Journal of Engineering and Applied Sciences 14 (Supplimentary 01): 8496-8502, 2019
ISSN: 1816-949X
© Medwell Journals, 2019

An IoT Enabled Home Automation System

C.R. Srinivasan, Guru Charan and P. Chenchu Saibabu
Department of Instrumentation and Control Engineering, Manipal Institute of Technology,
Manipal Academy of Higher Eductation (MAHE), 576104 Manipa, India
chenchu.saibabu@manipal.edu

Abstract: Internet of things in the current trend of engineering is one of the most widely researched field of technology. IoT has become a technological revolution that helps in making our lives better. The development of IoT triggered a huge demand for "Smart devices". A "Smart device" is laden with sensors that collects data of their surroundings, processes it and relays it for further analysis. For an IoT device, the data is sent to the internet using various means. This feature makes IoT special from other systems but also more prone to cyber-attacks. Proper means of security can minimize such risks. This study emphasizes on the need of smart homes, the risks and security concerns and ways to overcome them, list of various methods of home automation and discussion of smart homes using IoT. The main objective is to control the home appliances using a remote device utilizing the home WiFi-network.

Key words: Internet of things, IoT, smart homes, home automation, security, privacy

INTRODUCTION

There exists no universally accepted definition of IoT. The basic idea of an IoT is that every physical device that exists currently can become a computer and can be controlled when connected to the internet. An IoT device is tagged a smart device as they perform smarter things than they were initially designed to do (Pego and Nunes, 2017).

The number of Internet of Things (IoT) devices developed has increased dramatically over the past decade with the number reaching 15 billion, at approximately two devices per user, this implies a surprising conclusion that there exists more connected systems than living people. It is anticipated that this trend will continue with an estimated 26 billion connected devices as of 2020, several of which are IoT and wearable devices. IoT devices are equipped with sensors but also offer some kind of connectivity features and functionality, very much like the embedded systems they derive from. These devices, therefore, transmit the data that is collected to a remote collection point (Wurm *et al*., 2016).

Internet of things is a network of objects equipped with the capabilities of electronics, sensors, software and connectivity to enable communication and information exchange between these devices. We can design complex systems which can improve our standard of living by transmutation of the information obtained from each device and by interacting each device with the environment (Madeira and Nunes, 2016).

A smart networked home is a place that uses IoT technology to create an effective lifestyle and a comfortable environment. Compared to a typical home which primarily has local control, usually a combination of buttons and switches, devices that are not connected to the Wi-Fi or cellular network and access restricted to a limited number of people, essentially, a form of direct access and at certain times, this isn't the case for a smart home today. This research has been driven by the growing number of individuals interested in smart homes, widespread availability as well as emergence of IoT based devices in this society and rapidly increasing reports of privacy and security violations (Bugeja *et al*., 2017).

The two aspects of this project are home automation and wireless security. The system's currently constructed prototype sends notifications to owner about using the internet if any kind of physical movement is sensed nearby the house and if need be raise an alarm at the discretion of the user. The provision for the sending of alert notifications to the security personnel concerned is also incorporated into the system in the event of a critical situation.

The user can access the notifications and status of the IoT device from anywhere in the world, even if internet access is not readily accessible (because it's not

Corresponding Author: P. Chenchu Saibabu, Department of Instruemntation and Control Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, 576104 Manipal, Kanataka, India, chenchu.saibabu@manipal.edu

necessary to connect the smart phone to the internet, only the board must have Wi-Fi access) (Kodali *et al*., 2016).

Due to the dominance in the use of internet, the advancement of smartphone technology and significantly increased mobile communication standards, the IoT application is just this popular in this 21st century. There exist many sensors in this evolutionary area of IoT that the user needs to control. Now a virtual device must be developed to control these sensors which successively provides mobility by compartmentalizing each device and operating system. Due to the increasing demand for connectivity between the house and outside world, the need for IoT technologies for the home automation has increased (Dey *et al*., 2016).

In this study, we will be discussing the basics about the different types of techniques used for smart homes and elaborate illustration on smart homes using IoT. The theory behind the techniques, components used, the working and the result of this project will be discussed in the subsequent chapters.

