Journal of Electrical Engineering, Electronics, Control and Computer Science – JEEECCS, Volume 6, Issue 21, pages 1-8, 2020

Design and Simulation of IoT Network for Smart-Home

Fidelis Odinma Chete
Department of Computer Science
University of Benin
Benin, Nigeria

Aliu Adeyemi Adeniji
Department of Computer Science
University of Benin
Benin, Nigeria

***Abstract* – Internet of Things (IoT) devices are connected to the internet to allow the distant monitoring and controlling of different home appliances such as lighting, heating, cooling and alarming. Smart home is the technology of Internet of Things to automate different activities at home. This research modeled and simulated an IoT system for smart home in the department of computer science building, university of Benin, Benin-City. The system uses smart web cams, smart door, motion detector, smart fan, smart light, smoke detector, smart window, with each having their respective IP addresses, and allows these smart devices to transmit valuable information to the users. The designed smart home addresses security challenges by sending notification to the user's smartphone whenever an intruder tries to gain access to the departmental building and also giving live feeds to the user about the environmental condition of the department. The system is also capable of addressing fire incident by automatically triggering the fire sprinkler whenever it detects about 36 percent smoke level. Cisco packet tracer simulation software was used to model and simulate the IoT network for smart home, because this new version simulator now include different IoT services used for home automation, unlike the previous software which has only networking devices. The results of the simulation indicate that when the smart devices are connected in a wireless medium, they can send and receive data via a DLC100 home gateway which can be accessed by the user on internet enabled devices.**

Keywords-smart home; Internet of things (IoT); simulate; automate

I. INTRODUCTION

[1] defined IoT as an interconnection of smart devices that have identifiers, and uses standard communication protocol to interact with little or no human intervention. According to [2], IoT is an acronym of Internet of Things which refers to things that are uniquely identified and represented virtually in the configuration of an internet. This emergent technology, IoT has come into existence to improve interaction among objects by connecting them to the internet, thereby allowing these objects to be accessed remotely or locally.

Smart-Home refers to any building integrated with a communicating network of sensors, domestic devices and appliances enabling house owners to control the function of houses through sophisticated monitoring systems [3]. They allow house owners to automate activities of their environmental conditions without their involvement using various sensors like smoke detector, motion detector, temperature sensors etc., then sending digital signals based on the data generated from the sensors. Smart-Homes can offer numerous functions ranging from automated security system which uses alarm system like siren, automatic display of lights as well as forwarding electronic mail to legalized users. Home-Automation refers to method of employing micro-controllers or computer technology to access, manage and control home appliances [4]

[5] emphasizes that Smart-Home will help minimize the one-to-one monitoring of the home environment as well as providing remote access to the smart appliances through the use of sensors in strategic locations in the house. Home-Automation helps to bring about comfort, effectiveness as well as security to the environment. Automating the home involves controlling multiple systems using the technology of IoT. [6]. In this study, all the appliances that are required to be automated are registered to DCL100 Home-Gateway and are accessed via the smartphones by authorized users.

This research presents how the fire sprinkler can automatically ventilate the environment when it detects smoke level at a certain degree. It also addresses how it can detect unauthorized access to the department and automatically trigger the alarm. In addition, it explains how it can automatically switch on the lights at nights, when it detects movement alongside videoing the person with the hidden web cameras.

This study is aimed at modeling and simulating an IoT network for smart homes (a case study of Computer Science Department, University of Benin, Benin-City) that uses various smart devices with each having individual IP addresses, and allowing these smart devices to transmit valuable information to the users.

This research designs and simulates a smart-home using the new version of cisco packet tracer as a simulator. This simulator includes various IoT services, sensors, actuators and numerous smart IoT devices which can be employed as tools for automating the home. Some of the smart IoT devices employed are window, light, door, fan as well as detectors and sensors.

II. Brief Review of Related Literature

[7] developed and implemented a smart home using Internet of Things. The system, which was developed using the Rapid Application Development (RAD) methodology, consists of three subsystems viz: the Remote System, Simulated System and Cloud System. The developed system, on evaluation, showed that it was cost effective for at least a middle-class group.

[8], using Wireless Sensor Network (WSN) to facilitate energy-efficient data encryption, developed a secure IoT-based smart home automation. They proposed the Triangle Based Security Algorithm (TBSA) method, which is based on efficient key generation mechanism. The proposed method, in integration of the low power Wi-Fi, were included in WSNs with the Internet to develop a novel IoT-based smart home which could provide secure data transmission among several associated sensor nodes in the network over a long converge range. The authors further submitted that, on evaluation, the proposed algorithm, in comparison with some existing methods, consumed less energy.

