)#
Router2(config)#exit
Router2#
%SYS-5-CONFIG_I: Configured from console by console

Router2#
```

Figure 60

Verification

```
Well come to router 2

User Access Verification

Password:

Router>en
Password:
Router#
```

Figure 61-verification

1.5 Secure Shell (SSH)

Router 1

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Router1
Router1(config)#ip domain-name Cyber_local
Router1(config)#crypto key generate rsa
The name for the keys will be: Router1.Cyber_local
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Router1(config)#ip ssh version 2
*Mar 1 3:42:28.984: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router1(config)#line vty 0 4
Router1(config-line)#transport input ssh ?
  <cr>
Router1(config-line)#transport input ssh
Router1(config-line)#login local
Router1(config-line)#exec-timeout 0 30
Router1(config-line)#exit
Router1(config)#username admin password cisco123
Router1(config)#exit
Router1#
%SYS-5-CONFIG_I: Configured from console by console

Router1#wr
Building configuration...
[OK]
Router1#
```

Figure 62-SSH configuration

Here is main purpose is Provides encrypted remote access to the device, improving security over Telnet. Using SSH clients (such as PuTTY), users establish an encrypted connection to the device, preventing interception of personal data such as orders and passwords.

Verification

```
C:\>ssh -L admin 1.1.1.1

Password:

Wellcome Router 1

Router1>en
Password:
Router1#
```

Figure 63-SSH verification

Router 2

```
Router#
Router#
Router#hostname Router2
               ^
% Invalid input detected at '^' marker.

Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Router2
Router2(config)#ip domain-name cyber_local
Router2(config)#ip domain-name cyber_local 2
                                           ^
% Invalid input detected at '^' marker.

Router2(config)#ip domain-name cyber_local2
Router2(config)#crypto key generate rsa
The name for the keys will be: Router2.cyber_local2
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Router2(config)#ip ssh version 2
*Mar 1 3:58:53.704: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router2(config)#
Router2(config)#username admin2 password cisco123
Router2(config)#line vty 0 4
Router2(config-line)#transport input ssh
Router2(config-line)#login local
Router2(config-line)#exec-timeout 0 30
Router2(config-line)#exit
Router2(config)#exit
Router2#
%SYS-5-CONFIG_I: Configured from console by console

Router2#wr
Building configuration...
[OK]
Router2#
```

Figure 64-SSH Router 2

Here is main purpose is Provides encrypted remote access to the device, improving security over Telnet. Using SSH clients (such as PuTTY), users establish an encrypted connection to the device, preventing interception of personal data such as orders and passwords.

Verification

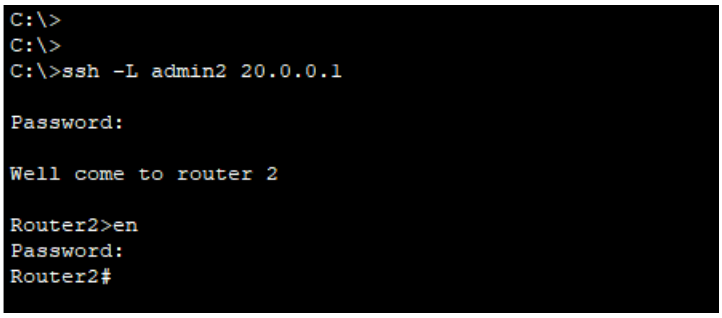


Figure 65

1.6 Access Control List Setup (ACL)

Rules are created to allow or deny access to the smart home system based on source IP addresses to set up access control lists (ACLs) for devices with certain IP addresses.

- Laptop IP: 1.0.0.53
- Smartphone IP: 20.0.0.8
- Remote PC IP: 192.168.1.11

ACL Rules router 1

```
Wellcome Router 1

User Access Verification

Password:

Router1>en
Password:
Router1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#access-list 10 permit 1.0.0.53
Router1(config)#access-list 10 permit 20.0.0.8
Router1(config)#access-list 10 permit 192.168.1.11
Router1(config)#access-list 10 deny any
Router1(config)#exit
Router1#
%SYS-5-CONFIG_I: Configured from console by console

Router1#wr
Building configuration...
[OK]
Router1#
```

Figure 66-ACL R1

ACL Rules router 2

```
Router2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#access-list 10 permit 1.0.0.53
Router2(config)#access-list 10 permit 20.0.0.8
Router2(config)#access-list 10 permit 192.168.1.11
Router2(config)#access-list 10 deny any
Router2(config)#exit
Router2#
%SYS-5-CONFIG_I: Configured from console by console

Router2#wr
Building configuration...
[OK]
Router2#
```