A IoT of research has been done on IoT for almost two decades before our research. The basic idea stems from the late 1980s as omnipresent computing and omnipresent computing (Weiser, 1991) and pervasive computing. The epithet Internet of Things (IoT) emerged in the late 1990s and as discussed by Atzori *et al*. (2010) has been researched thoroughly from several aspects. Their survey categorizes IoT paradigms into three paradigms: object-oriented, semantic-oriented and visions of the internet.

In IoT-based smart homes, Denning *et al*. (2013) surveyed the privacy and security landscape and provided a technique for logical reasoning on need for security. They have used scenario-based approach comprised of three components, namely the feasibility of carrying out an attack, the attractiveness of the system as a compromised platform and the damage caused by an attack.

In addition to existing ones, the notion that smart homes create cyber risks is explored by Roman *et al*., (2011) research in which an account is provided for security and privacy threats. They don't provide information about how to identify the risk and how to deal with it, though their reflection on this is interesting.

Kozlov *et al*. (2012) discuss privacy and security threats at the smart home's various architectural levels. In particular, they advertise mechanisms for privacy control, methods for analyzing the level of privacy risk and its energy aspects, trust and security.

Anonymous (2013) developed a room level presence detection system for a house. This uses a large amount of data collected from multiple sources to infer about presence. The sort of data in use and its primary source may clearly indicate explicit presence, for example, in the case of pressure sensors in chairs and beds or tacitly in the case of network traffic detection from a PlayStation system.

Through, a comprehensive study of "home automation using the internet of things" proposed by Shopan Dey, Sandip Das and Ayon Roy, it is seen that they had used the Raspberry Pi to connect the ESP8266-01 Wi-Fi module to the net. Using this, they control different devices via. the web page as well as via. Android application (Dey *et al*., 2016). In their study, K. Venkatesan and Dr. U. Ramachandraiah implemented Zigbee module in Arduino mega by controlling devices. They used different sensors for different purposes. They also provided with real-time notification and feedback on the web server that allows customers to see what's happening at home (Venkatesan and Ramachandraiah, 2015). The devices are also controlled from the web app using a Raspberry Pi, logic gates, flip-flop and 555 timer. The study by Shashank Shiva Kumar Jha, Tapan Pokharna, Vishwateja Mudiam Reddy, Naresh Vinay demonstrates how it's is done and controlled (Reddy *et al*., 2016).

Although, the concept of smart homes in India is new, considerable work has been done in other countries where there are already smart homes in place. Kang *et al*. (2015) discusses the acquiring and analyzing the sensor data used in smart homes. He proposed a contextual information architecture by analysis of the acquired data from different sensors and providing context-sensitive services. JeyaPadmini and Kashwan (2015) discusses efficient use and conservation of power in smart homes using IoT. Using image processing techniques it uses cameras to recognize human activities. Kamilaris and Pitsillides (2013) and Kang *et al*. (2015) traces the requirement of protocols and standards from Colmnon to develop sustainable IoT-based smart home applications. Gaikwad *et al*. (2015) uses loT to discuss challenges and issues that arise in smart home systems and suggest possible solutions.

MATERIALS AND METHODS

There are four functional layers that outline the Internet of Things (IoT) architecture: the interaction layer, the representation layer, the service layer and the application layer.

This layer includes all the physically attached pieces of hardware to an object that allows communication with other devices and the internet. This layer comprises all the

physically linked pieces of hardware to an object that allows communication with the internet other devices. This layer enables objects to communicate with the real world and the generated information is transferred to the upper layer.

The representation layer is mainly responsible for maintaining each object, creating a method of identification (e.g., Uniform Resource Identifier (URI)/Uniform Resource Locator (URL)) and a way for establishing proper communication with each and every object using their own methods. This layer allows the objects to share information with one another and the external world (internet), allowing the top layer to use it.

The service layer works across the representation layer to provide all connected objects with functionality and information. This layer will enable users or designers to standardize the use of this information. Lastly, many types of applications form the application layer where the characteristics and data collected by the service layer are used (Pego and Nunes, 2017).

