

## IoT Based Home Automation

Abu Bakar Siddique Kamboh<sup>1</sup>, Sanaullah Memon<sup>2</sup>

### Abstract:

IOT or the internet of things is an upcoming technology that allows us to control hardware devices through the internet. Here we propose to use the IOT in order to control home appliances, thus automating modern homes through the internet. The main purpose is to control any electric supply equipment load through the Internet network over cloud remotely on the basic principle of the Internet of things (IoT). In this proposed research work, the real-time scenario the electric load can be monitored as well as configured through web-based applications. The data sent from any password protected device through a webpage. A Wi-Fi adapter is configured with the wireless modem to access the internet. The received internet commands are put into the Wi-Fi module. IoT offers a wide scope of new advancements for observing and controlling, of clever structures and keen homes, by improving security to lessen vitality and support costs. With the home computerization control framework, we make our home gadgets shrewd. Savvy, as in, the gadgets can be checked or perform a task as per the client's guidelines. For instance, an entryway lock framework where on the off chance that anybody obscures individual attempts to go into the house without approval, at that point the entryway, lock will initiate an alert connected to the entryway and in this we can say our house is sufficiently brilliant to give us security.

**Keywords:** *Internet of Things (IoT), Cloud, IPv4, Machine to machine (M2M), OSPF, DHCP.*

### 1. Introduction

The Internet of Things (IoT) is a name that has been broadly perceived since the late 1990s. The IoT is an arrangement of physical things that open through the Internet. The term "Internet of Things" (IoT) was first used in 1999 by British technology pioneer Kevin Ashton to describe a system in which objects in the physical world could be connected to the Internet by sensors. The IoT is highlighted as one of the most important future technology and is getting vast attention from all over the world [1].

Homes of the 21st century will turn out to be increasingly more self-controlled and robotized because of the comfort it gives, particularly when utilized in a private home. A home robotization framework that enables clients to control electric apparatuses of a differing kind.

The primary registering gadgets (PCs) were monsters, a room-sized mechanical assembly that took groups of individuals to configuration, handle and keep up. Nowadays, they are exponentially quicker and just a variety of the extent of their ancestors. A gadget is electronic appliance that performs computations dependent on these principle segments: a processor, storage, and Input & output unit.

The smart thermostat runs the program by using a processor, store the programs of temperature parameters in storage and other data, and an I/O (screen, show, sound cautions, and so on).

### 2. Background

IoT aims is to form a network between Home appliance objects and the sensors that can save, examine, communicate and barter data together on the internet. This moves to competent industry, fabrication, efficient

<sup>1</sup> IICT Telecommunication, University of Sindh, Jamshoro, Sindh, Pakistan

<sup>2</sup> Shaheed Benazir Bhutto University, Naushahro feroze Campus, Sindh, Pakistan

Corresponding Author: Abubakar2k14@gmail.com

energy management, resource management, health care Management, smarter business take decisions on analyzed data, smart home automation and countless more applications. As this research paper focuses on smart home automation based on IoT, the smart home concept should be understood first. Smart homes combine common devices, found in homes, to be able to control it over the internet. The technology initially was designed and used to control environmental systems, but recently, almost any electrical component can be included within the system of a smart home such as doors, windows, fans, Webcam, etc. [2]. Wide range of articles of The IoT, including items and electric devices that are not generally associated. Cisco predicts that 99% of smart physical appliances will be interconnected. These items contain implanted innovation to collaborate with inward servers and the outside condition. These items are organized competently and can impart over a safe, dependable and accessible system stage. The IoT is based on the associations among the electronic mechanical assembly and things.

### **3. Aim and Objectives**

Using IPv4, OSPF protocols, we aim to remotely control the appliances, which are used in the home, by using IP. We can access it through the internet all over the world. We can implement in the real world because now in the market all Equipment are available which are used for Home Automation. Home appliances are connected through wireless connection and wires. Wireless is best rather than wire because of cost. In this research aims that controlling home appliances via end device using Wi-Fi or cellular network then the end user will directly access through a web-based interface by the web, whereas home appliances like lights, fan and door lock remotely switch [3].

