Open Ended Experiment

Experiment name : Design an IoT based smart home with security feature using cisco packet tracer

Abstract

The Internet of Things (IoT) connects technology devices or sensors to the internet so that they can be monitored and controlled remotely by the user. In this experiment, the implementation is accomplished by using the Cisco packet tracer to simulate a smart home system. To remotely monitor and control home appliances, the system includes smart devices such as a door, fan, light, window, lawn sprinklers, smoke detector, siren, camera, and so on. All of the devices are connected to the home gateway and can be controlled and monitored remotely from a laptop, desktop computer, or smartphone. The WEP-based security key is used to secure all of the devices. The simulation results show that smart devices can be monitored successfully.

Introduction

The term "IoT" stands for "Internet of Things," and it was originated by Kevin Ashton in 1999. Although the phrase was introduced in 1999, the concept of connected devices traced all the way back to 1832. When the first electromagnetic telegraph was invented, it enabled direct communication between two devices via the transmission of electrical signals.[1]

The world's first Internet of Things device was invented in the early 1980s at Carnegie Melon University. A group of students designed a system for their campus Coca-Cola vending machine to report on its contents via a network, saving them the trek if the machine was out of Coke. They installed micro-switches in the machine to notify them about how many Coke cans were available and if they were cold. In the 1990s, John Romkey was the first person to connect a toaster to the internet. A year later, a group of students from the University of Cambridge devised a plan to monitor the amount of coffee in their computer lab's coffee pot using the first web camera prototype. They accomplished this by programming the web camera to capture three photographs of the coffee pot every minute. The photos were then sent to local computers, allowing everyone to see if there was any coffee available.[1]

The Internet of Things (IoT) was a popular topic in the media at the beginning of the 21st century, with several major developments opening the way for IoT's future. In the year 2000, LG Electronics released the world's first internet-connected refrigerator. Allowing customers to do their grocery shopping and make video calls online. In 2005, a small rabbit-shaped robot was developed to report the latest news, weather forecasts, and stock market changes. In 2008, Switzerland hosted the first International Conference on the Internet of Things.[1]

The Internet of Things currently connects over 27 billion devices, with experts predicting that this number will rise to over 100 billion by 2030. [1]

Background Study

D. A. Hazim et al. introduced a method to deliver practical IoT simulation using Cisco Packet Tracer. They have connected different smart appliances to the home gateway wired or wirelessly. They have provided the necessary simulation results to justify their system. The smart devices were accessible by the smartphone or laptop. They have used a microcontroller board to provide a programming environment to control the smart devices. [2]

Using a Cisco package tracker, O. Sihombing et al. proposed creating a smartphone network to simulate a smart home system. They set up some electronic devices based on their condition and configured the networks and connected multiple electronic smart devices to connect over the wireless network. They indicated that with this simulation, design and implementation planning can be done in building smart home networks using IoT home gateways and that there is a possibility that this simulation can be applied in the real world based on current technology development, making it a necessity for community life whose potency can improve energy efficiency, reduce energy use costs, control electronic devices, and change the role of occupants, thus making it a necessity for community life. [3]

The author of [4] described a smart home system based on the recently released Cisco kit, which included numerous IOE devices for home automation. They used a home gateway to register smart devices and a Microcontroller (MCU) to connect different sensors and IOE devices to monitor them. MCU also has a variety of system programming environments and programming languages, but they chose to manage the device using JavaScript and Python.

Standard and codes

Although the IoT industry is still in its formative stages, some IoT standards organizations, trade associations, and industry groups have emerged to guide IoT security standards and recommended codes of practice, which are listed below:

- ETSI (European Telecommunications Standards Institute)
- IoTSF (Internet of Things Security Foundation)
- GSMA
- NIST (National Institute of Standards and Technology)
- IEEE
- IEC (International Electrotechnical Commission)
- ENISA [5]

European Telecommunications Standards Institute

The European Telecommunications Standards Institute (ETSI) is a European Standards Organization that oversees telecommunications, broadcasting, and other electronic communications networks and services. The institute, which has 900 members, is a global leader in the development and ratification of IT standards in existing and emerging technologies like the Internet of Things.[5]

