



Design and Execution of Secure Smart Home Environments on Visual Simulation Tool

Basant Kumar^(✉), Hothefa Shaker, and Josephmani

Modern College of Business and Science, Muscat, Sultanate of Oman
{basant, hothefa.shaker, drjosephmani}@mcbs.edu.om

Abstract. The advent of smart technologies is going to be a paradigm shift and game changer in resolving current universal issues such as climate change, cyber-security, health care, mental health, insecure home, food, water, and energy. Evolving smart home systems has been a prodigious and challenging task for engineers, architects, and technologists in real estate owing to the overhead and excess cost of execution and rigorous testing time and process of different types of sensors, smart home appliances, and other sophisticated electronic and electric devices used to transform a real smart environment encompassed with comfort and security. In this paper, we have proposed an amalgam of heterogeneous features of a smart home using a cisco packet tracer simulator encompassed with IoT devices to offer numerous network components that epitomize a factual network configuration and implementation of a diverse prevalent smart home simulation system with an integration of secure message exchange using RSA based Digital signature algorithm and spanning tree protocol (SPT) of VLAN to converge a smart home environment. The proposed layouts of homes on cisco's visual simulator tool called packet tracer are equipped with adequate smart home solutions with a tremendous set of functions to provide ease and comfort, safety, efficacy, and efficiency of digital security in the homes using electronic smart digital devices of the Internet of Things (IoT).

Keywords: Smart home · Packet tracer tool · Internet of Things · Sensors · IoT simulation · SPT

1 Introduction

The arena of ubiquitous computing offers access to information technology infrastructures for end users at anytime and anywhere [1, 2] during this digital information age. The Internet is very elastic. Smart is a word that is separated into five criteria which are Specific, Measurable, Achievable, and Realistic when you combine all of these criteria turns into smart, with the evolving world that we are living in, electronic devices are becoming smart electronic devices, when devices can become smart that means that any electronic device that we see around us can become a smart device from your smartphone that is now a computer on the palm of your hand to your home that can be turned into a smart home. Smart Home diminishes users' participation in observing the settings of the home and monitoring home applications by adding a distinct sensor for automation

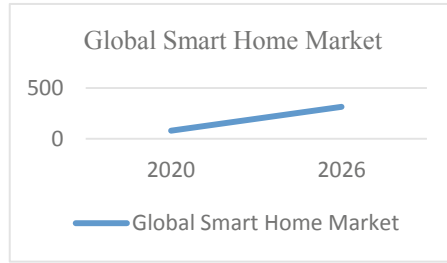


Fig. 1. Global Smart Home Market Trend

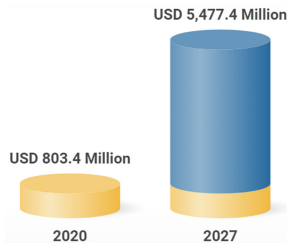


Fig. 2. GCC Home Automation Market Trend

settings [3], which all have the main objective of improving the quality of life that we are living and making it more convenient from the statistical view which is shown in the graph given (see Fig. 1).

The smart home market was valued at USD 79.13 billion in 2020 and is expected to reach USD 313.95 billion by 2026 according to Mordor Intelligence 2020, it shows that the smart home is going to be a prospering market [11]. According to Renub Research (see Fig. 2), the market of GCC Home Automation will grow with a staggering CAGR of 31.55% during 2020–2027 [12]. The impact of smart homes in the world is booming and demand for smart homes is moving at a fast pace therefore companies have presented ideas with their own significant features, although the research that we have gone through we have found that mainly researchers have applied basic features and implemented the default security features which are available in the home gateway router, therefore, we have applied the MCU-PT board which is not outdated but requires professional skills to be installed due to the fact that we have to insert the commands for the board by ourself, which motivated us to implement the (PT-IOT-NM-1W-AC) network adapter for its easy installation. IoT is an acronym of the Internet of Things that denotes distinctively recognizable things and their simulated depictions in global long-haul network setups [4]. IoT is an interconnection of heterogeneous smart devices on massive networks [5]. Cisco Packet Tracer 8.2 is a powerful visual communication tool acquainted to program our own smart solution to add numerous simulations to analyze network traffic, add Internet of Things (IoT) devices, and integrate programming code and hence has been used to build a framework of how a simple smart home can be automated with the use of the various IoT devices based on the application where all the devices are

connected together relying on the backend intelligence that we have set for them to be fully automated to work simultaneously, where we will be exploiting security features to secure the different layers more specific application layer, transport layer, and network layer of the smart home to mitigate the risks that can arise in a smart home. With the dawn of advancement in Information technology and in view of the instantaneous increase of senior citizens, crimes in society, to economize electricity, water, and gas bills, environmental protection, intrusion alarming, to provide a better and luxurious home living, dire needs of both husband and wife's engagement to earn more money to meet their life-saving requirements and consequently keep their child and elderly people alone at home with greater risks. However, smart home concepts can be introduced to face and mitigate these challenges to monitor and supervise elderly people and adolescents through smart components of the smart home with greater efficiency.

