International Journal of Advanced Scientific Technologies ,Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) Volume.3,Special Issue.1,March.2017

Internet of things – A driving force for latest technology

Dr K R Badhiti

Abstract: With the increased use of Automation, life is getting simpler and easier in all aspects. Nowadays, Automatic frameworks are being favored over manual system. With the rapid increase in the number of users of internet over the past decade has made Internet a part of life. The Internet of Things (IoT) is a global industry development that unites individuals, process, information, and things to make networked connections more relevant and valuable than ever before. It is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things in view of existing and developing interoperable data and communication technologies. In this paper, different communication models of IoT and how wireless home automation system works with biometrics are discussed. Home Automation System using IoT is a system that uses computers or mobile devices to control basic home functions automatically through internet from anywhere around the world, an automated home is sometimes called a smart home. We will explain how smart devices and smart apps are connected to the cloud and how data is stored.

Keywords:
Internet of Things, Communication models, Automation, Smart devices, Smart app, Cloud.

I.INTRODUCTION

Authentication is important for any secure system. Together with integrity, confidentiality and authorization it helps in preventing any kind of intrusions into the system. Few years back password based authentication was the most common form of authentication to any secure network[1]. As number of nodes increases from millions to probably billions the threat of malware, spam and viruses has increased. That's why one level of authentication is not enough to secure our applications. Biometrics is identifying a person based on his characteristics which are stable and unique throughout his life. Nowadays, Biometrics along with Internet of things (IoT) is a growing trend. The term "Internet of Things" (IoT) was first used in 1999 by British technology Innovator Kevin Ashton to explain a system in which objects in the physical world could be connected to the Internet by sensors. Internet of things (IoT) is a growing network of everyday object from industrial machine to customer products that can share data and complete tasks while you are busy with other activities. Internet of Things (IoT) denotes a pattern where a large number of embedded devices employ communication utilities offered by the Internet protocols. These devices are often called as smart objects, are not directly operated by individuals, but exist as components in buildings or vehicles, or are spread out in the environment. A thing in the IoT can be an individual with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has integral sensors to alert the driver when pressure is low in tire or any other natural or man-made object that can be provided with an IP address and has the ability to transfer data over a network. In this paper we present a Home Automation system (Smart home)[10] that employs the integration of cloud networking, wireless communication there by providing the user with secured access control.

II.LITERATURE SURVEY

Basil Hamed designed and implemented a control and monitor system for smart house. Smart house system consists of many systems that controlled by LabVIEW software. It is the main controlling system in his paper[8]. Also, the smart house system was assisted by remote control system as a sub controlling system. The system also is connected to the internet to supervise and control the house equipment's from any place in the world using LabVIEW. Denning et al. outlined a set of emergent threats to smart homes due to the steady and swift introduction of smart devices. For example, there are threats of eavesdropping and direct compromise of various smart home devices. Denning et al. also discussed the structure of attacks like data destruction, illegal physical entry, and privacy violations, among others[6]. Their work makes some of these risks concrete and demonstrates how remote attackers can weaken home security in practice. Although they are not the first in recognizing security risks of the modern home, they present the first study of the security properties of evolving smart home applications and their associated programming interfaces.

Zhang et al. used GSM to develop fingerprint based student attendance system. Here a GPRS based system was used to store fingerprint data along with student details. Authenticated authorities could interact with the incoming data from the device through a central server[3]. Maio et al. implementation of a wireless network for class attendance system using facial recognition and GSM. That system consists of a camera that captures the images of the classroom and sends it to the image enhancement module[4]. The attendance is exported to the database server. Here ZigBee network is used for communication between classroom and administrators. According to Mahalinga et al. biometric attendance management system

using wireless connection was developed in which the system scanned the fingerprints placed on the sensor and compared them against those stored in the database successfully[5]. Earlence Fernandes et al. presents the first in-depth empirical security analysis of one such emerging smart home programming platform[7]. They analyzed Samsung-owned Smart things, which has the largest number of apps among currently available smart home platforms, and supports a broad range of devices including motion sensors, fire alarms, and door locks. Smart things hosts the application runtime on a proprietary, closed-source cloud backend, making scrutiny challenging. They overcame the challenge with a static source code analysis of 499 Smart things apps (called Smart Apps) and 132 device handlers, and carefully crafted test cases that revealed many undocumented features of the platform.

Communication Models of IoT:

Device -to-Device Communications:

The device-to-device communication model represents two or more devices that directly connect and communicate between one another, without an intermediary application server. They communicate over many types of networks, including IP networks or the Internet. These devices use protocols like Bluetooth, Z-Wave, or ZigBee to establish direct device-to-device communications, as shown in Figure 1.