Internet of Things Security Foundation

IoTSF (Internet of Things Security Foundation) is a non-profit international organization that aims to make IoT safer so that its benefits can be fully realized.[5]

GSMA

The GSMA encourages best practices for the secure design, development, and deployment of IoT services and facilitates security measure evaluation. The organization represents mobile carriers, phone and device manufacturers, software businesses, equipment providers, and internet service providers around the world. The GSMA has regional offices in Asia Pacific, Greater China, Europe, Latin America, the Middle East, North Africa, Sub-Saharan Africa, and North America.[5]

National Institute of Standards and Technology

NIST (National Institute of Standards and Technology) is the official authority on technology standards for the United States of America.[5]

IEEE

IEEE is the world's biggest technical professional organization dedicated to technology advancements that benefit humanity.[5]

International Electrotechnical Commission

IEC (International Electrotechnical Commission) is an international standards body that releases international standards for all electrical technologies.[5]

ENISA

ENISA is the European Union Agency for Cybersecurity and aims to create a common level of cybersecurity measures for countries across Europe.[5]

Experimental Methods

The design of the Smart Home system has been performed by using the Cisco Packet Tracer simulation software. Smart Home system design includes a smartphone, laptop, or PC and a home gateway to connect to various smart home appliances. Home gateway is used to connect all the smart devices, and smartphones, laptops, or PC are used to communicate with the smart devices through the home gateway. The required devices are listed below:

1. Home Gateway
2. Door
3. Fan
4. Window
5. Light
6. Lawn Sprinkler
7. Smoke Detector
8. Siren
9. Webcam
10. Garage Door
11. Old Car
12. Smartphone
13. Laptop
14. Desktop Computer

All the devices should be connected as shown in Figure 1.

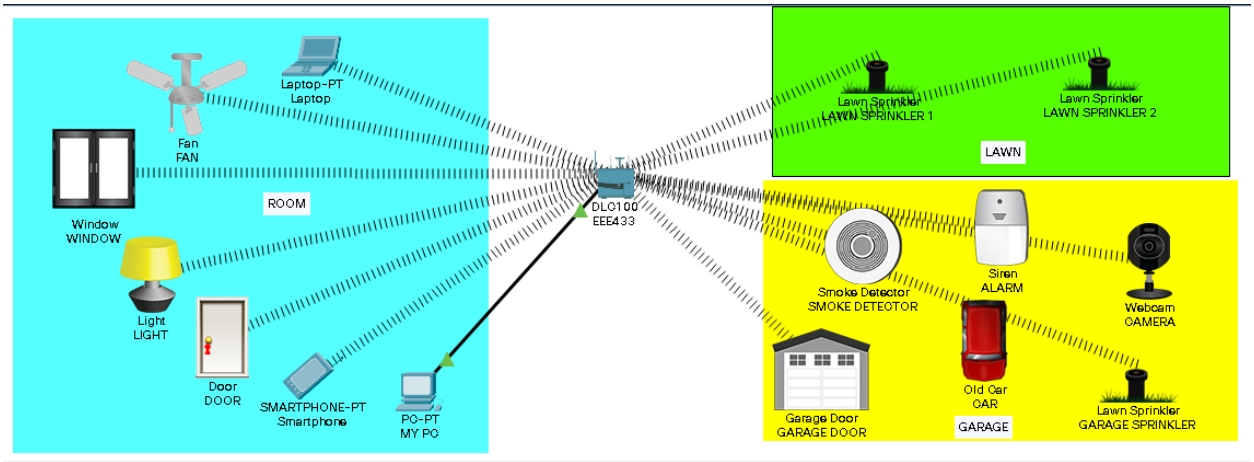

Figure 1: Connection Diagram.