[9], in their research, using RF based communication in a household to create an IoT-enabled smart home security system, presented a low-cost architecture for a smart door sensor. The authors were able to use affordable components to develop an IoT system that allows users of a household to view when a particular door has been opened.

A. *Existing System*

The existing appliances found in the building housing the department of Computer Science are manually managed and controlled since it requires the presence of the staff to operate them. Students' records are being stored in some strategic locations in the department. Also, a lot of sophisticated appliances are being used by the lecturers and these appliances are electrically operated. The department uses locks and keys as a primary means of preventing intruder from invading the building. In addition, the security officers were made available to patrol the department on a regular basis in order to ensure that the building is fully secured. The university has a fire service department located by the security department, at the main entrance to the university campus. These are all manual activities which may obviously have foreseeable challenges.

B. *Methodology*

In order to implement smart homes, the new released version of cisco networking simulator; cisco packet tracer 7.2.1 was used. This version includes different smart objects (such as smart fan, smart window, smart door, smart light, fire sprinkler etc.) used for home automation as well as different sensors and actuators. To control some of this smart objects and sensors, DLC100 Home Gateway was used since it serves as controlling mechanisms for registering smart devices. Also, Single Board Circuit (SBC-PT) was used, since it provides programming environment for controlling smart objects connected to it.

C. *Proposed System*

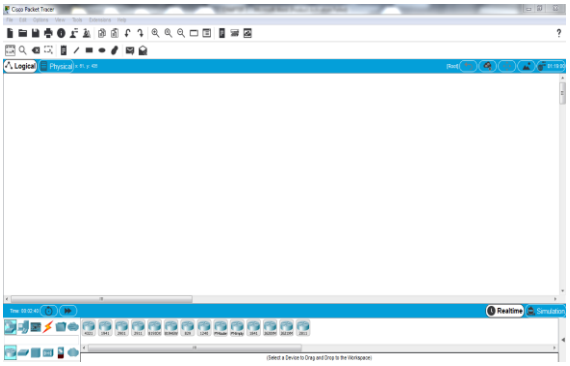
The proposed Smart home is a unique application of the technology of IoT. The main aim is to model and simulate an IoT system for smart home (Computer Science department) that uses smart web cams, smart door, motion detector, smart fan, smart light, smoke detector, smart window, with each having their respective IP addresses, and allowing these smart devices to transmit valuable information to the users (i.e. the Head of Department (H.O.D) and the Security Department). The designed smart home addresses security challenges which involve sending notification to the user's smartphone whenever an intruder tries to gain access to the building and giving live feeds to the user about the condition of the environment. The system is also capable of addressing fire incident by automatically triggering the fire sprinkler whenever it detects about 36 percent smoke level. Based on the recommendation of The Global Standards Initiative on the Internet of Things (IoT-GSI, 2012), the implementation of a multifaceted design for interconnecting between large numbers of devices is difficult to design. Thus, simulation modeling is required to carefully analyze the designs before implementing them. The smart home network is another high-tech product brought to people by the information age. It uses the existing computer network technology to connect various home appliances and devices in the home, and provides people with convenient, safe and efficient services through the network.

D. *Design Environment (Cisco Packet Tracer)*

The model of the proposed system was created and its operation was simulated using Cisco Packet Tracer 7.2.1. Cisco Packet Tracer is a network simulation which gives room for experimentation with network behaviors as well as allowing the researchers to give conditions to various devices prompting them to perform some task. As an integral part of Networking Academy, Packet Tracer provides simulation, visualization, authoring, assessment and collaboration capabilities. Recently, cisco released a new version of packet tracer that includes IoT services which facilitates the teaching and learning of complex technology concepts.

Figure 1 shows the design environment of Cisco Packet Tracer.

Figure 1. Design environment of Cisco Packet Tracer



E. Some Common Mistakes

- **Security**;

By using this system, the departmental building will be properly secured. It also enables those with the control of the system such as the staff of the department to allow access to those without controls such as the students remotely, into the premises.

- **Ease of use**;

By using this system, smart home appliances can easily be controlled and managed. The system can also be easily used even if someone is not high technology savvy.

- **Convenience**;

It is very convenient to customize the appliances and devices at the department based on one's needs. One can put on or off the appliances and devices in the department at one's convenience with just a touch on the mobile phone or any other internet enabled devices.

- **Energy saver**;

With the smart home system, you can ensure that there is no waste of energy. Smart home systems allow machines, devices and appliances to be managed and turned off immediately after usage thereby ensuring that there is little or no waste of energy.

- **Maintenance**.