Connection modes: There are many communication modes for receiving and sending information to or from objects. Every other type of communication has its own pros and cons and depending on its functionalities and objectives, objects can get to choose one or maybe more communication types. Connection modes are of four types: connection on demand, connection within range, permanent wireless connection and permanent wired connection.

Connection on demand type entails human interaction and it is predominantly used in the constant presence of the user in situations where exchange of information is required. The Quick Response Code (QRCODE), smart card or RFID are few examples.

The type "In-range connection" necessitates proximity between the two devices. This is only feasible when the two devices are sufficiently close and used on objects that do not necessitate a constant faultless communication. Examples of this type of communication are the Bluetooth and Near Field Communication (NFC).

Finally, we have the types of wireless and wired connections in the permanent connection mode. The need for physical connection (via. cable) distinguishes these two types. The 4G network, Wireless Fidelity (WiFi), Z-Wave and Zigbee are examples of wireless connections. We have the Digital Subscriber Line (DSL) or optical fiber (Ethernet) as examples for cable connection.

Communication protocols: We will outline the most widely used communication protocols within the IoT world in this study. In addition to the various connection modes defined in subsection II-A, other necessities such as required bandwidth or limitation of energy consumption open up space for these distinct methods of data transmission. In addition to the numerous connection modes defined, other essentials such as bandwidth required or limitation of energy consumption open up space for these distinct methods of data transmission. Some of the most widely used communication protocols on IoT today are the following:

- Bluetooth
- Zigbee
- Ethernet
- Z-Wave
- WiFi
- Cellular

The purpose of making a product easy for people to use that integrates more sorts of tasks within a house stands at the design basis for this kind of smart home. With a few configuration steps, it has a simple interface. The user connects his device to the web, sends the required commands from the house to the smart home portal and the physical component activates (Patru *et al*., 2016).

The architecture utilizes sensors and actuators which are installed in the place of residence just, so, they can interact with one another and can be accessed via. a web application and by a smartphone or computer connected to the same network. Any smart device registered can be managed and the access permission can be customized in a simplified manner such as customizing the existence of different levels which can represent, for example, a residence's rooms as in the tree hierarchy. Furthermore, a user could automatically or manually activate or deactivate devices by optimizing a set of guidelines or rules from sensor data, viewing sensor data and creating device groups that can be triggered together.

Because of chip-supported Wi-Fi connectivity and security protocols such as WPS, WEP, WPA2-PSK and WPA-PSK, the devices are all mainly based on the ESP8266 (Wi-Fi module) microcontroller which allow direct integration with a local server between the sensors and actuators. Because of the local environment where this is placed to be based solely on web communication protocols, these properties of this device fulfil the need of this type of architecture.

A typical smart home automation system comprises of a vast number of internet-smart devices that are heterogeneous storage), audio and video interfaces (e.g., HDMI) and network protocols (e.g., Ethernet) that enable connectivity between the home network and the internet

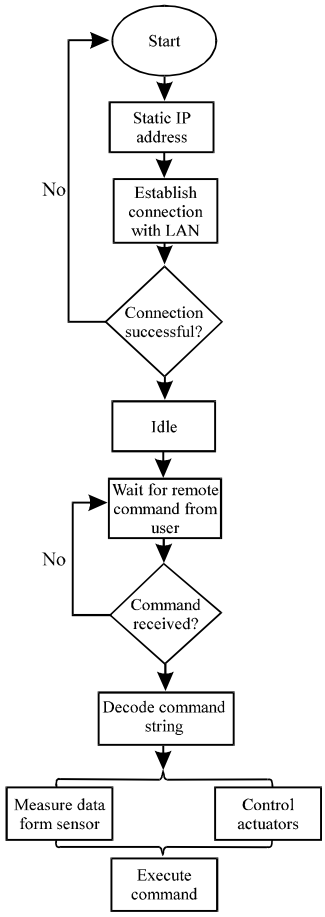

Fig. 1: Flowchart of execution of code with internet

(Ray, 2016). The device is made of integrated sensors or actuators which send or receive information which in turn is used to control the device. The device can be powered by variety of battery packs depending on its nature varying from 4×AA batteries to high voltage batteries (Bugeja *et al*., 2018). Home devices typically tend to be immobile (e.g., heater) but they may also include other mobile devices (e.g., vacuum cleaners).