To secure the home network, we have used WEP- based protection, the home gateway configuration is,

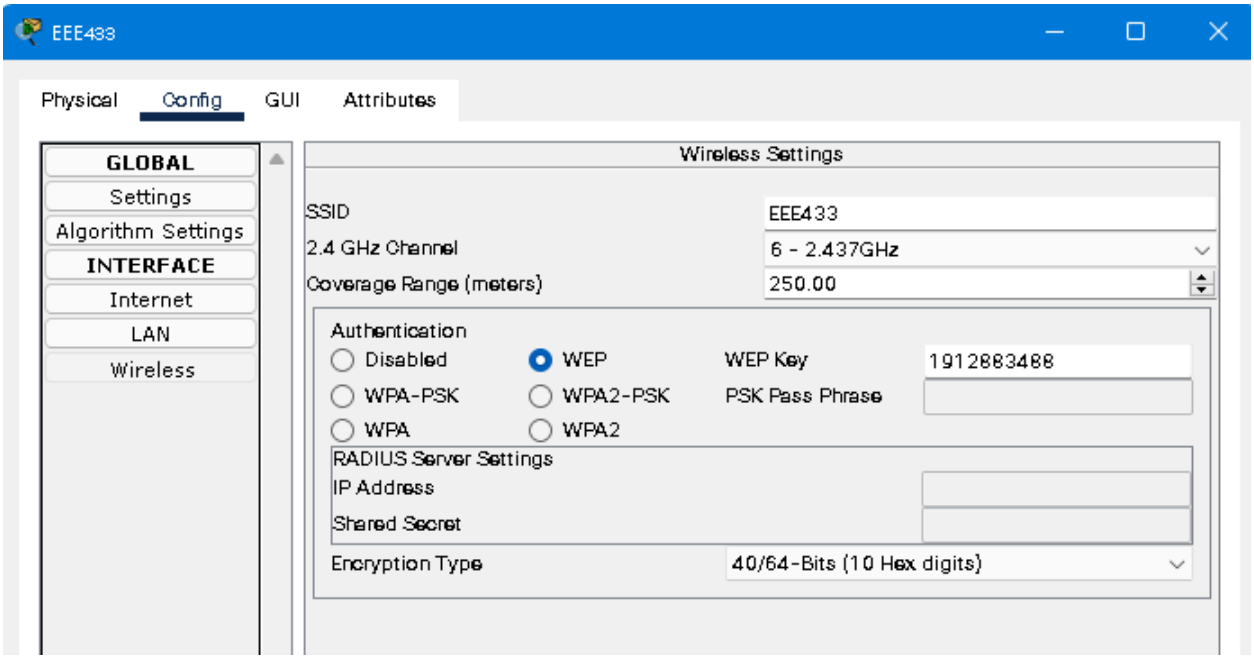

Figure 2: Home gateway configuration.

For all the devices configuration, First, we need to change the IoT server to Home Gateway which would be found from settings,

Figure 3: Device configuration.