2 Motivation

The current release of the Cisco Packet Tracer is encompassed with additional features of IoT devices, smart sensors, microcontrollers, and a gateway to perform simulation works without having any physical network setup [6] which can be costly to do. Through this simulation prototype, a smart home simulation can be administered. The new Cisco Packet Tracer 8.2 version is the IoT power adapter (PT-UNV-PMW-ADAPTER) that allowed us to configure the Internet of Things (IoT) device to connect wirelessly to the home gateway, whereas in the past versions they were relying on using MCU-PT board, which can be referred to in the modern days as the raspberry pi board. One of the main advantages of using the Cisco Packet Tracer in this paper is that it does not only allow us to configure smart homes but we can also configure smart cities, smart campus and smart farming with the supply of various smart devices, which makes planning, creating, and customizing smart cities less complex where it can be the base framework for the physical framework in the future.

3 Methodology

The proposed tool Cisco Packet Tracer 8.2 in our research permits learners to design network interfaces in real-time as well as in simulation mode without purchasing expensive network hardware [8]. In our proposed network layout as shown in Fig. 3. The home gateway has been used to control the IoT devices and star topology that allows every device to connect to the central device. In addition, it is easier to install because we will be using a wireless connection to connect all the devices which means that it's going to be less expensive to configure, secondly, the maintenance cost will be cheap compared to other network topology, therefore we will be able to identify a faulty link easily. However, it has its disadvantages as if the hub goes down then the whole network will be down therefore for a contingency plan, we made another hub that is identical to the main hub, which turns on when the main hub is down, to resume functionality till the main hub is fixed. In this paper, we have emphasized our research on the integration of smart devices and network security of smart homes [7]. Python programming is done to apply garage lighting, room temperature monitoring, and kitchen smoke monitoring from security perspectives [9, 10].

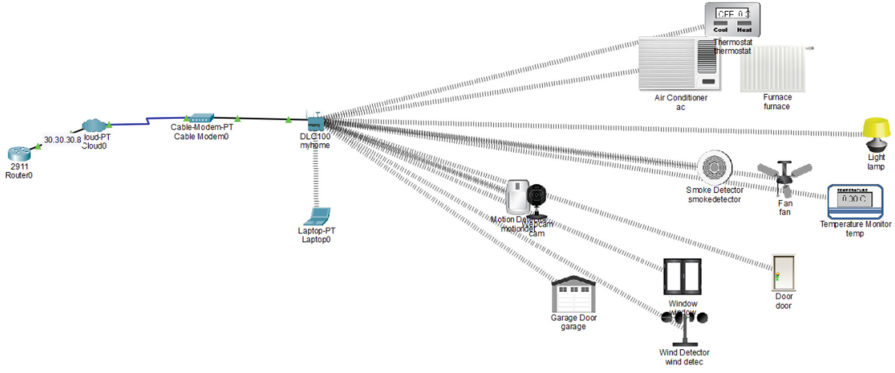


Fig. 3. Proposed Network Layout

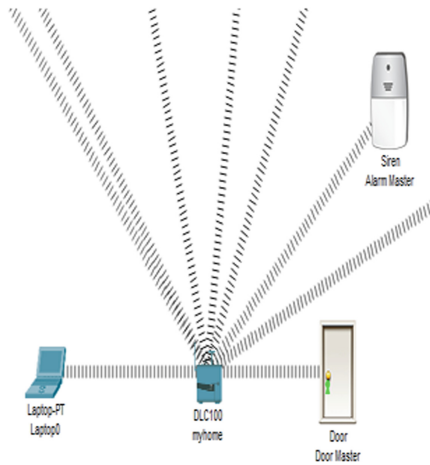


Fig. 4. Home Gateway Router

3.1 Network Topology

This network topology (see Fig. 4) shows a laptop is connected to a home gateway router DLC-100 which is a router from cisco that allows IoT devices to be interconnected in the network, this router it allows the owner to set certain conditions for their home from trip sensor notifications, smoke detectors, and home temperature.

The flowchart as shown in Fig. 5 depicts the diagrammatic representation to add and configure network devices such as routers, switches, and end devices including IoT devices to create a smart home prototype and thereafter simulate all these devices as a prototype of the smart home environment. When connecting the Internet of things (IoT) devices we will be using the DLC-100 home gateway router which will allow us to connect to the IoT server that allows monitoring with the help of the home Gateway Router. The system that the house owner feels that he needs from a simple home to a fully secure home with all the sensors and cameras, to an elderly smart home that has

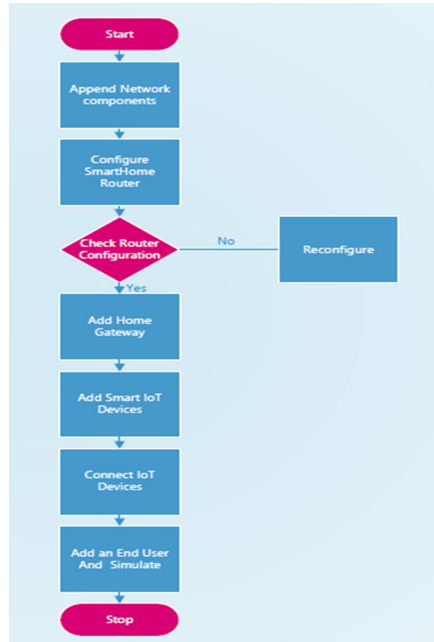


Fig. 5. Smart Home architecture process

health monitoring devices being connected to the internet for any emergency support needed, this topology is mainly for a person that has an interest in the computer field and is worried about the privacy of his own home, where also it can be done by professional hands to make more convenient to elderly people.