A number of software user interfaces are also supported by the device. Specifically, those with high hardware specs such as home automation gateways or portals, may offer: Application Program Interfaces (APIs) enabling the functionality of the device to be integrated, IFTTT (If this Then That) enabling users to create automated command generation in response to changes in the environment and services typically accessible via. a smartphone app or web browser. In addition, devices can offer cloud based/server support that enables data storage and communication with third party service providers as well as protocols that enable remote operation as well as control (Fig. 1).

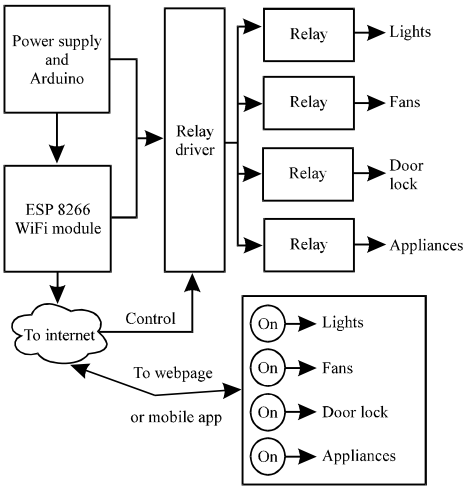

Fig. 2: General block diagram of home automation circuit

The system connects via. the home Wi-Fi network to the mainframe unit and use protocols such as MQTT, HTTP(S) and WebSocket. Choosing which protocol is to be used depends primarily on response time required to transfer data, e.g., switching on a lamp and sending the measure of a water tank have different priorities. The lamp requires instant action while the water tank does not need an instant response. In addition to displaying the data compiled in the monitor, all systems also report to the mainframe unit when they identify any deformities in their own operations such as problems with sending data or when they cannot connect to the internet (Fig. 2).

The system includes a mobile app developed using the Android platform and using a micro web server based on Arduino Ethernet. The Arduino is the main controller hosting and performing the necessary actions to be performed. The main controller which is the Arduino is connected directly to all actuators/relays and sensors. With the smart home mobile app, the smart home environment can be controlled and monitored from a remote location. The user device can use any internet connection via. Wi-Fi or 3G/4G network to communicate with the device (Alkar and Buhur, 2005).

Circuit is set up such that the Arduino is the main microcontroller connected to a set of relays that controls the switching of the smart home appliances. The mode of switching used is through WiFi module ESP8266 connected to the Arduino which is connected to the smart phone or a PC. It is necessary that only the WiFi module should be connected to the home network while the mobile phone or PC used to control the smart home can be connected to any network. Once the WiFi module is connected to the internet, the IP address and the port number is displayed which is used as a medium to connect the device to the internet.

The mobile app will include options for giving the appliances different commands and controlling them. The application's main page will have a login page to authenticate the user using the IP address and password. After the successful login, the user can use the mobile app to control all appliances. The app will provide switches to control the home's devices and appliances and these switches can be manually customized.

Security concerns are taken care such that only the person with the IP address can be able to access the login page. And even, if someone reaches the login page, one requires the login credentials to control the smart home.

RESULTS AND DISCUSSION

In this study, we have discussed about the implementation of a smart home system using ESP8266 WiFi module and set of relays with Arduino as the primary microcontroller. The IoT system designed was tested in various load conditions. The user must have the software installed on their computer or smart phone after installing the experimental setup. User can login from the Android application after obtaining the IP address and port address. Upon completion of the setup, a home page that allows the user to keep track of all devices connected to the server will appear.