Then we need to connect the devices using the WEP key,

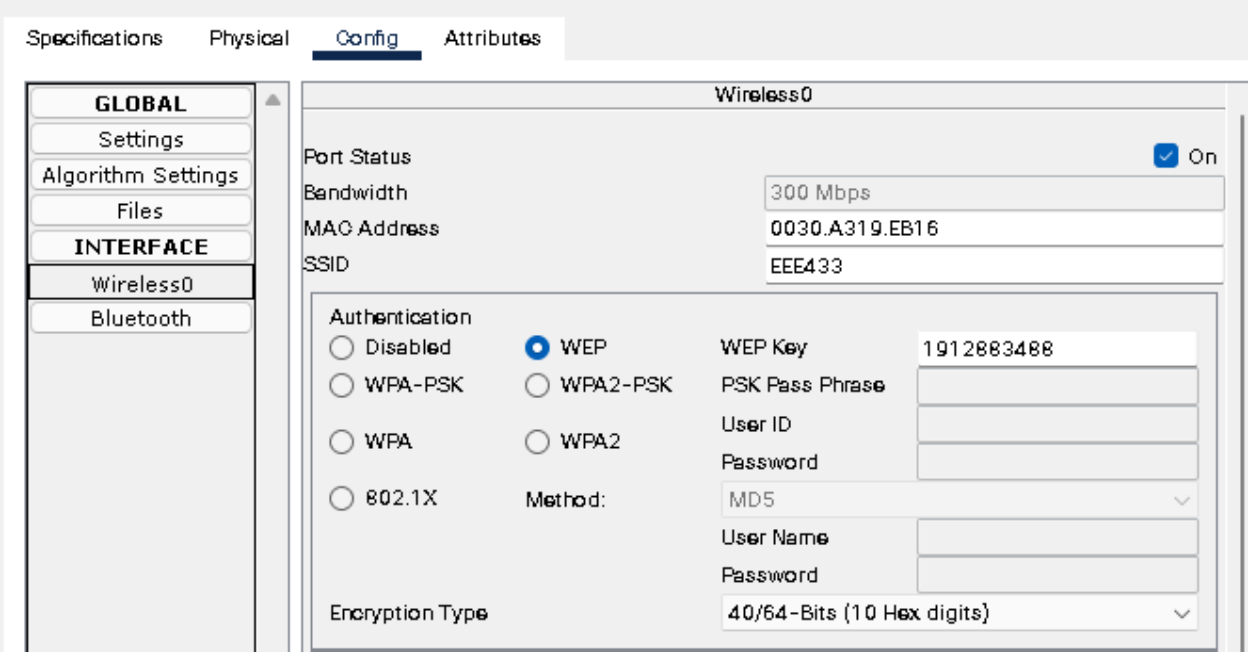

Figure 4: Device configuration.

For automation, we can use conditions to operate devices. To do that, firstly we need to open the smartphone, laptop or PC. Then we need to go to the IoT monitor section. Then we need to log in. From the conditions section, we can add conditions as follows,

IoT Monitor X

IoT Server - Device Conditions

Home | Conditions | Editor | Log Out

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Fire Alarm ON	SMOKE DETECTOR Level > 0.03	Set ALARM On to true
Edit Remove	Yes	Garage sprinker ON	ALARM On is true	Set GARAGE SPRINKLER Status to true
Edit Remove	Yes	Garage Sprinkler OFF	ALARM On is false	Set GARAGE SPRINKLER Status to false
Edit Remove	Yes	Fire Alarm OFF	SMOKE DETECTOR Level < 0.01	Set ALARM On to false

Figure 5: Device conditions.

Results and Discussions

Simulation from Smartphone

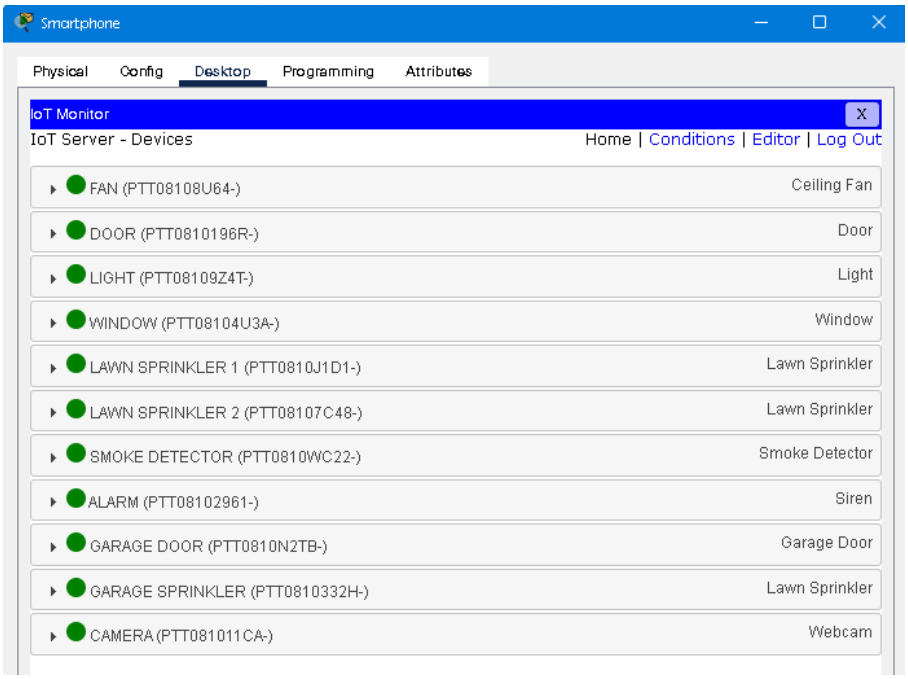

Figure 6: Connect from a smartphone.