IoT offers a wide scope of new advancements for observing and controlling, of wise structures and keen homes, by upgrading security to lessen vitality and upkeep costs. With the home computerization

control framework, we make our home gadgets shrewd. Savvy as in, the gadgets can be checked or perform the task as indicated by the client's directions. For instance, an entryway lock framework where on the off chance that anybody obscure individual attempts to go into the house without approval, at that point the entryway lock will initiate a caution connected to the entryway and in this we can say our house is keen enough to give us security.

The fundamental target is to interconnect all home appliances with Home gateway via Unguided or guided media to access the internet cloud for controlling and monitoring the home appliances by using API interface.

In this research paper, we focused on home automation and use end devices like cell and computer. The IoT appliances handle and control the electronic electrical and mechanical systems which are used in Homes, institutes, and buildings. The appliances are connected to the cloud server and controlled by a single admin which give the permissions to several users. The admin can approach and control all the nodes connected to each end user but a single end user can control only those appliances to which the user itself is connected [4]. It performs a reality in which we can design this in the real world. We need ISP to connect with the internet and we make a registration server in which every equipment which is using at home registers and we can control remotely.

### **4. Data Storage**

Following are the data storage units:

- 1 KB =  $(10^3)$  bytes
- 1 MB =  $(10^6)$  bytes
- 1 GB =  $(10^9)$  bytes
- 1 TB =  $(10^{12})$  bytes
- 1 PB =  $(10^{15})$  bytes
- 1 EB =  $(10^{18})$  bytes

## 5. Management of Data

### 5.1. Structured Data

Structured data is inserted and sustained in a file. Structured data can easily be listed, categorized, reviewed, and evaluated by a computer. For example, in an office you submit employee name, address, salary, and other information to a website, you are creating structured data. Structured data decrease errors and make simpler for the computer to evaluate.

### 5.2. Unstructured Data

Unstructured data is raw facts and figures. It does not sustain record. So, easily cannot understand unstructured data.

## 6. IP Addressing

An IP address is a logical address which identifies the device over a computer network. The main task of the IP address are to give an identity of computers and routing of the packets on the network.

### 6.1. Public address:

A public IP address is an IP address that can be accessed over the Internet. Like postal address used to deliver a postal mail to your home, a public IP address is the globally unique IP address assign to an end device.

### 6.2. Private Address:

A private IP address is commonly used for local area networks within a building, office, and enterprise environments.

The interconnected network has different sizes. There are many small networks and a few large networks.

In network to provide efficient use of IPv4 32-bit address space, the IPv4 defined several address classes and associated address formats:

Class A: allows 8 bits for the Network portion and 24 bits for the host portion.

Class B: In class, B allows 16 bits for the network portion and 16 bits for the host portion.

Class C: In class, C allows 24 bits for network portion and 8 bits for the host portion.

Class D: Class D is used for multicasting. And

Class E: Class E IP address reserved for research purposes.

## 7. Network Models

Networking models pattern how data flows within a network. Networking models include:

### 7.1. Client Server Model

This is the most common model used in networks. Client computer request for service to the server. Servers are often located maybe locally or remotely and managed by the administrator. For example, Microsoft Outlook is a client-server model where end users connect to the email server using a locally installed email client.

### 7.2. Cloud Computing Model

This is a new model where servers and services are scattered globally in distributed data centers. Synchronized data across multiple servers. Organizations simply subscribe to different services within the Cloud. End users access applications from Cloud servers without requiring an application-specific client. For instance, Gmail email is a cloud service where end-users can access their email from anywhere without requiring a locally installed application. [5]

## 8. Threats To Physical Safety In IoT

Many IoT devices in the home take part in so-called ‘home automation’ activities and interact with physical world components to make life ‘easier’. However, depending on the nature of the physical world interaction there could be the potential for actual physical safety threats.

For example:

IoT smart meters & thermostats – depending on the level of integration of smart meters with the gas/electricity supply in a

household, remote access to these might give a hacker the opportunity to tamper with temperature levels to dangerously low or high values that could, for example, affect the health of elderly or unwell occupants, or in extreme cases start a fire or gas leak.