Figure 67-ACL router2

- Same as router 1, we can check the security

Verification connectivity IOT server

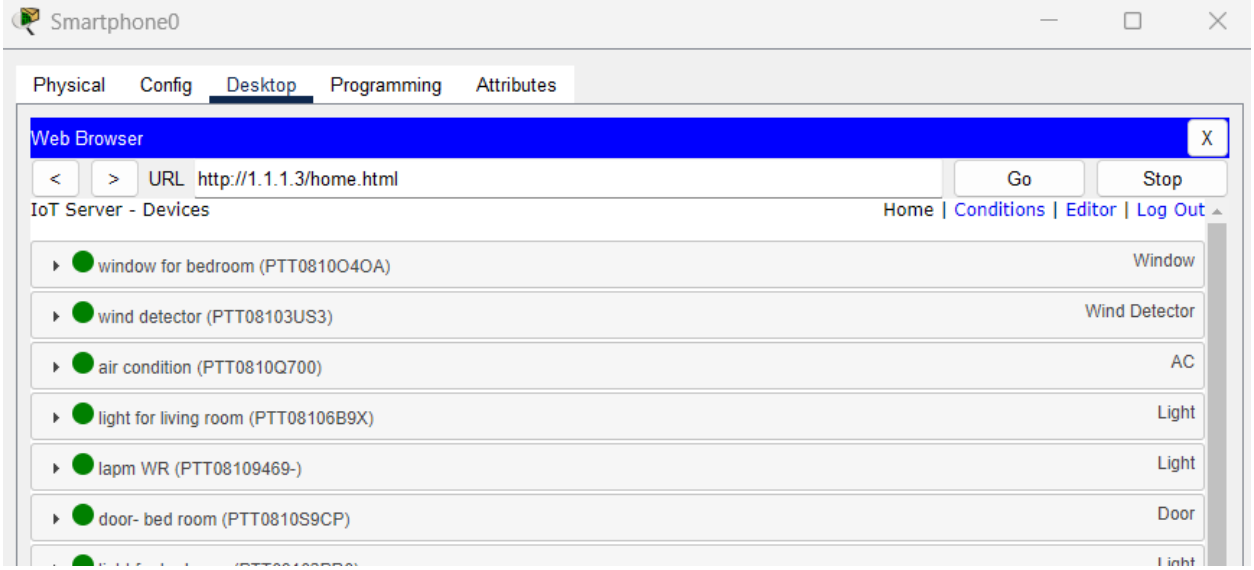


Figure 68-using smart phone

- These configuration ensure that only authorized people can access and control smart home devices. By combining network security (Telnet, SSH, ACL), physical security (console and auxiliary passwords), and encryption (password encryption and SSH), the system achieves a strong security posture, protecting it from attacks both inside and outside the system.

4. Challenges faced during the project

- Device Compatibility
- Sensors connectivity
- Scalability issues
- Architecture design issue

Conclusion

I have effectively designed an automated home system for the IoT-Smart Home project, which aims to improve consumer comfort, convenience, and security. The system integrates various Internet of Things components, including sensors, actuators, and controllers, to monitor and manage different areas of the home environment. This includes smart appliances, motion and smoke detection, water management, lighting, and other features that make a home more responsive and efficient.

The project places a strong emphasis on energy conservation by automating processes such as turning off lights and appliances when not in use, using sensors to optimize water consumption, and incorporating renewable energy sources such as solar panels. These features encourage sustainable living and reduce wasteful electricity use.

The system's ability to enable remote access and management using a mobile phone is one of its most notable advantages; it enables the homeowner to monitor and manage their home from anywhere in the world. This level of connectivity ensures enhanced security and convenience, as the system can transmit alerts and take pre-determined actions in response to detected abnormalities, high smoke levels, or illegal entry.

Although there is a significant upfront cost associated with implementing an IoT-Smart Home system, the long-term benefits far outweigh the costs. Technology makes life easier and more productive by automating repetitive tasks, which also saves time and human labor. Furthermore, advanced security systems provide peace of mind by ensuring that the home is safe even when the owner is not present.

In summary, this IoT-Smart Home project shows how IoT technology has the power to completely transform contemporary life. It opens the door to a smarter, safer, and more sustainable future by combining automation, energy efficiency, and remote accessibility.

References

[1]. Samuel, S. Sujin. “A review of connectivity challenges in IOT-Smart Home.” *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, Mar. 2016, pp. 1–4, https://doi.org/10.1109/icbdsc.2016.7460395. [2] Vishwakarma, Satyendra K., et al. “Smart Energy Efficient Home Automation System using IOT.” *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Apr. 2019, https://doi.org/10.1109/iot-siu.2019.8777607. [3] Malche, Timothy, and Priti Maheshwary. “Internet of things (IOT) for Building Smart Home System.” *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Feb. 2017, pp. 65–70, https://doi.org/10.1109/i-smac.2017.8058258. [4] Verma, Gaurav, et al. “Smart Home Automation with smart security system over the cloud.” *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 6 July 2023, pp. 1–7, https://doi.org/10.1109/icccnt56998.2023.10306548. [5] Mandula, Kumar, et al. “Mobile based home automation using internet of things(iot).” *2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, Dec. 2015, https://doi.org/10.1109/iccicct.2015.7475301. [6] Assim, Marwa, and Alauddin Al-Omary. “Design and implementation of smart home using WSN and IOT Technologies.” *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, 20 Dec. 2020, pp. 1–6, https://doi.org/10.1109/3ict51146.2020.9311966.