These device-to-device networks allow devices that adhere to a particular communication protocol to exchange messages there by achieving their function[2]. This communication model is commonly used in applications like smart homes, which typically use small data packets of information to communicate between devices with low data rate requirements. Residential IoT devices like light bulbs, light switches, thermostats, and door locks normally send small amounts of data to each other (e.g. a door lock status message or turn on light command) in a home automation scenario.

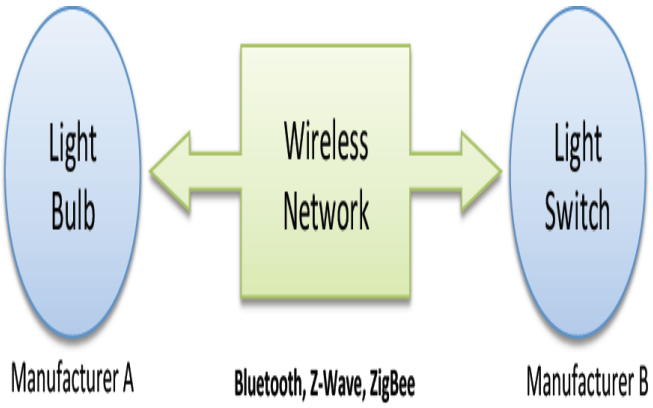

Figure 1. Example of device-to-device communication model.

Device-to-cloud Communications:

In this model, the IoT device connects directly to an Internet cloud service like an application service provider to communicate information and control message traffic. This approach frequently exploits existing communications mechanisms like conventional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service (shown in Figure 2).

This communication model is used by some popular customer IoT devices like the Thermostat and the Samsung Smart TV. In the case of the Thermostat, the device transmits data to a cloud database where the data can be used to analyze energy consumption[2]. Further, the cloud connection enables the user to obtain remote access to their thermostat via a smart phone or Web interface, and it also supports software updates to the thermostat. Similarly with the Samsung Smart TV technology, the television uses an Internet connection to transmit user viewing information to Samsung for analysis.

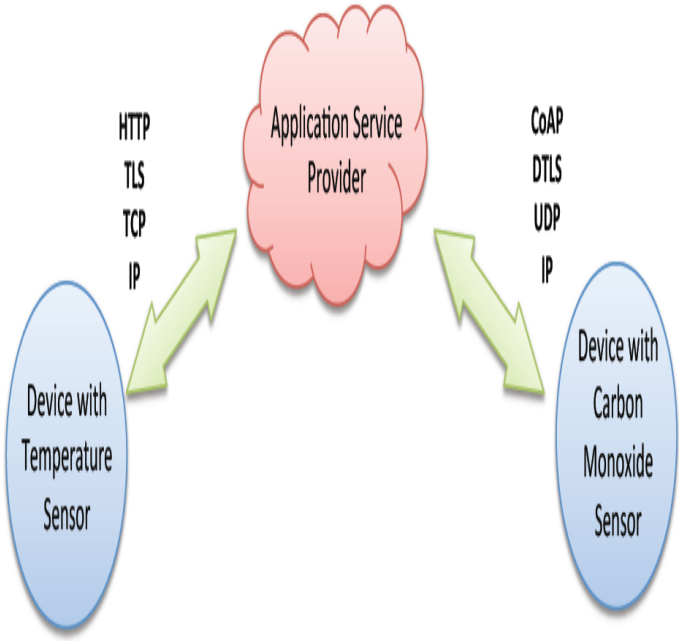

Figure 2. Example of device-to-cloud communication model.

Device to Gateway Model:

In the device-to-gateway model, or more typically, the device-to-application-layer gateway (ALG) model, the IoT device associates through an ALG service as a conduit to reach a cloud service. In simpler terms, there is application software operating on a local gateway device, which acts as an intermediary between the device and cloud service there

by providing security and other functionality such as data or protocol translation(shown in Figure 3).