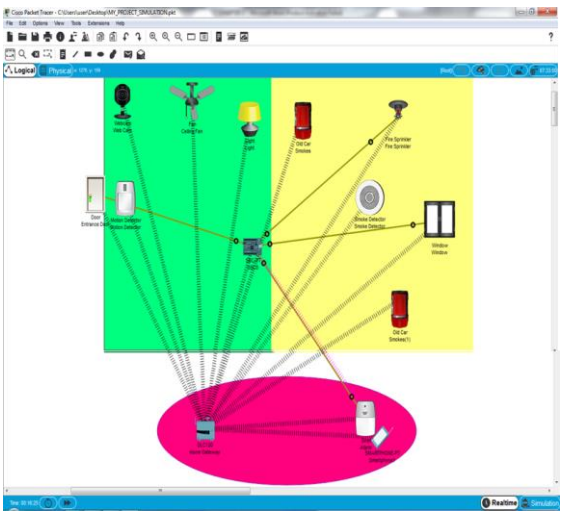
With the use of smart home system, one can easily be notified about the state of any of the device so as to take necessary maintenance actions if needed.

F. Design of the Proposed System

1) Logical design

Figure 2 shows the logical view of the proposed system which shows the abstract demonstration of the data flows, inputs and outputs of the system.

Figure 2. Logical view of the proposed system

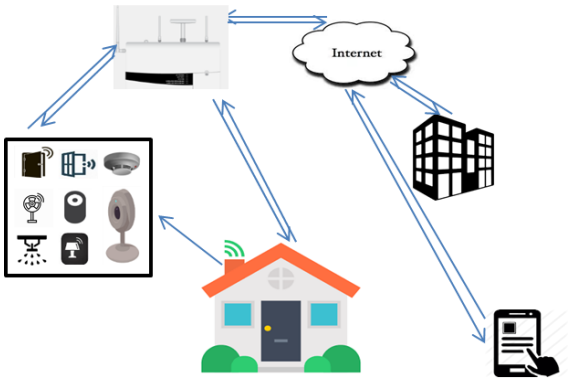


In figure 2, three (3) sophisticated devices were used which include the following:

- **DCL100 Home gateway** is used to register all the smart things such as Webcam, Door, Motion detector, fan, lamp, window etc., by assigning IP addresses to each of them;
- **Single Board Circuit (SBC-PT)** is used to inter-connect different smart objects and provide programing environment with different language such as JavaScript, python, to control the connected smart object;
- **Smartphone** is used to remotely log into the home gateway through the website or application software; view the devices in order to monitor their operations; put on/off some devices.

2) Physical design

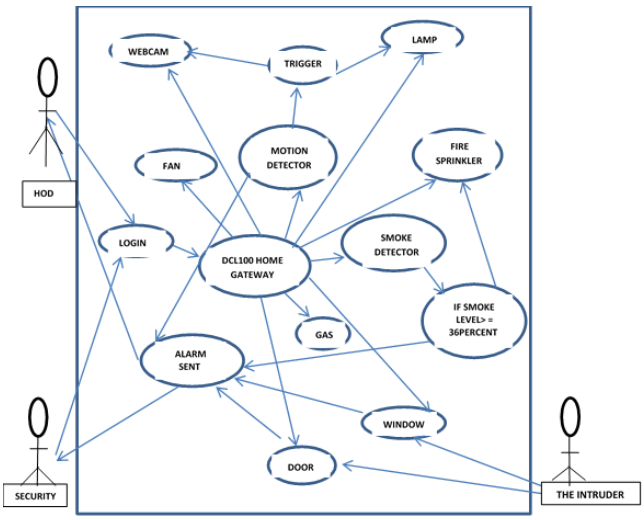
Figure 3. Physical design of the proposed system



3) Functionality of the proposed system (Use Case Diagram)

Figure 4 depicts the use case diagram of the proposed system.

Figure 4. Use case of the proposed system



- **HOD**: The use case of the proposed system by the Head of Department (H.O.D) includes the following:

- **Login**: The Head of Department (H.O.D) uses the correct user name and password to log into the DLC100 Home gateway where the smart things are registered using their respective IP address. After logging in, he gains access to all the smart things registered on the gateway. Then he is able to view the status of the devices and can also switch on/ off some of the devices.

- **SECURITY OFFICER**: The use case of the proposed system by the security officer includes the following:
  - **Login**: The Security Officer uses the correct user name and password to log into the DLC100 Home gateway where the smart things are registered using their respective IP address. After logging in, He gains access to all the smart things registered on the gateway. Then, he is able to view the status of the devices and can also switch or/ off some of the devices.
- **THE INTRUDER**: The use case of the proposed system by the intruder includes the following:
  - **Door**: The intruder may try to burgle into the department through the door. Once this attempt is made, a notification is automatically sent to the mobile phone of the H.O.D as well as the mobile phone of the security officer. Both of them can then log into the home gateway to observe what is going on;
  - **Window**: The intruder may try to burgle into the department through the window. Once this attempt is made, a notification is automatically sent to the mobile phone of the H.O.D as well as the mobile phone of the security officer. Both of them can then log into the home gateway to observe what is going on.