For doing this experiment we have chosen to go with network topology for these main factors:

- Flexibility of the network topology with no restrictions.
- Cost of equipment and maintenance is low compared to the first network topology.
- Custom security features that can be done.
- The choice of isolating the network from the cloud or the internet.

3.2 IoT Simulation

In this paper we will be explaining how the IoT simulation is going to operate in different scenarios, we will be discussing the methodology that we used in-depth and lay down the steps on how to configure the IoT servers.

The smart home is known to be smart because it has its own intelligence to react to certain scenarios where it varies from altering the temperature of the house to turning on the alarm when there is an emergency, in this simulation we have customized the intelligence of the IoT device to a level that can be changed in future if needed.

Here we have listed all the devices and their functions as shown in Table 1.

Table 1. Smart devices and their function

Router (1941)	To interconnect the home network with Mux of ISP
Home gateway DLC-100	Used to register the smart device to the IoT server and provide each device with a unique IP address.
PC/Laptop	A computing device that allows the user to access the network if he has the privilege to do so.
Fan	Used for circulating the air in the area.
Webcam	Provides visual surveillance.
Siren/Alarm	Provides sound attention when needed.
Light/Lamp	Provide light.
Motion detector	Detects motion in its coverage area.
Smart Door	Can be linked to other IoT devices through the IoT server to provide event-based functions.
CO Detector	Used to detect the level of CO in the area.
CO2 Detector	Used to detect the level of CO2 in the area.
Smoke sensor	Used to detect the level of smoke in the area.
Temperature sensor	To monitor the temperature in the area.
Fire sprinkler	In case of a fire, the sprinkle will release water.
Old car	To simulate the smoke, CO, and CO2 in an area with sensors.
Air Condition	To cool the house.
Smart window	Can be linked to other IoT devices through the IoT server to provide event-based functions
Fire Monitor	It has sensors to detect if there is any fire in the area.
Trip sensor	It will give a notification if someone interrupts its laser
Garage Door	Can be linked to other IoT devices through the IoT server to provide event-based functions
RFID Reader	To read custom-modified RFID cards to allow access.
RFID Card	A chip that can be configured to be read by the RFID reader.
Wind detector	Detects the speed of the wind.

The following are the scenario's that we have created and the conditions that we have set for the IoT devices to follow: Note: all these scenarios will be using the network adapter (PT-IOT-NM-1W-AC) which can connect to the DLC-100 home gateway router.

The Bedroom Scheme

The bedroom is a room where you want it to be comfortable whenever it is needed with this simulation you will be able to configure the room temperature to a certain range for it to provide you with the optimal comfort you need using the AC, Furnace and temperature monitor (see Figs. 7 and 8), also we will configure it with an alarm that will

go off and windows to be opened to assist in solving the emergency when a smoke or a fire is detected in the house using the smoke detector (CO or CO₂) or the fire monitor, where also you will have you a main laptop that is connected to the home gateway where you can control all of the **IoT devices** that you have. This is all done by setting specific conditions in the **IoT server** which are shown in Fig. 6(a).

The Garage Scheme: For this scenario, it is mainly to configure garage doors and their automation, for this we will be using motion sensors to detect the motion of the car so that the garage door will be open to allow the car to enter the garage as shown in Fig. 9 and Fig. 10. When the car enters the garage the lamps in the garage is open to allow the driver to see where to park his car, on top of that we have implemented safety and security measures if person parked his car and when the motion detectors do not detect any movement the garage door automatically closes but the lamps are still on till the person enters the house and the trip sensor is true then the lamps in the garage are closed to save energy, for the safety measure we have added smoke, CO and CO₂ detectors along with a fire monitor that activates the fire sprinkle in case of a fire, as shown in Fig. 6(d,e,f).

Outer Perimeter Scheme

This is to control the outer perimeter of the house mainly for security purposes we have used the trip sensor to detect movement and lock the doors and sound the alarm if an intruder has gained access to the house perimeter, also if there is a smoke or wind we have implemented smart windows (see Fig. 11 and Fig. 12) that with conditions like smoke, CO or CO₂ being higher than the normal level the windows will open to help in removing the gas or smoke from the house, conditions are shown in Fig. 6(c,d,e,f).

3.3 Smart Home Configuration

In this paper we will be presenting the steps to configure a smart home in packet tracer we start by creating a new PKT (packet tracer file) which is used to create the network topology, configure devices, and simulate a network.