Simulation from Laptop

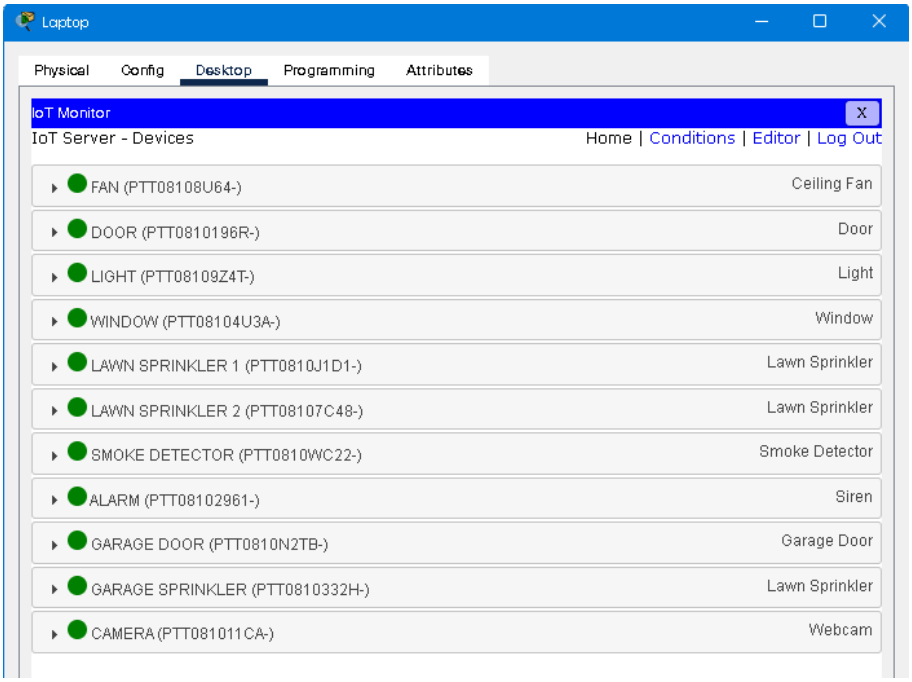

Figure 7: Connect from a laptop.

Simulation from Desktop PC

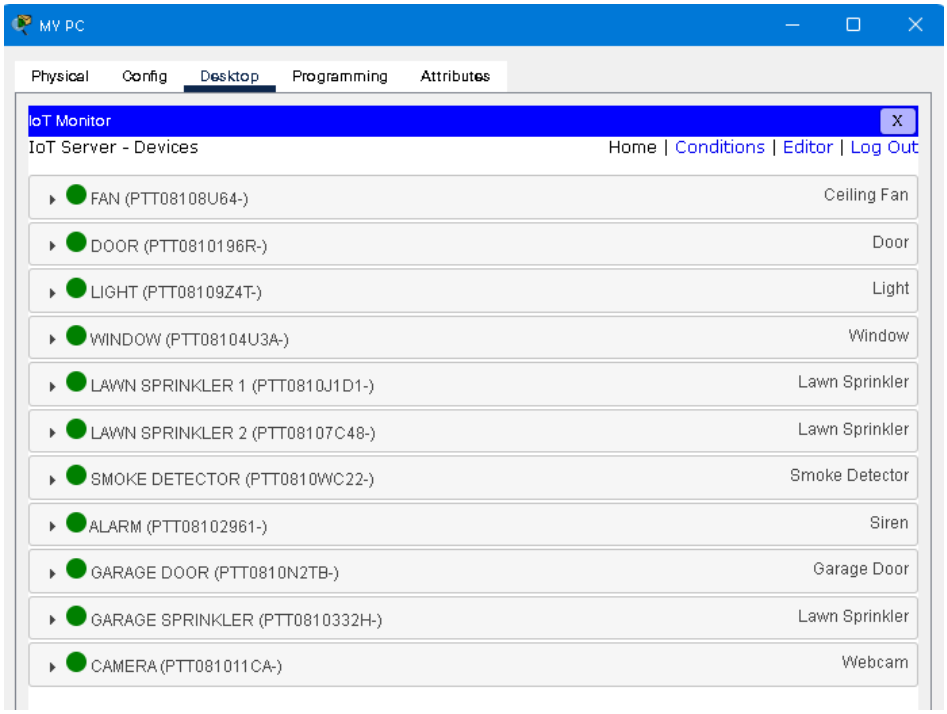

Figure 8: Connect from a desktop PC.