- **The DCL100 home gateway** has the gas, fire sprinkler and smoke detector registered in it. The essence of this smoke detector is to detect the level of smoke in the room. If the smoke level rises up to 36 percent or beyond, the fire sprinkler will automatically be triggered to cool the environment, at the same time, a notification will automatically be sent to the H.O.D and the Security officer's phone. Both of them can then log into the home gateway to observe what is going on;

- **The DCL100 home gateway** also has the motion detector, webcam, smart fan, and smart lamp registered in it. The essence of the motion detector is to sense any movement in the environment. Once the motion detector detects any movement in the department, the web cam and the smart light get triggered automatically in order to monitor what is going on. At the same time, a notification will automatically be sent to the H.O.D and the Security officer's phone. Both of them can then log into the home gateway to observe what is going on.

III. System Implementation and Testing

A. Data Network

A data network is a telecommunications network which allows computers to transmit and receive data. The implementation of our new system requires a broadband Internet access like ZigBee and Z-Wave, with decent speeds. The two most prominent radio networks in home automation are ZigBee and Z-Wave and are both mesh networks technologies which allows for a message to get to its destination through several paths [10].

1) Z-Wave

This is a wireless communication protocol used primarily in smart home networks, allowing smart devices to connect [11]. This protocol employs a Source Routing Algorithm which helps to determine the fastest route a message can take [10]. In addition, every device compatible with Z-Wave is embedded with a code such that when a device is plugged into the system, the code is recognized by the network controller which also determines its location and adds it to the network [10].

2) ZigBee

This is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks [11]. The name ZigBee uses the concept of mesh networking because messages from the transmitter travel in a zigzag manner like bees, looking for the best route to the receiver [10] and its platform is based on the standard set by the Institute for Electrical and Electronics Engineers for wireless personal networks [10]. Zigbee, in addition, supports much lower data rates and uses a mesh networking protocol to avoid hub devices and create a self-healing architecture, in contrast to Wi-Fi networks used to connect endpoints to high-speed networks [11].

B. Network Simulation Program

The modeler used in this work is Cisco Packet Tracer 7.2.1. Cisco recently released this version of packet tracer that include IoT services which will provide a user with assistance like: offering a realistic simulation and visualization of IoT devices, allowing the user to design, build, and configure smart home by providing different smart objects, boards to control the smart objects, and providing detector for sensors. Since it is expensive to buy some networking equipment and smart devices, packet tracer can be used to understand computer networks.

C. Hardware Requirements

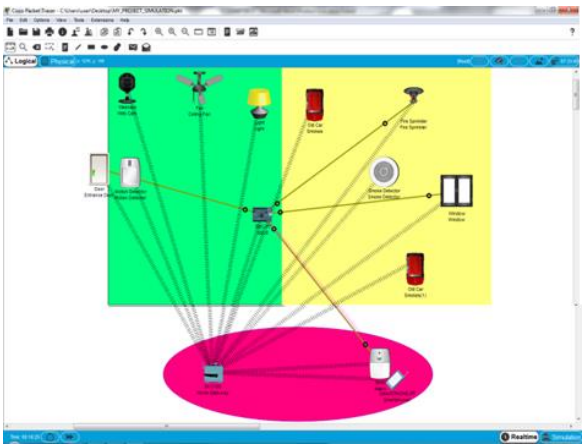
The device used in modeling the network includes:

- DLC Home gateway;
- Single Board Circuit (SBC-PT);
- Smart Things;
- Smartphone;
- IoT custom cables.

D. Network Model

Figure 5 depicts the network model of the proposed system.

Figure 5. Network model of the proposed system



In figure 5, three (3) sophisticated devices were used which include the following:

- **DCL100 Home gateway** is used to register all the smart things such as Webcam, Door, Motion detector, fan, lamp, window etc., by assigning IP addresses to each of them;
- **Single Board Circuit (SBC-PT)** is used to interconnect the door, window, fire sprinkler and the alarm. Then it provides programing environment with different language such as JavaScript, python, to control the connected smart objects;
- **Smartphone** is used to remotely log into the home gateway through the website or application software; view the devices in order to monitor their operations; switch t on/off some devices.

