SMART HOME AUTOMATION USING IOT

Ms.S.Sivasankari,M.Sc.,M.Phil.,
Assistant Professor,

Mr.P.Karthick,M.C.A.,
M.Phil Research Scholar,

Dept of Computer Science & Computer Application,
Prist University , Madurai Campus.

ABSTRACT: Internet, a revolutionary invention, is always transforming into some new kind of hardware and software making it unavoidable for anyone. The form of communication that we see now is either human-human or human-device, but the Internet of Things (IoT) promises a great future for the internet where the type of commu- nication is machine-machine (M2M). This paper aims to provide a comprehensive overview of the IoT scenario and reviews its en- abling technologies and the sensor networks. Also, it describes a six-layered architecture of IoT and points out the related key chal- lenges.

Keywords: Internet of Things, RFID, WSN, IOT architecture, IoT Vision, IoT applications, IoT security.

1. Introduction

The internet of things can be described as the technology in which the actual physical entities (electronic devices) with data sensing, processing & self adoption capacity can be used to interact with other such device and process that data to take an intelligent decision which will prove useful for our daily day to day life. IoT is defined as an environment in which objects (devices) are given unique identifiers and the ability to transfer data over a network without having human-to-human or human-to-computer interaction.

IoT mainly has the following three characteristics: comprehensive perception, which means that entity's information can be obtained at anytime and anywhere; reliable transmission, which means that entity's sensory information is required to pass out accurately in real-time; intelligent processing, which means that the mass of information can be analyzed and processed efficiently, then the entity's intelligent control is realized.

Internet of Things is refer to the general idea of things, especially everyday objects, that are readable, recognizable, locatable, addressable through information sensing device and/or controllable via the Internet, irrespective of the communication means (whether via RFID, wireless LAN, wide area networks, or other means). Everyday objects include not only the electronic devices we encounter or the products of higher technological development such as vehicles and equipment but things that we do not ordinarily think of as electronic at all - such as food , clothing ,chair, animal, tree, water etc.

Objects make themselves recognizable and they obtain intelligence by making or enabling context related decisions thanks to the fact that they can communicate information about themselves. They can access information that has been aggregated by other things, or they can be components of complex services.

IoT is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

With the IoT the communication is extended via Internet to all the things that surround us. The Internet of Things is much more than machine to machine communication, wireless sensor networks, sensor networks, 2G/3G/4G,GSM,GPRS,RFID, WI-FI, GPS, microcontroller, microprocessor etc. These are considered as being the enabling technologies that make “Internet of Things” applications possible.

2. VISION

In 2005, ITU reported about a ubiquitous networking era in which all the networks are interconnected and everything from tires to attires will be a part of this huge network . Imagine yourself do- ing an internet search for your watch you lost somewhere in your house. So this is the main vision of IoT, an environment where things are able to talk and their data can be processed to perform desired tasks through machine learning . A practical implemen- tation of IoT is demonstrated by a soon-to-be released Twine, a compact

and low-power hardware working together with real-time web software to make this vision a reality . However different people and organizations have their own different visions for the IoT .

An article published in Network World revealed IoT strategies of top IT vendors, they carried out some interviews from the key IT vendors. As of HP's vision, they see a world where people are al- ways connected to their content. Cisco believes in the industrial automation and convergence of operational technology. Intel is fo- cused on empowering billions of existing devices with intelligence. Microsoft does not consider IoT as any futuristic technology; they believe that it already exists in today's powerful devices and that the devices just need to be connected for a large amount of informa- tion which could be helpful. While, IBM has a vision of a Smarter Planet by remotely controlling the devices via secured servers.

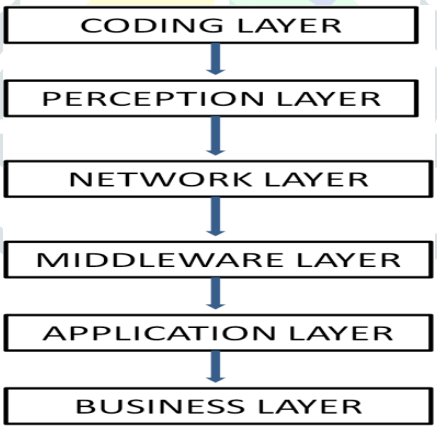
Despite of having different visions, they all agree about a network of interconnected devices therefore more developments within the coming decades are expected to be seen including that of a new converged information society.