This study mainly demonstrates a smart home automation system with the help of low cost Arduino board and set of relays. Since, IoT is a vastly growing technology in the recent years which can change the context of smart homes, it can be associated with various challenges. Perhaps one of the biggest challenges in the absence of standards to integrate different sensors and other already existing smart embedded devices. Another major challenge is to provide unique IP address for networked devices as well as privacy and security in the smart home. As IoT handles massive amounts of data collected from different sensors used in a smart environment, suitable measures need to be taken to handle, store and secure the data stored. Data analysis and visualisation can also be used in future to monitor and manage IoT devices effectively (Fig. 3).

The common IoT Android application as above is used in this study where we can control the devise by using the smart phone by just tapping the button using the means of IoT. The application is connected to the device using the WiFi module. The features of the type of appliances to be controlled can be easily created and modified in the application (Fig. 4).

Fig. 3: App controls

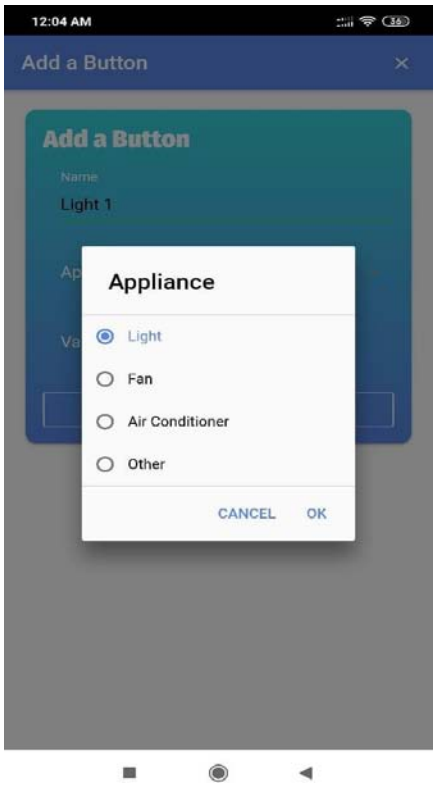

Fig. 4: App interface

CONCLUSION

In this study, we have presented a prototype of a smart home system using IoT. The system is operational without any defects but there is always scope of improvements. One basic idea is to reduce the time delay to turn off and on an appliance from 3 sec currently to <1 sec for a device with good accuracy. Instead of the old-fashioned yet highly used and recommended way of buttons or touch screen or clicking from the mobile app, we can try to develop a way where we can control the devices by speech recognition, making a an even smarter and effective system.

A possibility where an intruder is detected and the smart home can identify a non-home member's arrival and can alert the user of the presence of the said intruder can be developed. Also, in cases where the unknown person has to be let in by the user, the user can grant access from anywhere such that the smart home system can unlock the door for the guest to enter in the absence of the user. If anything is connected to the internet, it possesses a high privacy and security risk. Aspects related to the security and privacy of user and the layout of the smart home devices also require further attention. One key remaining challenge to secure the smart homes is analysis and risk assessment of flux information. With such understanding in place, privacy and security support systems can be designed efficiently and it is possible to overcome the growth barrier for energy-efficient and secure IoT-based smart homes.

REFERENCES

Alkar, A.Z. and U. Buhur, 2005. An internet based wireless home automation system for multifunctional devices. IEEE. Trans. Consum. Electron., 51: 1169-1174.

Anonymous, 2013. Smart home occupancy & presence. Smartisan Technology Co., Ltd,ý Beijing, China. https://smartisant.com/research/presence/index.php

Atzori, L., A. Iera and G. Morabito, 2010. The internet of things: A survey. Comput. Netw., 54: 2787-2805.

Bugeja, J., A. Jacobsson and P. Davidsson, 2017. An analysis of malicious threat agents for the smart connected home. Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), March 13-17, 2017, IEEE, Kona, Hawaii, USA., pp: 557-562.

Bugeja, J., P. Davidsson and A. Jacobsson, 2018. Functional classification and quantitative analysis of smart connected home devices. Proceedings of the 2018 International Conference on Global Internet of Things Summit (GIoTS), June 4-7, 2018, IEEE, Bilbao, Spain, pp: 1-6.

Denning, T., T. Kohno and H.M. Levy, 2013. Computer security and the modern home. Commun. ACM., 56: 94-103.