E. Program Documentation

Program documentation indicates some sub programs used in the configuration and their respective functions.

a) IoT custom cable

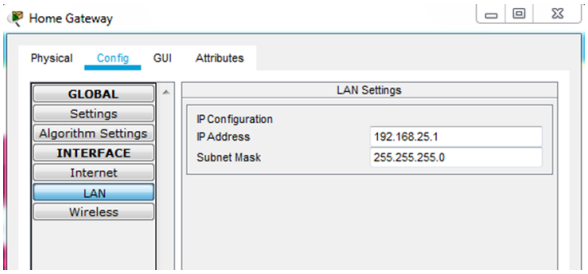
This cable is used to establish network connection that exist between the single board circuit (SBC-PT) and the smart objects. The cable is shown in figure 6:

Figure 6. IoT custom cable

b) Internet protocol address (IP address)

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication [12]. An IP address serves two principal functions: host or network interface identification and location addressing. IP addresses can be determined statically where each computer is assigned internet address by network administrator or dynamically whereby IP address are assigned on demand by another device on the network. In the model of the proposed system, only the Home gateway was assigned IP address manually. All other devices got their IP addresses automatically by DHCP server. Figure 7 shows how the Home Gateway was assigned a static IP address.

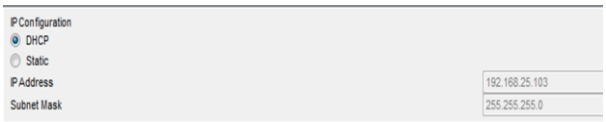
Figure 7. Configuring the Home Gateway



c) Dynamic host configuration protocol (DHCP)

Dynamic Host Configuration Protocol is a client/server protocol that automatically assigns internet protocol address, subnet mask and the default gateway to the host [13]. It is a standard used on IP networks for dynamically distributing internet address protocols and other services. DHCP reduces the need for manually setting the configuration of a host thereby minimizing the stress of the network administrator. It is a protocol that assigns different and unique internet protocol address to devices every time it is connected to the network. In the model of the proposed system, all the devices except the Home gateway are assigned IP addresses automatically by DHCP server. Figure 8 shows the assignment of DHCP to a device.

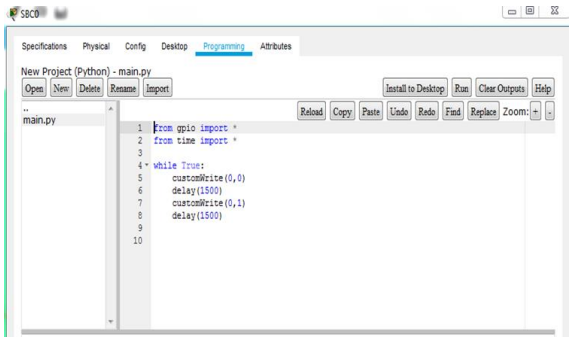
Figure 8. Assigning dynamic address



d) Single Board Circuit (SBC-PT)

Single Board Circuit (SBC-PT) is used to inter-connect different smart object as well as providing programing environment to control the connected smart objects. The different programming languages that can be used to program the SBC includes: JavaScript, python, Figure 9 shows the programming environment of the Single Board Circuit (SBC-PT).

Figure 9. Programming the SBC-PT

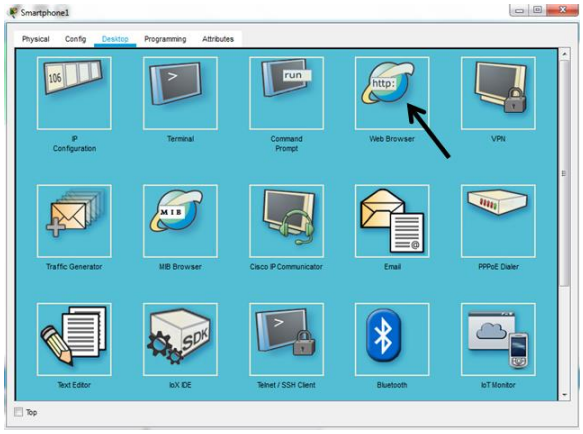


F. Program Interfaces

These are the program interfaces that show the step by step way of executing the model to test its performance.

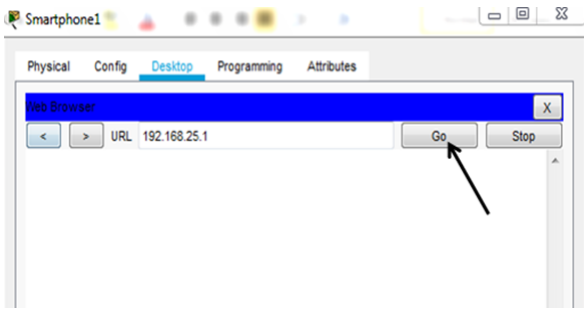
- Double clicking on the smartphone so as to gain access to the desktop environment of the home gateway as shown in figure 10;
- Then clicking on web browser in order to enter the Internet protocol address of the home gateway which is 192.168.25.1;