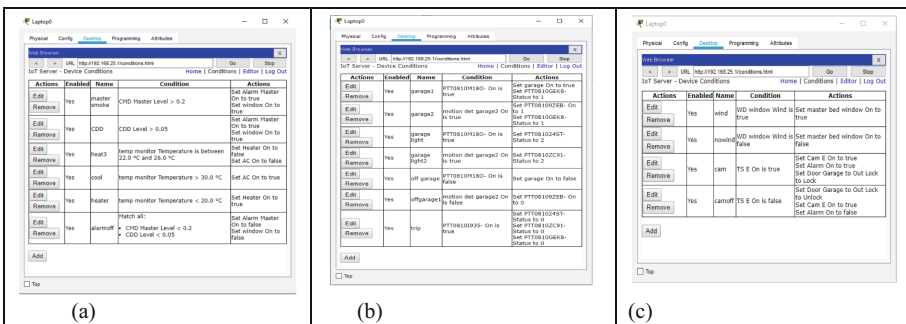
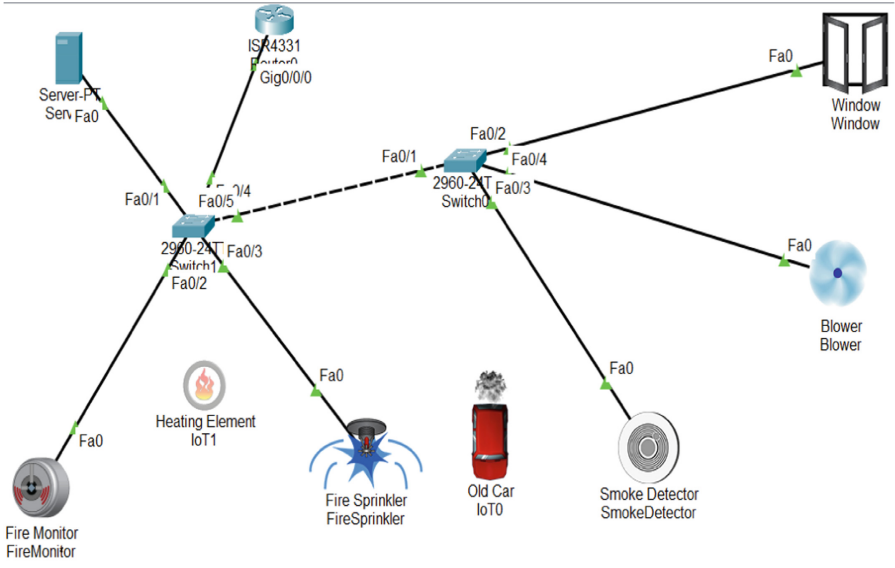
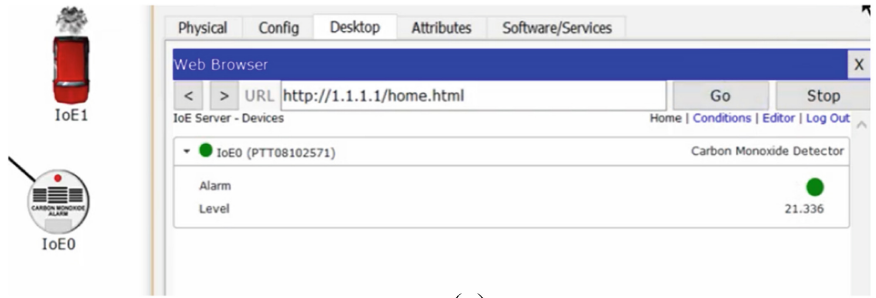


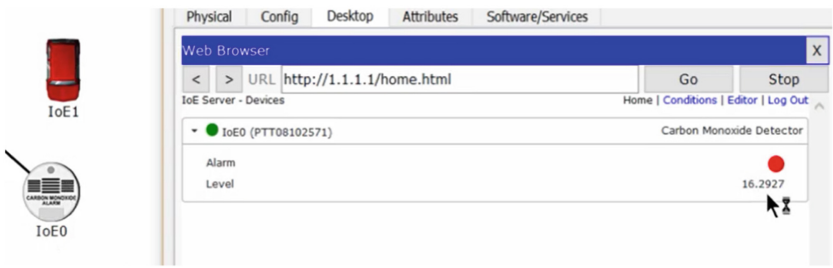
Fig. 6. (a) Bedroom scheme (b) Garage Scheme (c) Outer Perimeter Scheme (d) Fire and smoke detection (e) Gas detection on normal level (f) Gas detection on high risk level



(d)



(e)



(f)

Fig. 6. (continued)

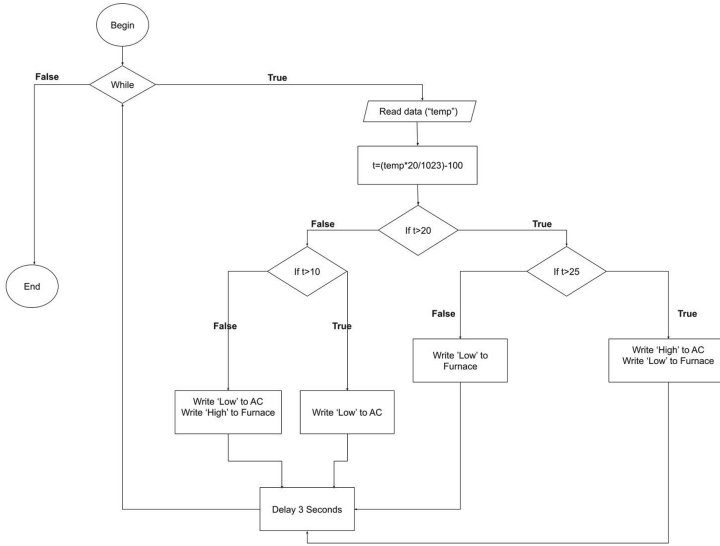


Fig. 7. Room temperature Monitoring flowchart.

```

1  from gpio import *
2  from time import *
3
4  def main():
5      pinMode(0, OUT) #Window pin
6      #A0 is the smoke sensor pin
7      MIN=2.0
8      MAX=20.0
9      while True:
10         smoke=float(customRead(A0))
11         if smoke<MIN:
12             customWrite(0,[0])
13         elif smoke>MAX:
14             customWrite(0,[1])
15         sleep(1)
  
```

Fig. 8. Room temperature Monitoring python code

We started by grabbing the router into the framework then we start inserting the rest of the devices needed for the framework from IoT devices to routers, switches, and home gateways.