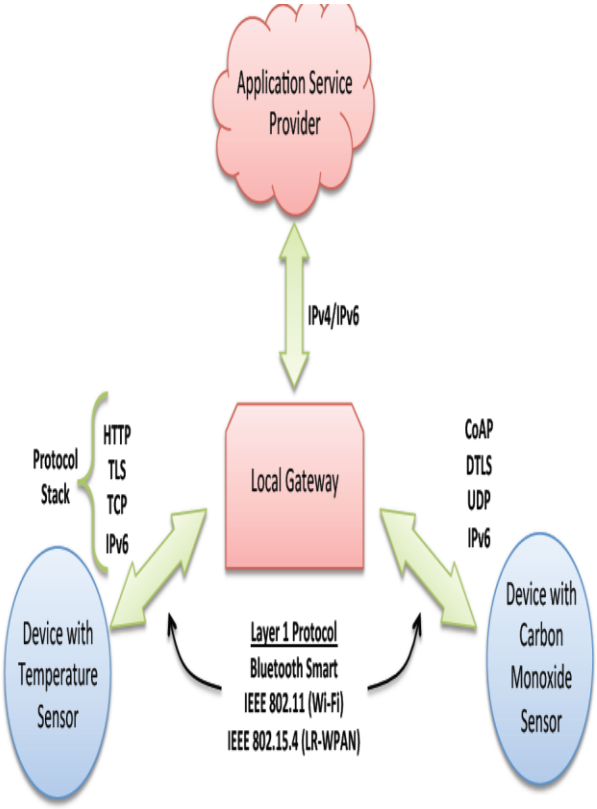

Figure 3. Example of Device-to- Gateway communication model.

Several forms of this model are found in consumer devices. Normally, the local gateway device is a smart phone running an app to communicate with a device and relay information to a cloud service. This is the model associated with popular consumer items like personal fitness trackers. These devices dont have the native capacity to connect directly to a cloud service, so they often depend on smart phone app software to act as an intermediary gateway to connect the fitness device to the cloud.

The other form of this device-to-gateway model is the appearance of "hub" devices in home automation applications. These are devices that acts as a local gateway between individual IoT devices and a cloud service, but they can also bridge the interoperability gap between devices. When we consider the Smart things hub, it is a stand-alone gateway device that has Z-Wave and Zigbee transceivers installed to exchange information with both families of devices[2]. It then connects to the Smart things cloud service, which allows the user to gain access to the devices using a smart phone app and an Internet connection.

Back- End Data-Sharing Model:

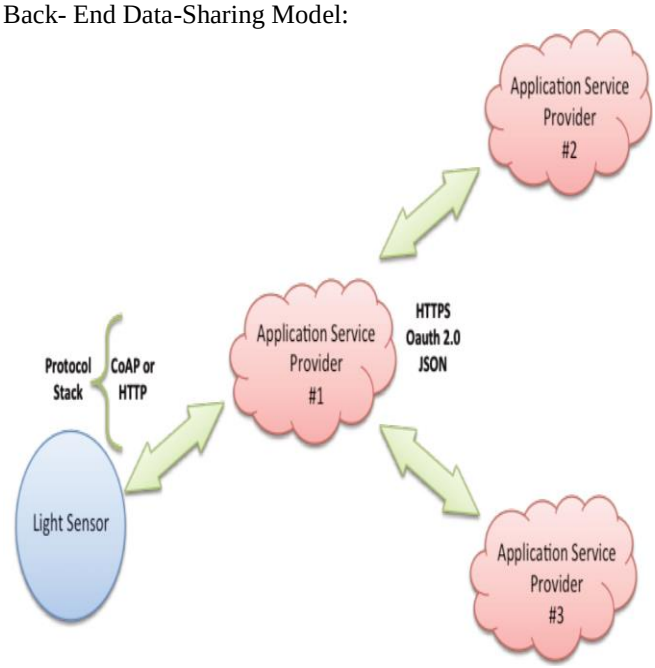

Figure 4. Back- End Data-sharing model Diagram.

The back-end data-sharing model refers to a communication architecture that empowers clients to export and analyze smart object data from a cloud service in combination with data from other sources[2]. This model supports the user's desire for granting access to the uploaded sensor data to third parties. This architecture is an extension of the single device-to-cloud communication model, which can lead to data where "IoT devices upload data only to a single application service provider''. A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed.

Methodology:

In this methodology, we consider device- to-gateway model as we discuss cloud back end and hub. The system consists of four major components: hubs, the Smart things cloud backend, and the smart phone companion app and devices like biometrics sensor or remote devices.(see Figure 5). Each hub, purchased by a user, supports multiple radio protocols including ZWave, ZigBee, and WiFi to interact with physical devices around the client's home. Users(clients) manage their hubs, associate devices with the hubs, and install Smart apps from an app store using the smart phone companion app. The cloud backend runs Smart apps. The cloud backend also runs Smart devices, which are software wrappers for physical devices in a user's home. The companion app, hubs, and the backend communicate over a proprietary SSL-protected protocol.

Smart apps and Smart devices communicate in two ways. First, Smart apps can invoke operations on Smart devices via method calls (e.g., to lock a door lock) by giving their finger print etc. Second, Smart apps can subscribe to events that Smart devices or other Smart apps can generate. A Smart app can send SMSs and make network calls using Smart things APIs. Smart devices communicate with the hub over a proprietary protocol[6].