Figure 10. Desktop environment of the Smart Home



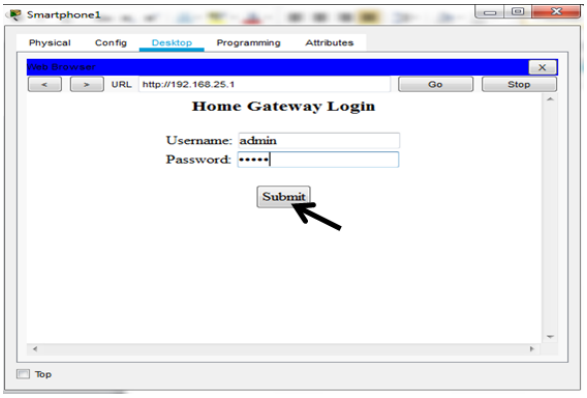
- Entering the IP address 192.168.25.1 at the URL as shown in figure 11, then clicking the **go** button;

Figure 11. Entering the IP address



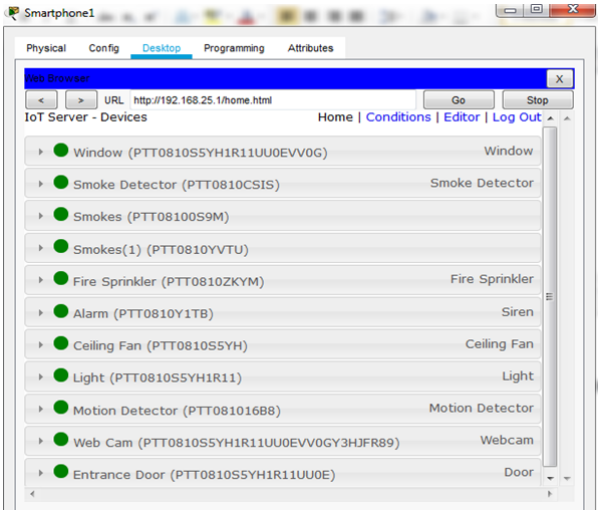
- Logging into the home gateway by using the **username: admin** and **password: admin** as shown in figure 12, then clicking of the submit button;

Figure 12. Home gateway login



- After the submit button is clicked, we will automatically be directed to the Home gateway environment, where we can have access to all the devices registered into it. Figure 13 shows the various devices registered on the home gateway;

Figure 13. Registered IoT devices on gateway



- Figures 14, 15 and 16 depict the various IoT devices registered on the home gateway alongside with their status before implementation. The red colors in each of the devices indicate that they are currently down. While the level of the smoke detector indicate that it is currently at zero level, which means that the environment is smoke free;