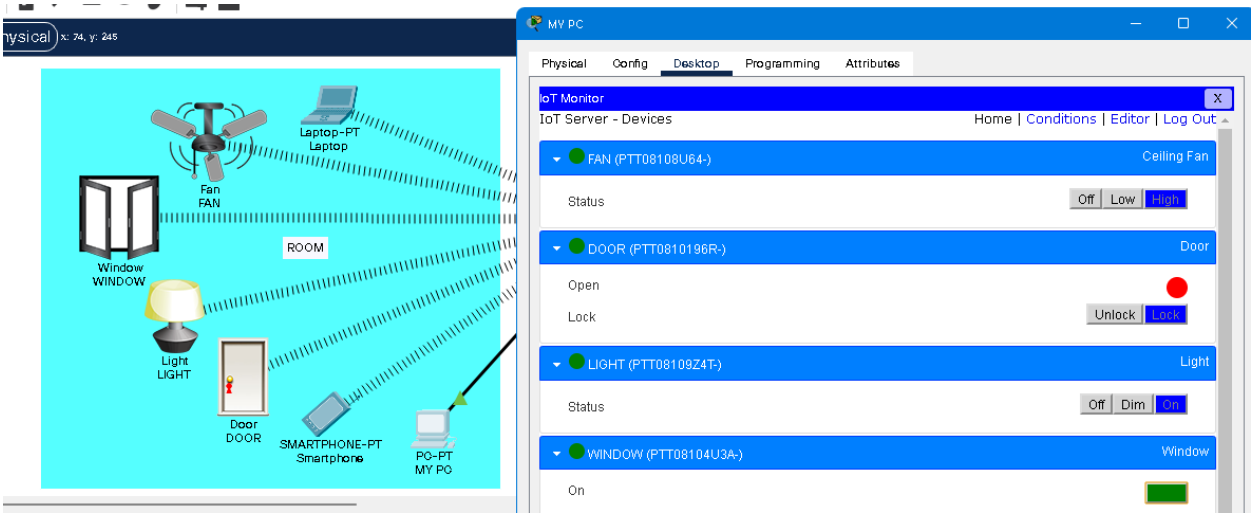

Figure 9: Simulation results.

Here we can see that the smart devices can be controlled using a desktop. The fan speed can be controlled. We can lock or unlock the door, we can open or close the window as well. We can also control the light to be on, off, or dimmed.

Figure 10: Simulation results.

In the above figure, we can see that the lawn sprinklers can be controlled.