- IoT lightbulbs – remote access to these devices might allow for on/off switching which could affect the personal safety of occupants suffering from poor eyesight.
- IoT door lock – the ability to tamper with IoT door locks could affect the safety of occupants living in dangerous neighborhoods or might be used to deliberately lock them in their homes/rooms for nefarious purposes. Previous research by others has shown potential issues with such devices.

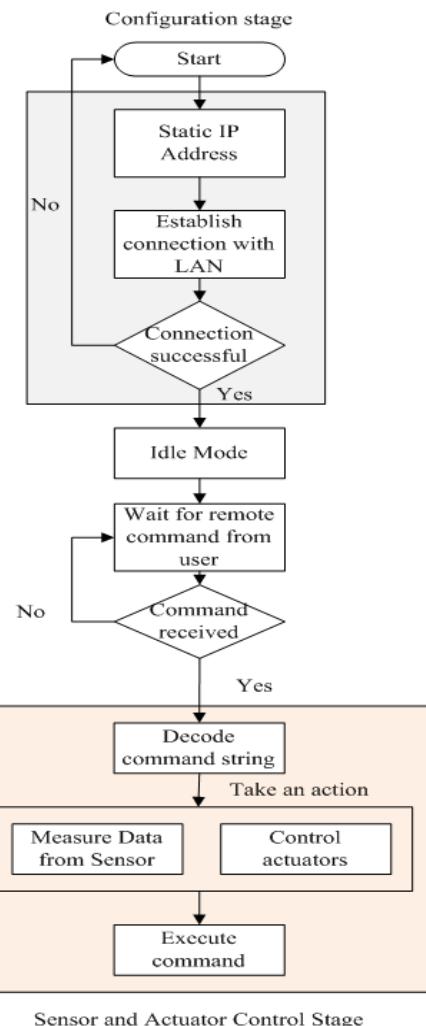
## 9. Wireless Security

The difficulties in keeping a wired network secure are amplified with a wireless network. A wireless network is open to anyone within range of an access point and the appropriate credentials to associate to it. Security and privacy remain a major challenge in IoT [6]. The smart home aim is to enhance the level of intelligence living environment and improves human life [7].

Basic wireless security includes:

- Setting strong authentication protocols with strong passwords
- Configuring administrative security
- Enabling encryption
- Changing all default settings
- Keeping firmware up-to-date

## 10. System Analysis And Tools

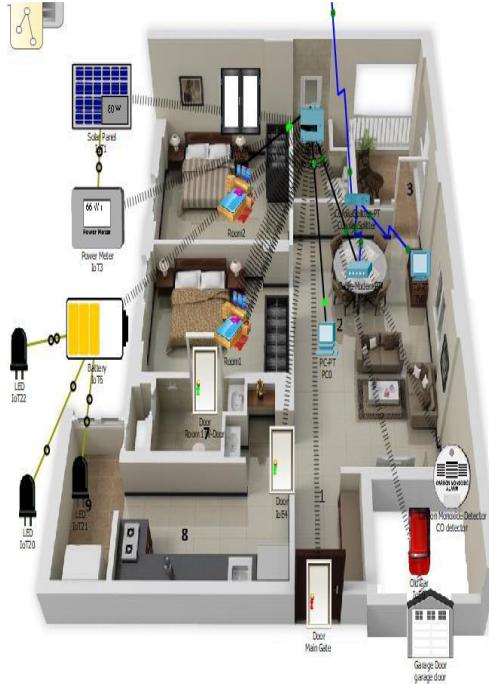


**Fig.1** Flow Chart of IoT Based Home Automation

## 11. Methodology & Implementation

### 11.1. IoT Based for Home Automation:

There are two major components ISP (Internet Service Provider) and Home Appliances which are connected and accessible through ISP internet.



**Fig.2** IoT Based for Home Automation Environment

In the home, all appliances are connected & registered with central the home gateway ([www.register.com](http://www.register.com)) and the home gateway is connected with ISP. We have reported that the very impressive implementation of the Internet of Things used to monitor the interconnected sensors and transmissions of data via the internet [8]. When Home Gateway Switched "ON", Wi-Fi signal spread in the home covered area & all home appliances can connect after the authentication process. The authentication process successfully completes then automatically IP address assigned by DHCP. If not, then try again.