After that we need to configure the IoT devices that we are using by modifying them with the network adapter that we are meant to use in this framework we will be using the network adapter PT-IOT-NM-1W-AC which allows us to be able to connect to the home gateway through a wireless connection which will make us save in the cost of wiring, by selecting the advance button in the IoT device then choosing the network adapter we choose as shown in Fig. 13.

After configuring the IoT device to use this network adapter then we will have to add the configuration of the network that we will be connecting to the home gateway, by adding the network SSID (Service Set Identifier) and the password of the network for the IoT device to connect directly to the network, which is demonstrated (see Fig. 14).

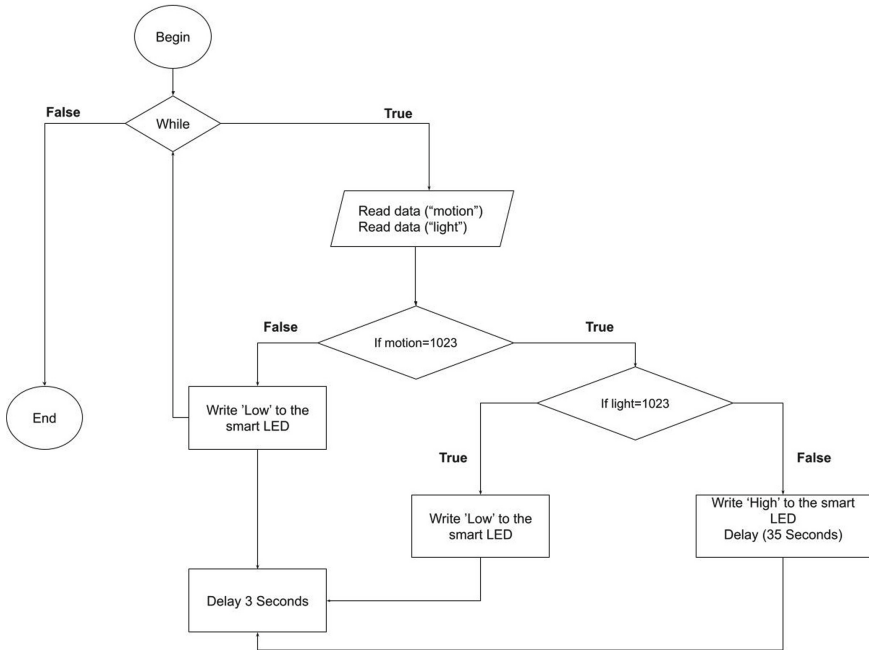


Fig. 9. Garage lighting flowchart

```

1  from gpio import *
2  from time import *
3
4  def main():
5      pinMode(0, IN) #Light sensor pin
6      pinMode(1, IN) #Motion sensor pin
7      pinMode(2, OUT) #Smart LED pin
8      print("Getting data...")
9
10     while True:
11         motion=analogRead(1);
12         light=analogRead(0);
13         if (motion==1023):
14             if (light==1023):
15                 analogWrite(2, [0]) # [0] --> "Low"
16             else:
17                 analogWrite(2, [1023]) # [1023] --> "High"
18                 delay(35000)
19         else:
20             analogWrite(2, [0])
21             delay(3000);
  
```

Fig. 10. Illustrates the Garage lighting python code

Lastly, we go to the Global settings and scroll down to the IoT server and select the Home Gateway, this will allow the device to be registered to the IoT server that will be controlling the functions of the IoT devices in the network without this being chosen it will be registered as a normal device and not an IoT device is to be controlled by the home gateway, therefore, the device is giving the router permission to control this

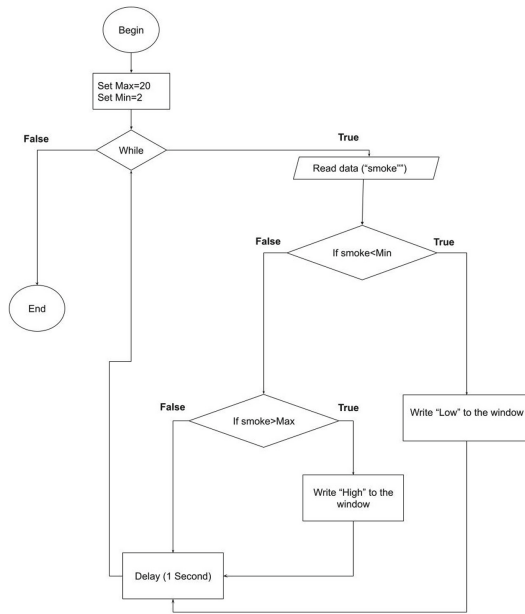


Fig. 11. Kitchen smoke monitoring flowchart

```

1  from gpio import *
2  from time import *
3
4  def main():
5      pinMode(0, OUT) #Window pin
6      #A0 is the smoke sensor pin
7      MIN=2.0
8      MAX=20.0
9      while True:
10         smoke=float(customRead(A0))
11         if smoke<MIN:
12             customWrite(0,[0])
13         elif smoke>MAX:
14             customWrite(0,[1])
15         sleep(1)
    
```