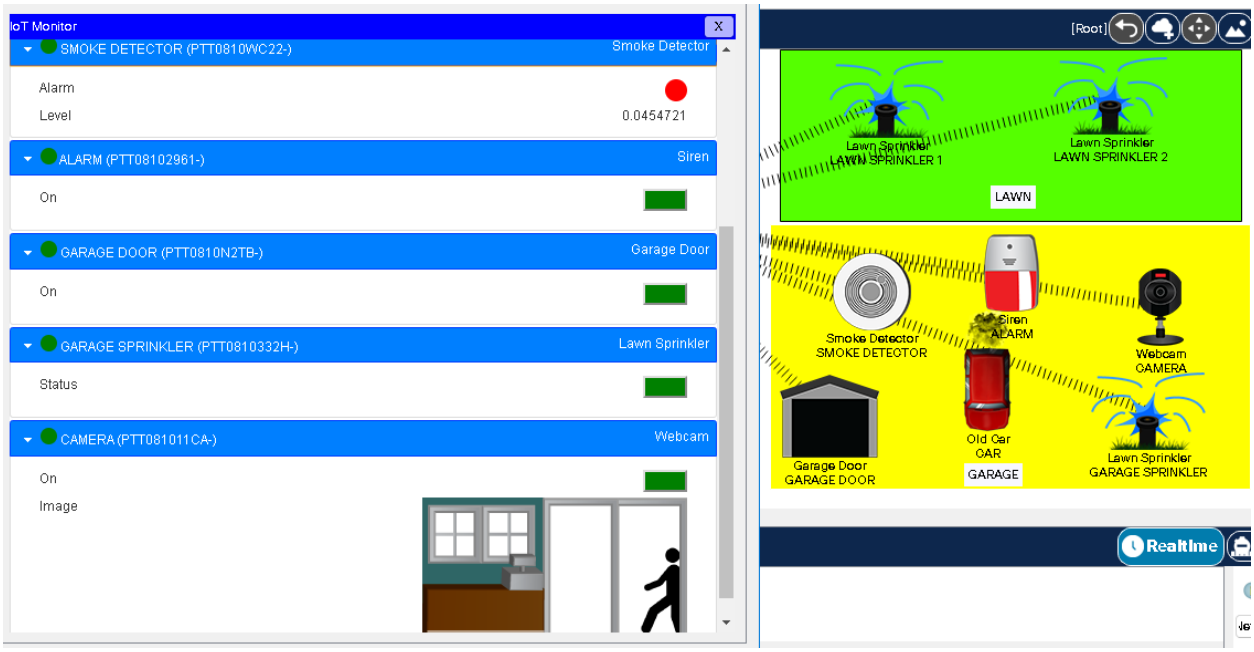

Figure 11 Simulation results.

Figure 11 represents the garage. Here we can control the garage door. Here we have a security camera. In this section, we have automated the smoke sensor, alarm, and sprinkler. Smoke can be produced from an old car. If the smoke detector detects a certain amount of smoke[threshold of 0.03] then the alarm will buzz. And immediately the sprinkler will be turned on. If the smoke is less than 0.01 then the alarm will turn off and the sprinkler will be turned off as well.

After registering the devices with the home gateway, the IoT devices can be controlled remotely. The IoT devices that have been registered can be viewed on a desktop, laptop, or smartphone. The devices may be controlled manually, and the values can be examined and monitored in real-time.

Conclusion

The proposed smart home system in this experiment can support a wide range of home automation systems. The smart home is connected via wireless communication with different smart appliances and sensors, and monitoring devices. The system can be operated in the local network. It is secured with WEP-based protection. We can successfully control and monitor smart devices. This system can be upgraded using more sensors and devices. We can add more security features. This system is based on the local network, but it can also be upgraded to the global network. So that the smart devices can be controlled from anywhere. In today's technologically advanced era, technology has become a necessity for existence in today's society. So far, turning off and turning on the home electronic devices has been accomplished by pressing the switch or remote button, making electronic device control less effective. To create a smart home, we can turn on and off electronic devices via smartphone. Which is very much effective in this modern era.

References

[1] 'History of the Internet of Things (IoT) | IT Blog', *ITonlinelearning*, Mar. 02, 2020. https://www.itonlinelearning.com/blog-history-iot/ (accessed Jan. 12, 2022).

[2] D. A. Hazim and S. A. Alabady, 'SMART HOME DESIGN AND IMPLEMENTATION USING CISCO PACKET TRACER'.

[3] O. Sihombing *et al.*, 'Smart home design for electronic devices monitoring based wireless gateway network using cisco packet tracer', in *Journal of Physics: Conference Series*, 2018, vol. 1007, no. 1, p. 012021.

[4] 'SMART HOME USING CISCO PACKET TRACER - SMART HOME USING CISCO PACKET TRACER ABSTRACT Smart Home is a', *StuDocu*. https://www.studocu.com/en-gb/document/kingston-university/network-security/smart-home-using-cisco-packet-tracer/14467719 (accessed Jan. 12, 2022).

[5] 'IoT Device Security Standards & Code of Practice for IoT Security', *Coderus*, Apr. 12, 2021. https://www.coderus.com/iot-device-security-standards-and-code-of-practice-for-iot-security/ (accessed Jan. 12, 2022).