Figure 14. Status of registered devices before implementation

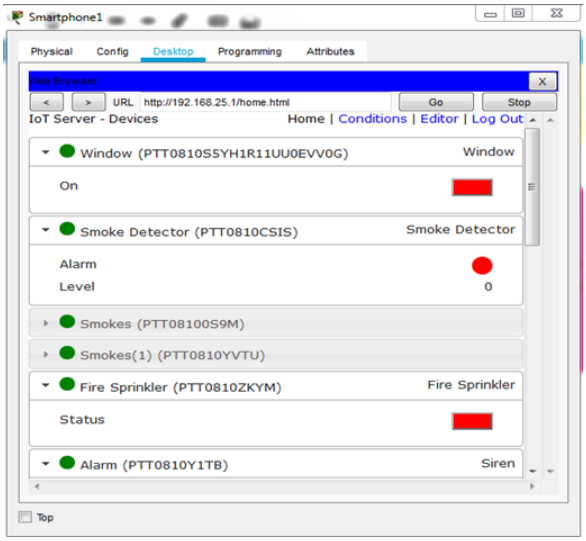


Figure 15. Status of registered devices before implementation

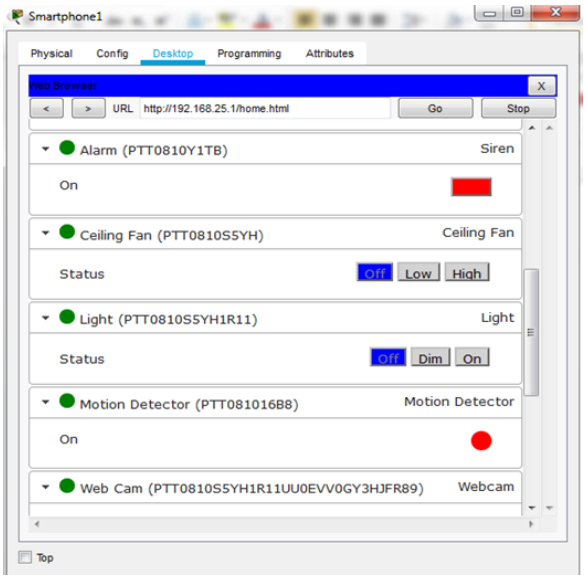
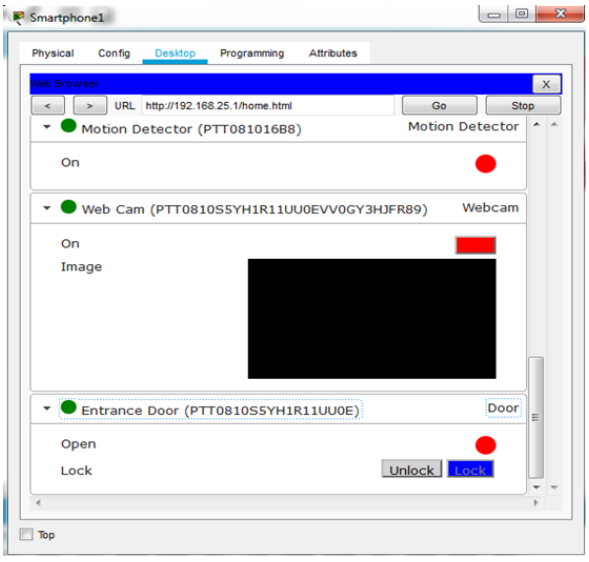
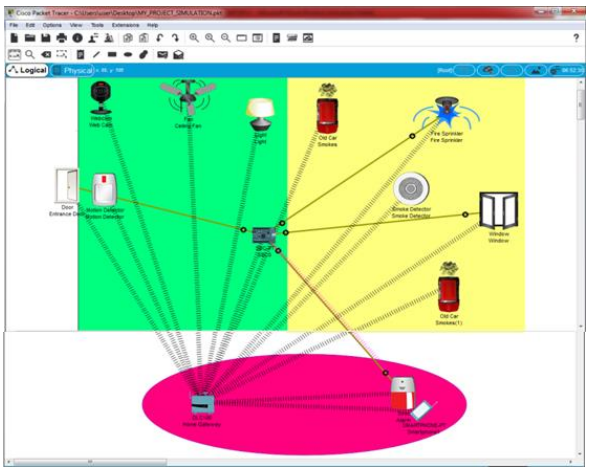


Figure 16. Status of registered devices before implementation



- Figure 17 shows the result of simulation of the proposed system. The system has already been activated. It is evident that if an intruder tries to access the building, a notification will be sent to the user's phone. The blinking alarm is used to represent the notification that will be sent. Also, if the user is able to forcefully gain access into the building, the motion detector will detect his movement and the moment the motion detector senses any movement, it converts the movement into digital signals and automatically send notification to the user's phone, alongside with automatically switching on the smart light as well as triggering the webcam in order to video the intruder. Similarly, the result of the simulation clearly pictured that the old car which is used as a means of emitting carbon monoxide is already powered on, and as soon as the smoke it emits reaches 36 percent, then the fire sprinkler automatically get triggered, and a notification is also sent to the user's phone;

Figure 17. Result of implementation



- Figures 18, 19 and 20 show the status of registered devices after implementation. The green colors in each of the devices indicate that they are currently activated. The level of the smoke detector indicated that it is currently at 36 percent level, which means that the environment is full of smoke. Then, since the smoke level has risen up to this extent, the fire sprinkler gets triggered automatically and a notification is also sent to the user;