## 12. Protocols

### 12.1. DHCP Protocol:

Dynamic Host Configuration Protocol is used for assigning dynamic IP addresses to the network devices. In DHCP, a device can assign different IP, when the device connects

after switched off. In many systems, the device's IP address can even change while it is still connected. DHCP also provides both static and dynamic IP addresses.

In this research, we prefer to use the OSPF routing protocol for routing of packets in different networks.

### 12.2. OSPF Protocol:

**15.2.1. OSPF Packets:** OSPF protocol exchange the routing information packets with neighbor routers and maintain a complete map of the network.



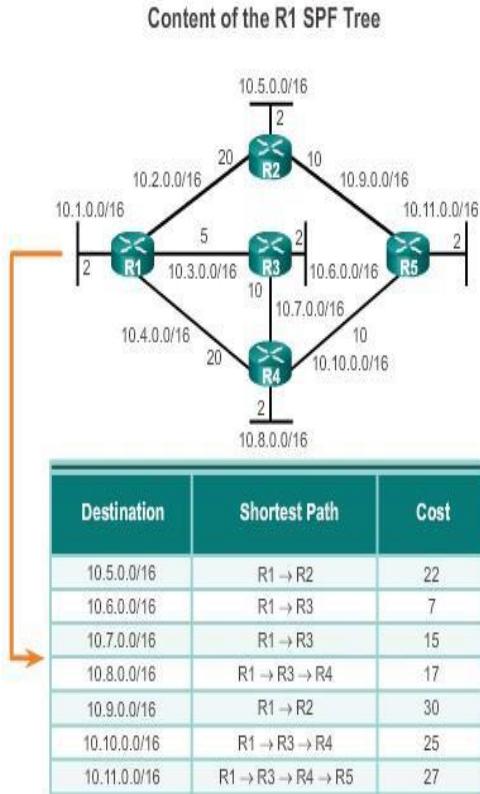
**Fig 3.** OSPF Packets

**15.2.2. If a neighbor is present, the OSPF protocol:** Router establishes the neighbor adjacency and creates a routing table.

**15.2.3. LSAs keep the state and cost of each directly connected link.** Routers flood LSAs to the neighbor. neighbors receiving the LSA immediately flood to other directly connected neighbors to its, until all routers in the area have LSAs.

**15.2.4. Build the topology table based on LSAs that received.** This database keeps all the information about the topology of the network by using Shortest Path First Algorithm

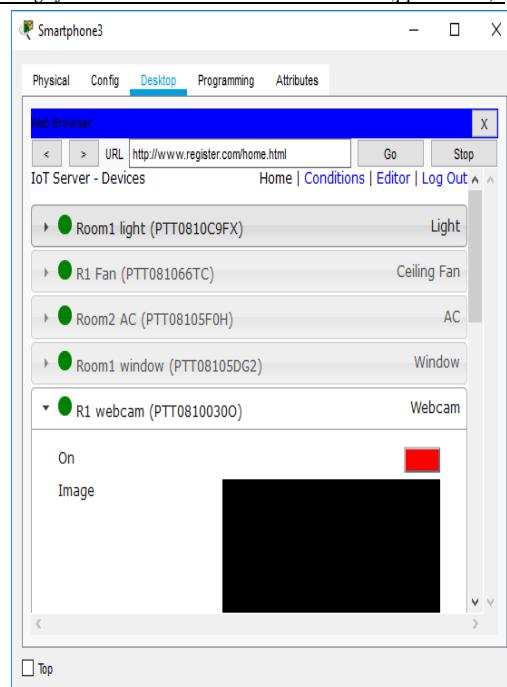
**15.2.5. From the SPF database, the best paths are selected and insert into the routing table.**

**Fig 4.** Routing Table

### 13. Results

The appliances which registered with the Server can control remotely through the internet. Steps are given below:

- Step I. Access to the Register Server through a smartphone/end device.
- Step II. Open the web browser and log in with the website ([www.register.com](http://www.register.com)) Username and password required for access to Home Appliances.
- Step III. Successfully, login into a register web server then the list of the Home appliances will show in the popup menu. (See figure. 5)