3. ARCHITECTURE

More than 25 Billion things are expected to be connected by 2020 which is a huge number so the existing architecture of Internet with TCP/IP protocols, adopted in 1980, cannot handle a net- work as big as IoT which caused a need for a new open architecture that could address various security and Quality of Service (QoS) issues as well as it could support the existing network applications using open protocols. Without a proper privacy assurance, IoT is not likely to be adopted by many. Therefore protection of data and privacy of users are key challenges for IoT.

For further development of IoT, a number of multi-layered security architectures are proposed. described a three key level archi- tecture of IoT while described a four key level architecture. proposed a five layered architecture using the best features of the architectures of Internet and Telecommunication management networks based on TCP/IP and TMN models respectively. Simi- larly a six-layered architecture was also proposed based on the net- work hierarchical structure.

The six layers of IoT are described below:



3.1 Coding Layer

Coding layer is the foundation of IoT which provides identification to the objects of interest. In this layer, each object is assigned a unique ID which makes it easy to discern the objects .

3.2 Perception Layer

This is the device layer of IoT which gives a physical meaning to each object. It consists of data sensors in different forms like RFID tags, IR sensors or other sensor networks which could sense the temperature, humidity, speed and location etc of the objects. This layer gathers the useful information of the objects from the sensor devices linked with them and converts the information into digital signals which is then passed onto the Network Layer for further action.

3.3 Network Layer

The purpose of this layer is receive the useful information in the form of digital signals from the Perception Layer and transmit it to the processing systems in the Middleware Layer through the trans- mission mediums like WiFi, Bluetooth, WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc.

3.4 Middlware Layer

This layer processes the information received from the sensor de- vices . It includes the technologies like Cloud computing, Ubiq- uitous computing which ensures a direct access to the database to store all the necessary information in it. Using some Intelligent Pro- cessing Equipment, the information is processed and a fully auto- mated action is taken based on the processed results of the infor- mation.

3.5 Application Layer

This layer realizes the applications of IoT for all kinds of industry, based on the processed data. Because applications promote the de- velopment of IoT so this layer is very helpful in the large scale de- velopment of IoT network . The IoT related applications could be smart homes, smart transportation, smart planet etc.

3.6 Business Layer

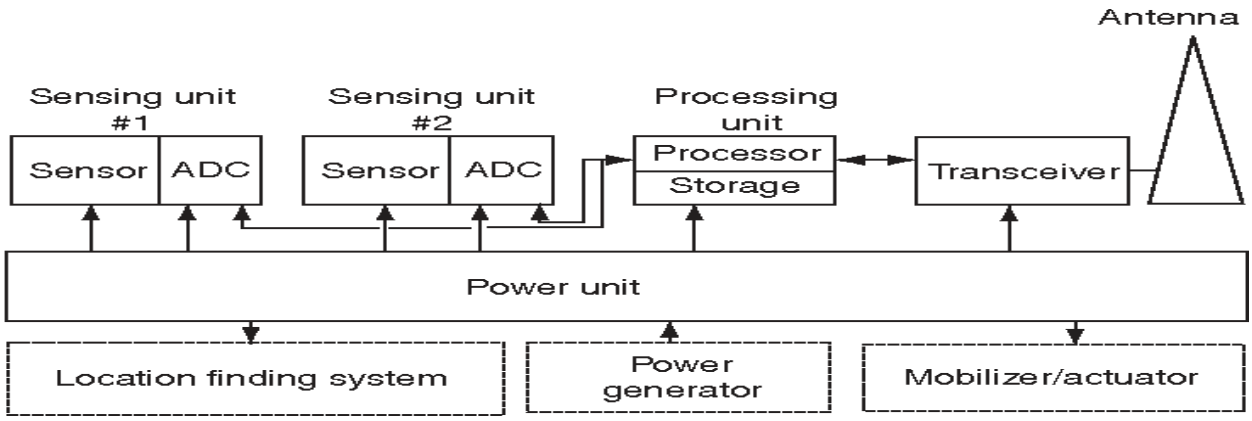
This layer manages the applications and services of IoT and is re- sponsible for all the research related to IoT. It generates different business models for effective business strategies.