Smart apps and Smart devices: A programming framework enables creating Smart apps and Smart devices, that are written in a restricted subset of Groovy, a language that compiles to Java Byte code. Since Smart apps and Smart Devices execute on the closed-source cloud backend, Smart things provides a Web-based environment, hosted on the cloud backend, for software development.

Through the biometric sensor, authenticated samples have been stored in Cloud backend by using smart things hub. For example, when the authenticated user wants to open the door, he will use smart app and from it will subscribe events in cloud backend. If the user is authenticated, then the door will be opened. If any relatives are at home, we can open the door from our office as well by invoking events using smart app. We can access other smart devices like air conditioners etc anywhere in the house from smart app when we are busy in other work by communicating with hub.

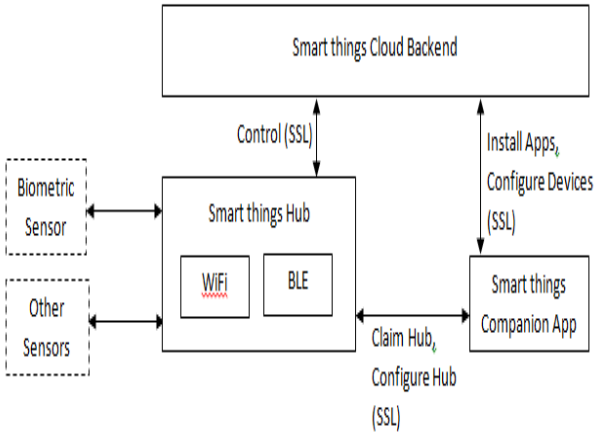

Figure 5: Architecture Overview

CONCLUSION AND FUTURE WORK

The home automation using Internet of Things will work satisfactorily by connecting simple appliances to it and controlled remotely through the internet[14]. We can also use this technique in case of smart cars, smart offices, and smart airports[15]. There are some threats when we consider event spoofing. As the attacker can trigger the same event (i.e. open a door) to gain unauthorized access. So more research work has to be done in this area.

REFERENCES

[1] Udit gupta ,"Application of Multi factor authentication in Internet of Things domain", Information Networking Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA .

[2] "The internet of things: An overview, understanding the challenges and issues of more connected world" by the internet society.

[3] Zhang Yongqiang and Liu Ji., "The design of wireless fingerprint attendance system", Proceedings of International Conference on Communication Technology., Vol.1, pp.1-4, 2006.

[4] D.Maio and D. Maltoni., "Direct gray-scale minutiae detection in fingerprints", IEEE transactions on pattern analysis and machine intelligence,Vol.19, No 1, pp.27-40, 1997.

[5] Mahalinga V.Mandi, Ashwini K.S, Chaitra H.S, Kavitha R and Kavitha U., "Biometric Based Attendance Management System Using Wi-Fi", International Journal of Emerging Technology and Research., Vol.1, No 5, pp.32-36, 2014.

[6] T. Denning, T. Kohno, and H. M. Levy, "Computer security and the modern home," Commun. ACM, vol. 56, no. 1, pp. 94–103, Jan. 2013.

[7] Earlence Fernandes, Jaeyeon Jung, Atul Prakash, "Security Analysis of Emerging Smart Home Applications", 2016 IEEE Symposium on Security and Privacy.

[8] Basil Hamed, "Design & Implementation of Smart House Control Using LabVIEW" at International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6, January 2012

[9] Divil Jain , Dr. P.S. Ramkumar, Dr. K.V.S. Sairam, "IoT based Biometric access control system", International journal of innovative Research, Engineering and Technology, volume 5,special issue 9,May 2016.

[10] Vinay Sagar, Kusuma, "Home Automation using Internet of Things", International Journal of Engineering and Technology, volume 2,issue 3, June 2015.

[11] Stalin Marcelo Arciniegas-Aguirre "Biometric access control system based on Internet of Things and using Free Hardware", International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 10, October 2015.

[12] S.D.T. Kelly, N.K. Suryadevara, S.C. Mukhopadhyay, "Towards the Implementation of IoT for Environmental Condition Monitoring in Homes", IEEE, Vol. 13, pp. 3846-3853, 2013.

[13] Nicholas D., Darrell B., Somsak S., "Home Automation using Cloud Network and Mobile Devices", IEEE Southeastcon 2012, Proceedings of IEEE.

[14] "Vera Smart Home Controller," http://getvera.com/controllers/vera3/,Accessed: Oct 2015.

[15] Samsung, "SmartApp Location object," http://docs.smartthings.com/en/latest/ref-docs/location-ref.html#location-ref, Accessed: Oct 2015.