Fig. 12. Kitchen smoke monitoring python code

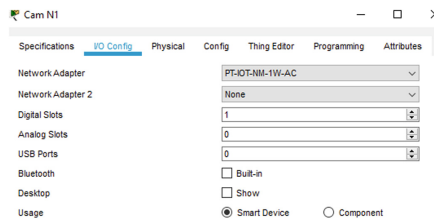


Fig. 13. Network adapter PT-IOT-NM-1W-AC

The screenshot shows the configuration for the 'Wireless0' interface. Key settings include:

- Port Status: On
- Bandwidth: 300 Mbps
- MAC Address: 0001:63C5:9B21
- SSID: HomeGateway
- Authentication:
 - Disabled
 - WEP
 - WPA-PSK
 - WPA2-PSK
 - WPA
 - WPA2
 - IEEE 802.1X
- Encryption Type: Disabled
- IP Configuration:
 - DHCP
 - Static
- Pv4 Address: 192.168.25.102
- Subnet Mask: 255.255.255.0
- Pv6 Configuration:
 - Automatic
 - Static
- Link Local Address: FE80:201:63FF:FE05:9B21

Fig. 14. SSID: Home Gateway

The screenshot shows the configuration for 'Cam N1' in the 'Config' tab. Key settings include:

- Display Name: Cam N1
- Serial Number: PTT08105XPC-
- Gateway/DNS IPv4:
 - DHCP
 - Static
 - Default Gateway: 192.168.25.1
 - DNS Server: 8.8.8.8
- Gateway/DNS IPv6:
 - Automatic
 - Static
 - Default Gateway: [Empty]
 - DNS Server: [Empty]
- IoT Server:
 - None
 - Home Gateway
 - Remote Server
 - Server Address: [Empty]
 - User Name: [Empty]
 - Password: [Empty]

Fig. 15. DHCP Server configuration

device as the conditions in the router are set as shown in the Fig. 15 of DHCP server configuration.

4 Implementation

When we repeat this process to each device and make sure that it is connected to the network then it will look like the below picture as shown in Fig. 16 showing that everything is connected.

Now we start with the conditions of the IoT devices which were discussed in the scenario section done in the home gateway we need to access the router's default IP

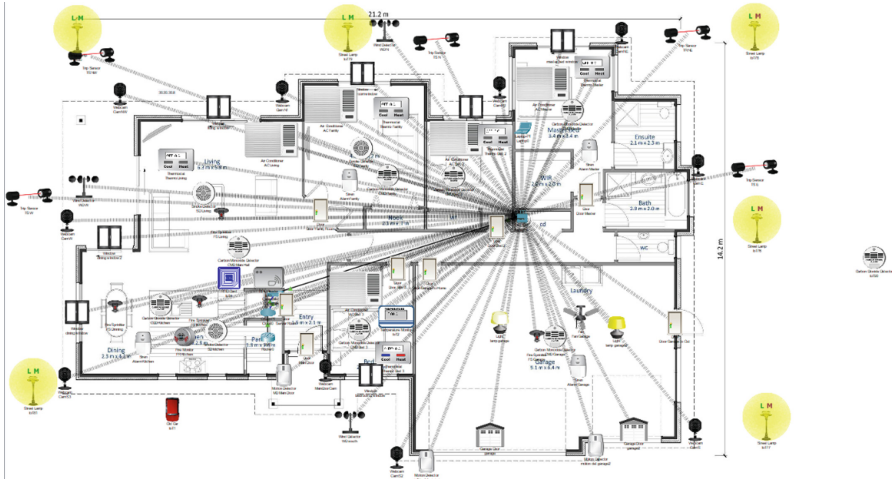


Fig. 16. Smart Devices of Smart Home

address and from there it will take us to the registration server which is the place where we control our IoT devices that are connected to our network and set their conditions for them to work on the way we want them, the main benefit of this system that it is fully customizable for the preference of the user. The implementation consists of three parts: the smart home, internet cloud, and IoT server [13].

4.1 Security Features

The security features that we will be implementing in our network are the following:

- Basic switch and router security which includes adding a password and changing the hostnames.
- Encryption of the password and using a secret password.
- Configuring the SSH connection.
- VLAN configuration.
- MAC address filtering.
- Access control list. Below are the steps that we have done to secure the smart home network which consists of two-part switch hardening and router hardening.

4.2 Switch Hardening

```
Switching to the configuration terminal
no ip domain-lookup
Enabling the password for the configuration terminal
enabling a secret password
password projection
line con 0
exec-timeout 0 0
```

config the VTY line which stands for the virtual terminal lines of the router
In this simulation, we will be configuring two pcs to do that we have to follow the current steps when in the configuration terminal.

```
“line vty 0 4”
```

We can set a password “vty”

```
“password vty”
```

```
“login”
```

Now for the other pc

```
“line vty 5 15” “Password vty2”
```

```
“login”
```

To Configure the banner to show whenever we connect to the device command line interface

```
“banner motd ^ our msg here ^”
```

This will configure the message of the day whenever we log into the device.