4. TECHNOLOGIES

The development of a ubiquitous computing system where digi- tal objects can be uniquely identified and can be able to think and interact with other objects to collect data on the basis of which au- tomated actions are taken, requires the need for a combination of new and effective technologies which is only possible through an integration of different technologies which can make the objects to be identified and communicate with each other . In this section we discuss the relevant technologies that can help in the large-scale development of IoT.

4.1 Wireless Sensor Network (WSN)

WSN is a bi-directional wirelessly connected network of sensors in a multi-hop fashion, built from several nodes scattered in a sensor field each connected to one or several sensors which can collect the object specific data such as temperature, humidity, speed etc and then pass on to the processing equipment. The sensing nodes communicate in multi-hop Each sensor is a transceiver having an antenna, a micro-controller and an interfacing circuit for the sensors as a communication, actuation and sensing unit respectively along with a source of power which could be both battery or any energy harvesting technology However has proposed an additional unit for saving the data, named as Memory Unit which could also be a part of the sensing node. A typical sensing node is shown in the figure below:



Wireless Sensors Network technology and RFID technology when combined together opens up possibilities for even more smart de- vices, for which a number of solutions have been proposed . An example solution is provided by the Intel Research Labs in the form of Wireless Identification Sensing Platform (WISP). WISP is a passive wireless sensor network with built-in light, temperature and many other

sensors. Both WSN and RFID Sensor Networks have their own advantages but RFID Sensor Networks have a low range and their communication is Asymmetric while WSNs have a comparatively longer range and their communication is Peer-to- Peer. Moreover most of the WSNs are based on the IEEE 802.15.4 standard, which specifies the Physical and MAC layer of Low- Rate Wireless Personal Area Networks (LR-WPANs).

The technologies that enables the integration of WSN with the IOT are a hot research topic, many solutions have been proposed for that including that of a 6LOWPAN standard, that allows IPv6 pack- ets to be transmitted through the networks that are computationally restricted. Also there's ROLL routing standard for end-to-end rout- ing solutions.

4.2 Cloud Computing

With millions of devices expected to come by 2020, the cloud seems to be the only technology that can analyze and store all the data effectively. It is an intelligent computing technology in which number of servers are converged on one cloud platform to allow sharing of resources between each other which can be accessed at any time and any place. Cloud computing is the most important part of IoT, which not only converges the servers but also processes on an increased processing power and analyzes the useful infor- mation obtained from the sensors and even provide good storage capacity. But this is just a beginning of unleashing the true po- tential of this technology. Cloud computing interfaced with smart objects using potentially millions of sensors can be of enormous benefits and can help IoT for a very large scale development so re- searches are being carried out since IoT will be totally dependent on the Cloud Computing.

4.3 Networking Technologies

These technologies have an important role in the success of IoT since they are responsible for the connection between the objects, so we need a fast and an effective network to handle a large number of potential devices. For wide-range transmission network we com- monly use 3G, 4G etc. but As we know, mobile traffic is so much predictable since it only has to perform the usual tasks like making a call, sending a text message etc. so as we step into this modern era of ubiquitous computing, it will not be predictable anymore which calls for a need of a super-fast, super-efficient fifth generation wire- less system which could offer a lot more bandwidth . Similarly for a short-range communication network we use technologies like Bluetooth, WiFi etc.

4.4 Nano Technologies

This technology realizes smaller and improved version of the things that are interconnected. It can decrease the consumption of a sys- tem by enabling the development of devices in nano meters scale which can be used as a sensor and an actuator just like a normal device. Such a nano device is made from nano components and the resulting network defines a new networking paradigm which is Internet of Nano-Things

4.5 Micro-Electro-Mechanical Systems (MEMS) Technologies

MEMS are a combination of electric and mechanical components working together to provide several applications including sensing and actuating which are already being commercially used in many field in the form of transducers and accelerometers etc. MEMS

combined with Nano technologies are a cost-effective solution for improvising the communication system of IoT and other advan- tages like size reduction of sensors and actuators, integrated ubiq- uitous computing devices and higher range of frequencies etc .