Dey, S., A. Roy and S. Das, 2016. Home automation using internet of thing. Proceedings of the 2016 IEEE 7th Annual Conference on Ubiquitous Computing, Electronics & Mobile Communication (UEMCON), October 20-22, 2016, IEEE, New York, USA., ISBN:978-1-5090-1497-2, pp: 1-6.

Gaikwad, P.P., J.P. Gabhane and S.S. Golait, 2015. A survey based on smart homes system using internet-of-things. Proceedings of the 2015 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), April 22-23, 2015, IEEE, Chennai, India, ISBN:978-1-4673-6525-3, pp: 0330-0335.

JeyaPadmini, J. and K.R. Kashwan, 2015. Effective power utilization and conservation in smart homes using IoT. Proceedings of the 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), April 22-23, 2015, IEEE, Chennai, India, pp: 0195-0199.

Kamilaris, A. and A. Pitsillides, 2013. Towards interoperable and sustainable smart homes. Proceedings of the 2013 IST-Africa Conference & Exhibition, May 29-31, 2013, IEEE, Nairobi, Kenya, ISBN:978-1-905824-38-0, pp: 1-11.

Kang, B., S. Park, T. Lee and S. Park, 2015. IoT-based monitoring system using tri-level context making model for smart home services. Proceedings of the 2015 IEEE International Conference on Consumer Electronics (ICCE), January 9-12, 2015, IEEE, Las Vegas, Nevada, USA., pp: 198-199.

Kodali, R.K., V. Jain, S. Bose and L. Boppana, 2016. IoT based smart security and home automation system. Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), April 29-30, 2016, IEEE, Noida, India, ISBN:978-1-5090-1667-9, pp: 1286-1289.

Kozlov, D., J. Veijalainen and Y. Ali, 2012. Security and privacy threats in IoT architectures. Proceedings of the 7th International Conference on Body Area Networks (BodyNets'12), February 24-26, 2012, ICST, Oslo, Norway, pp: 256-262.

Madeira, R. and L. Nunes, 2016. A machine learning approach for indirect human presence detection using IoT devices. Proceedings of the 2016 11th International Conference on Digital Information Management (ICDIM), September 19-21, 2016, IEEE, Porto, Portugal, pp: 145-150.

Patru, I.I., M. Carabas, M. Barbulescu and L. Gheorghe, 2016. Smart home IoT system. Proceedings of the 2016 15th RoEduNet Conference on Networking in Education and Research, September 7-9, 2016, IEEE, Bucharest, Romania, ISBN:978-1-5090-5399-5, pp: 1-6.

Pego, P.R.J. and L. Nunes, 2017. Automatic discovery and classifications of IoT devices. Proceedings of the 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), June 21-24, 2017, IEEE, Lisbon, Portugal, pp: 1-10.

Ray, P.P., 2016. A survey on internet of things architectures. J. King Saud Univ. Comput. Inf. Sci., 30: 219-319.

Reddy, V.M., N. Vinay, T. Pokharna and S.S.K. Jha, 2016. Internet of things enabled smart switch. Proceedings of the 2016 13th International Conference on Wireless and Optical Communications Networks (WOCN), July 21-23, 2016, IEEE, Hyderabad, India, ISBN:978-1-4673-8976-1, pp: 1-4.

Roman, R., P. Najera and J. Lopez, 2011. Securing the internet of things. Comput., 44: 51-58.

Venkatesan, K. and U. Ramachandraiah, 2015. Networked switching and polymorphing control of electrical loads with web and wireless sensor network. Proceedings of the 2015 International Conference on Robotics, Automation, Control and Embedded Systems (RACE), February 18-20, 2015, IEEE, Chennai, India, pp: 1-9.

Weiser, M., 1991. The computer for the 21st century. Scient. Am., 265: 94-104.

Wurm, J., K. Hoang, O. Arias, A.R. Sadeghi and Y. Jin, 2016. Security analysis on consumer and industrial IoT devices. Proceedings of the 2016 21st Asia and South Conference on Pacific Design Automation (ASP-DAC), January 25-28, 2016, IEEE, Macau, China, pp: 519-524