**Fig 5.** Registered List of Home Appliances

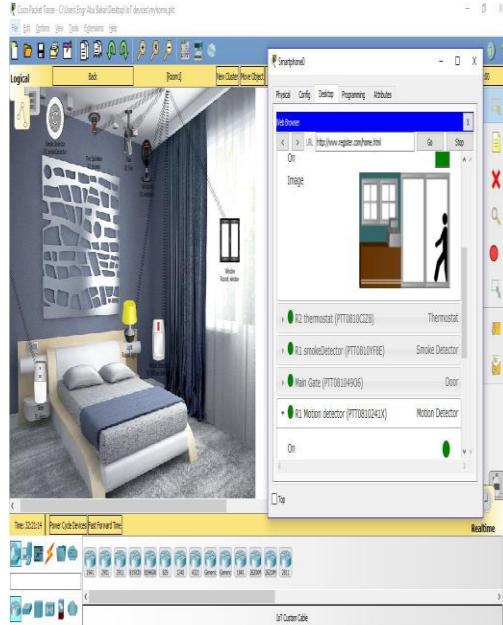
- Step IV. And we can switch ON/Off any electronic appliance by web server interface at any time anywhere.

#### 13.1. Practical: 1 CARBON MONOXIDE DETECTOR & THE GARAGE DOOR AUTOMATION

- In the Garage, When Car switched ON, the car emits the carbon monoxide gas and the sensor detects carbon monoxide when it reaches to set level (2) of carbon monoxide gas then the garage door auto opens and closes.

#### 13.2. Practical 2:

- When the motion detector detects the motion inside the room, the Webcam automatically switched “ON” and start to record video and store it into the registered web server. (see figure. 6)



**Fig 6.** After motion detection

## 14. Conclusion

The Web-based Internet of Things for home automation has been controlled remotely through a web-based interface. The designed network system not just monitors the sensor information, but also senses the temperature, light, movements as well. For example, Light switched ON when the room gets dark.

Additionally, stores the parameters in the cloud server. This will help, the client user to analyze the state of different parameters in the home whenever anywhere.

All over the world paying attention to IoT, which is the third wave of IT after cellular communication and the Internet. In this paper, we proposed the Web-Based Internet of Things for home automation based on Internet and GPRS that presented the data transmission between wireless sensor networks and cellular mobile networks [9].

## ACKNOWLEDGMENT

This research has been conducted at the University of Sindh Jamshoro.

## REFERENCES

- [1] Lee, I. and Lee, K., 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), pp.431-440.
- [2] Ricquebourg, D., Menga, D., Durand, B., Marhic, L., Delahoche, and C. Loge. The smart home concept : our immediate future. In 2006 1ST IEEE International Conference on E-Learning in Industrial Electronics, pages 23–28, Dec 2006.
- [3] Pavithra, D., and Ranjith Balakrishnan. "IoT based monitoring and control system for home automation." 2015 global conference on communication technologies (GCCT). IEEE, 2015.
- [4] Dey, S., Roy, A. and Das, S., 2016, October. Home automation using Internet of Thing. In 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 1-6). IEEE.
- [5] Doukas, C. and Maglogiannis, I., 2012, July. Bringing IoT and cloud computing towards pervasive healthcare. In 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (pp. 922-926). IEEE.
- [6] Dorri, A., Kanhere, S.S., Jurdak, R. and Gauravaram, P., 2017, March. Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 618-623). IEEE.
- [7] Feng, Shuo, Peyman Setoodeh, and Simon Haykin. "Smart home: Cognitive interactive people-centric Internet of Things." *IEEE Communications Magazine* 55.2 (2017): 34-39.
- [8] Kelly, S.D.T., Suryadevara, N.K. and Mukhopadhyay, S.C., 2013. Towards the implementation of IoT for environmental condition monitoring in homes. *IEEE sensors journal*, 13(10), pp.3846-3853.
- [9] Zhu, Q., Wang, R., Chen, Q., Liu, Y. and Qin, W., 2010, December. Iot gateway: Bridgingwireless sensor networks into internet of things. In 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (pp. 347-352). Ieee.