Now we will be encrypting the password because if anyone hooks up their line and turned on Wireshark, they can get out passwords Now to do that we have to go to the configuration terminal and write the following commands

```
“service password-encryption”
```

Now all the passwords on our device are encrypted to show you that we can go to privilege mode and write the following command to show you that our passwords are encrypted

“show running-config” There are two types of passwords: type 5 and type 7.

The type 5 password is the MD5 hash which is used in the secret command and is very hard to crack, but type 7 uses a weak algorithm that can be easily reversed. Right now we are connected through telnet which is not secure so now we will be configuring SSH which is a secure shell and a secure connection that has encrypted ssh uses port 22 so if we do have a firewall in our network then we have to make sure the port 22 is open so that we can access the ssh Now we will be configuring the ssh connection We will be creating a domain name which can be done by this command in the configuration terminal “ip domain-name mcbs.local” Then we will have to create a username and set the privilege range from 0 to 15, 0 means we have no access what so ever so we will set it to 15 by typing this command if we have privilege level 15 it will take us straight to enable mode level access also configure a secret password with it which will be “Basant” “username Basant privilege 15 secret Basant” And then we must configure the crypto key generator for secure access of the ssh by using this command “crypto key generate rsa” Then we will be prompted to choose the size of the key which will range from 360 to 2048 the bigger the number the harder it is to crack.

Choose the size of the key “1024” as shown in Table 2. Configure the SSH version by using this command in the configuration terminal “ip ssh version 2”. Use version 2 because it is more secure than version 1 Then we start configuring the VTY lines First, we have to go into the line vty from the configuration terminal by using this command “line vty 0 15” Set the VTY line to local check the password with this command “login local”. Now all the communication will be done through SSH protocol by typing this command “transport input ssh”.

Table 2. Router and their size of the key

Router	360 bits	512 bits	1024 bits	2048 bits (maximum)
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	More than 1 hour
Cisco 4700	Less 1 second	1 second	4 seconds	50 seconds

4.3 Router Hardening

Firstly, change the hostname in the configuration level

ProjectRouter

“no ip domain-lookup” “enable password projectr” “enable secret projectr1”.

Now this password is encrypted as shown using the show running-config command.

“password projectr3” “login”

While we are in the line console, we configure the device to not time out when we are away from the keyboard by using this command “exec-timeout 0 0”

This will configure the device to never time out when we are using it. Then we start configuring the VTY lines by going to the configuration level and from there to the line vty 0 15 to configure them and set a password by using this command “password project4” “login”. Now we configure the banner message of the day which will show whoever is trying to access the device on who this device belongs to and all of that so I typed in this message for the day to do that you need to go to the configuration level and type the following command “banner motd ^. This will set a message for every time you try to connect to the device it will show you this message “line aux 0” “password aux0” “login” show running config it will show us that we can see all the passwords that we used so if someone is using wireshark in our network it can see all these passwords so we encrypt them by going into the configuration level and typing in the following command: “service password-encryption” Now we need to configure the SSH which uses port 22 the default remote connection that the router uses is the router So now we need to configure the domain name by going to the configuration level and typing the following commands “ip domain-name mcbs.local” Then we need to give it a username and a password “username basant privilege 15 secret projectr” This command creates a username which has a privilege level 15 which means he can access and alter the configuration in the router as he pleases with also a secret password that will be prompted whenever he wants to log in to the device. Now we need to create the crypto key in the configuration level so that whenever we connect to the device the channel that we will be using is going to be encrypted using this key by typing these commands “crypto key generate rsa” “ip ssh version 2” “line vty 0 15” And then type the following command

“transport input ssh”

4.4 VLAN

We create a VLAN by going into the configuration level and we type the following command

```
“vlan 10”
```

Which will take it to the vlan 10 configuration where can set a name for it by using this command “name finalproject”. For security reasons we created a vlan to keep all the unused port in and we named it “unused” Now for us to move all these unused ports we need to type in the following command in the configuration level “interface range f0/1–24”

```
“switchport mode access”
```

```
“switchport access vlan 99”
```

```
“shut”
```

```
“int f0/1”
```

```
“switchport access vlan 10”
```

“no shut”. We have been implementing STP (spanning tree protocol) to control the looping and single point of failure issues in the network. In case link1 is failed then automatically link2 will be enabled and using FF forward state link will be established between switch A and Switch B users using STP protocol. Again if the main link is active then automatically the second link will be blocked.

4.5 Signing and Verifying a Message in Home Network

For signing and verifying a message RSA digital signature scheme as shown in Fig. 17 is applied as given below

$n = pq$ here p and q are 2 prime nos

$\Phi(n) = (p-1) \times (q-1)$

$ed = 1 \pmod{\Phi(n)}$ $ed \pmod{\Phi(n)} = 1$

e = public exponent

d = private exponent

Encryption $C = M^e \pmod{n}$

Signing $S = M^d \pmod{n}$

Verifying $M' = S^e \pmod{n}$

$M = C^d \pmod{n}$

Is $M' = M$

We also propose applying VLAN to secure Smart home devices to secure the home network. Generally, any Smart home or IoT device on the network will have complete access to all other devices on the network, and hence VLANS on the home network can play a significant role to mitigate security and privacy risk. In the case of redundancy topology to avoid a single point of failure we propose to implement SPT (spanning tree protocol) (Fig. 18).