Figure 18. Status of registered devices after implementation

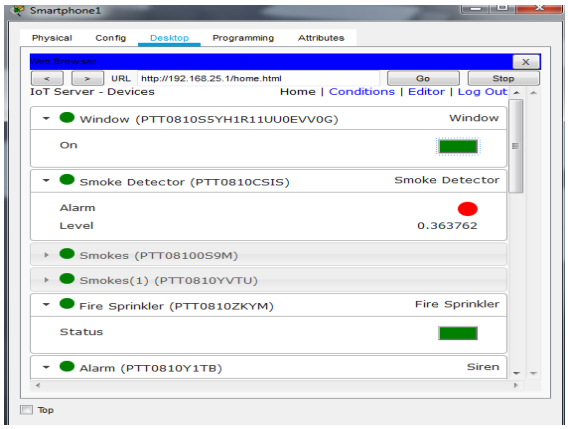


Figure 19. Status of registered devices after implementation

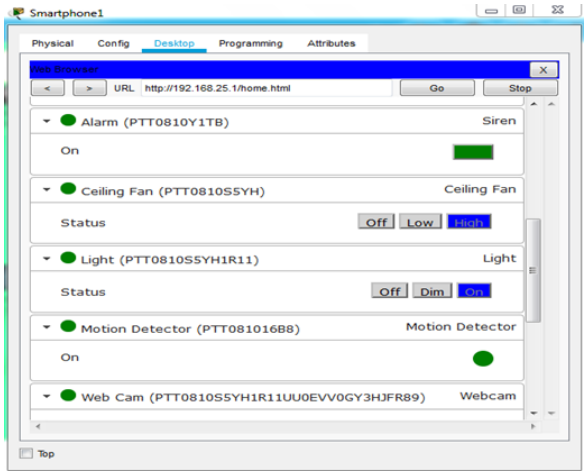
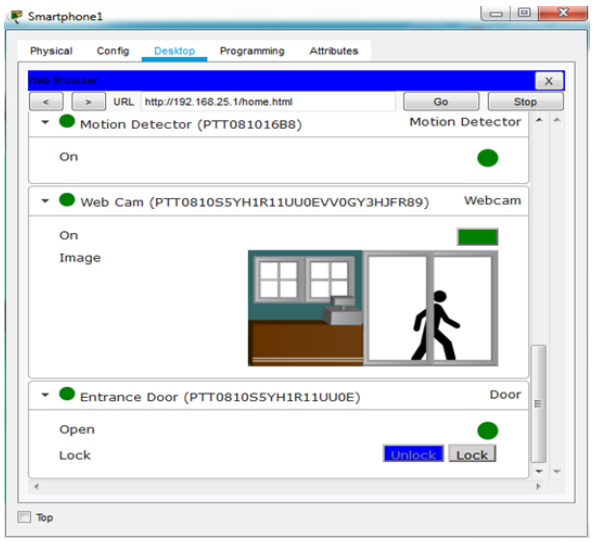


Figure 20. Status of registered devices after implementation



CONCLUSION

This study simulates the model of IoT networks for smart home for the Department of computer science, university of Benin, Benin-City, Nigeria. The system addresses important issues which include intruder detection and the occurrence of fire outbreak. A primary attraction of this system is its ability to be remotely monitored by the authenticated users via the smartphone. One advantage of this system is its ability to detect intruder by receiving notification as soon as the departmental door or window is accessed after which the system has been activated. Another benefit is its ability to detect smoke level of about 36% within the departmental building.

REFERENCES

[1] J., Gubbi., R. Buyya,, S., Marusic and, M. Palaniswami (2013). Internet of things (iot): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.

[2] Y., Jie, and, J. Yie (2013). Smart home system based on iot technologies. Computational and Information Sciences (ICCIS).

[3] A., Ghaffarianhoseini, J. Tookey, H. Omrany,, , A., Fleury, N. Naismith and M. Ghaffarianhoseini (2016). The essence of smart homes: Application of intelligent technologies towards smarter urban future. 79-121.

[4] S., Chattoraj,, and, C.. Subhankar (2015). Smart Home Automation based on different sensors and Arduino as the master controller. International Journal of Scientific and Research Publications. 1-4.

[5] M., Soliman, and, S. Moataz (2013). Smart home: Integrating internet of things with web services and cloud computing. Cloud Computing Technology and Science (CloudCom), 2.

[6] A., Brush , B. Lee,, R., Mahajan, S., Agarwal, S. Saroiu, and, C.. Dixon (2011).. Home automation in the wild: challenges and opportunities. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2115–2124.

[7] E.I Daviess and V.I.E Anireh (2019). Design and Implementation of Smart Home System using Internet of Things. Journal of Digital Innovations & Contemporary Research In Science., Engineering & Technology. 7(1), 33-42.

[8] S., Pirbhulal, H. Zhang , M. E. E Alahi , H. Ghayvat , S. C. Mukhopadhyay, Y.-T. Zhang and W. Wu (2017). A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network. Sensors 2017, 17(1), 69.

[9] M. A. Hoque and C. Davidson (2019) . Design and Implementation of an IoT-Based Smart Home Security System. International Journal of Networked and Distributed Computing 7 (2) , 85–92.

[10] R. J. Robles and T. Kim (2010). A Review on Security in Smart Home Development International Journal of Advanced Science and Technology Vol.(15) , February, 2010. https://www.researchgate.net/publication/228416463.

[11] M. Rouse (2015). Z-wave. TechTarget IIoT agentda. Retrieved April 15, 2020 from https://internetofthingsagenda.techtarget.com/definition/Z-Wave.

[12] R. Kumar and P. R. Shinde (2016).. Computer Network - IP Address & Subnetting. International Journal of Engineering and Advanced Technology (IJEAT) .5(4), 242-246.

[13] Microsoft.com (2016) . Dynamic Host Configuration Protocol (DHCP). Retrieved April 15, 2020 from https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top.