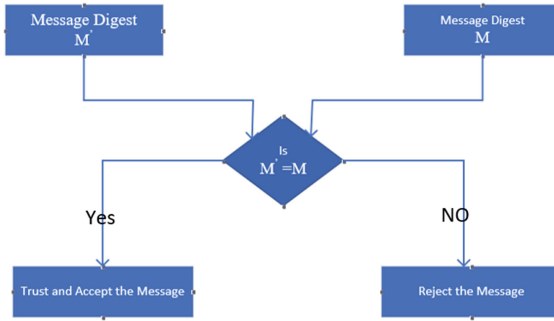


Fig. 17. Signing and Verifying a message

```

Switch#
Switch#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
Address    0002.168B.18E2
Cost       19
Port       2(FastEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
Address    00D0.5868.878B
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/2        Root FWD 19        128.2    P2p
Fa0/1        Altn BLK 19        128.1    P2p
Switch#
Switch#
Switch#
  
```

Fig. 18. SPT in VLAN

5 Conclusions

The human population is growing rapidly and hence there is a need for smart homes encompassed with smart devices to leverage effective and efficient use of energy, home appliance, safety, and security, environmental controls, and intrusion alarming. With the advent of advancement in Information technology and in view of the swift rise of senior citizens, the rate and frequency of crimes in the city and the inevitable need for parent’s engagement to earn money and keep the child and elderly people alone which can be supervised and monitored through smart components of the smart home. Lots of projects are knocking at the door in view of the current requirement of the inhabitants and hence an arena of the smart home is definitely going to be a smart choice. The proposed research is the depiction of a technological revolution in smart homes and how this may be implemented in reality. To avoid MAC Flooding and a single point of failure in the home network we have proposed the SPT protocol of VLAN which is encompassed with a signing and verifying algorithm using RSA Digital signature in view of secure

message exchange at smart home. Nothing is permanent but change and hence testing all possible network designs and their interface and appending smart IoT devices with enriched libraries of python programming and JavaScript compatible with packet tracer (virtual simulation tool) will be a milestone of success in the future for the smart city, smart campus architecture, smart farming, and smart grid.

The tracer tools and their simulation results are far essential and impendent to economize time and money before stepping into the actual hardware setup.

References

1. Mark Weiser, Ubiquitous Computing. Nikkei Electronics, pp. 137–143 (2013).
2. M. Weiser, The Computer for the 21st Century. American Science, pp. 3–9 (1991).
3. Soliman, Moataz, et al., Smart home: Integrating internet of things with web services and cloud computing. Cloud Computing Technology and Science (CloudCom), IEEE 5th International Conference on. Vol. 2(2013).
4. Jie, Yin, et al. ; Smart home system based on IoT technologies. Computational and Information Sciences (ICCIS) (2013).
5. Maguluri, Lakshmana Phaneendra.: Efficient Smart Emergency Response System for Fire Hazards using IoT. International Journal of Advanced Computer Science and Applications. Vol. 9, No. 1,314–320(2018).
6. Rambabu K., Venkatram N.:Traffic flow features as metrics (TFFM): Detection of application layer level DDOS attack scope of IOT traffic flows. International Journal of Engineering and Technology (UAE). 7(2): 203-208(2018).
7. T. Mendes, R. Godina, E. Rodrigues, J. Matias, and J. Catalao. Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources, vol. 8, no. 7. [Online](2017). Available: <http://www.mdpi.com/1996-1073/8/7/7279/>
8. Muzammil Parvez M., Shanmugam J., Mohan Rao K.R.R., Lakshmana C., Shameem S.: Alive node and network lifetime analysis of DEEC protocol and EDDEEC protocol. International Journal of Engineering and Technology (UAE). 7(Issue) 661–664, ISSN: 2227524X(2018).
9. Ashok G.L.P., Saleem Akram P.: Implementation of smart home by using packet tracer. International Journal of Scientific and Technology Research. 9(2): 678–685 ISSN: 22778616 (2020).
10. V. Dankan Gowda, S. B. Sridhara, K. B. Naveen, M. Ramesha and G. Naveena Pai.: Internet of Things: Internet Revolution, Impact, Technology Road Map and Features. Advances in Mathematics: Scientific Journal. 9(7): 4405-4414N:1857-8365 (2020).
11. Smart homes market - growth, trends, covid-19 impact, and forecasts (2022 2027). <https://www.mordorintelligence.com/industry-reports/global-smart-homes-market-industry>
12. GCC Smart Homes Market by Countries, Application, Company Analysis, Forecast. <https://www.renub.com/gcc-smart-home-market-p.php>
13. G.L.P Ashok, P. Saleem Akram, M. Sai Neelima, J. Nagasaikumar, A. Vamshi.: ‘Implementation Of Smart Home By Using Packet Tracer’, International journal of scientific & technology research, vol.9(Issue. 2)(2020)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