4.6 Optical Technologies

Rapid developments in the field of Optical technologies in the form of technologies like Li-Fi and Cisco's BiDi optical technology could be a major breakthrough in the development of IoT. Li-Fi, an epoch-making Visible Light Communication (VLC) technology, will provide a great connectivity on a higher bandwidth for the ob- jects interconnected on the concept of IoT. Similarly Bi-Directional (BiDi) technology gives a 40G ethernet for a big data from multi- farious devices of IoT .

5. APPLICATIONS

Most of the daily life applications that we normally see are al- ready smart but they are unable to communicate with each other and enabling them to communicate with each other and share use- ful information with each other will create a wide range of inno- vative applications . These emerging applications with some autonomous capabilities would certainly improve the quality of our lives. A few of such applications are already in the market , let's take the example of the Google Car which is an initiative to provide a self-driving car experience with real-time traffic, road conditions, weather and other information exchanges, all due to the con- cept of IoT. There are a number of possible future applications that can be of great advantage. In this section, we present few of these applications.

5.1 Smart Traffic System. Traffic is an important part of a soci- ety therefore all the related problems must be properly addressed. There is a need for a system that can improve the traffic situation based on the traffic information obtained from objects using IoT technologies . For such an intelligent traffic monitoring sys- tem, realization of a proper system for automatic identification of vehicles and other traffic factors is very important for which we need IoT technologies instead of using common image processing methods . The intelligent traffic monitoring system will provide a good transportation experience by easing the congestion. It will provide features like theft-detection, reporting of traffic accidents, less environmental pollution. The roads of this smart city will give diversions with climatic changes or unexpected traffic jams due to which driving and walking routes will be optimized . The traf- fic lighting system will be weather adaptive to save energy. Avail- ability of parking spaces throughout the city will be accessible by everyone.

5.2 Smart Environment. Prediction of natural disasters such as flood, fire, earthquakes etc will be possible due to innovative tech- nologies of IoT. There will be a proper monitoring of air pollution in the environment.

5.3 Smart Home. IoT will also provide DIY solutions for Home Automation with which we will be able to remotely con- trol our appliances as per our needs. Proper monitoring of utility meters, energy and water supply will help saving resources and detecting unexpected overloading, water leaks etc. There will be proper encroachment detection system which will prevent burglar- ies. Gardening sensors will be able to measure the light, humidity, temperature, moisture and other gardening vitals, as well as it will water the plants according to their needs.

5.4 Smart Hospitals. Hospitals will be equipped with smart flexible wearable embedded with RFID tags which will be given to the patients on arrivals, through which not just doctors but nurses will also be able to monitor heart rate, blood pressure, temperature and other conditions of patients inside or outside the premises of hospital . There are many medical emergencies such as cardiac arrest but ambulances take some time to reach patient, Drone Am- bulances are already in the market which can fly to the scene with the emergency kit so due to proper monitoring, doctors will be able to track the patients and can send in the drone to provide quick medical care until the ambulance arrive.

5.5 Smart Agriculture. It will monitor Soil nutrition, Light, Humidity etc and improve the green housing experience by au- tomatic adjustment of temperature to maximize the production. Accurate watering and fertilization will help improving the water quality and saving the fertilizers respectively.

5.6 Smart Retailing and Supply-chain Management. IoT with RFID provides many advantages to retailers. With RFID equipped products, a retailer can easily track the stocks and detect shoplift- ing. It can keep a track of all the items in a store and to prevent them from going out-of-stock, it places an order automatically. Moreover the retailer can even generate the sales chart and graphs for effec- tive strategies.

6. SECURITY AND PRIVACY CHALLENGES

IoT makes every thing and person locatable and addressable which will make our lives much easier than before; however without a lack of confidence about the security and privacy of the user's data, it's more unlikely to be adopted by many . So for its ubiquitous adoption, IoT must have a strong security infrastructure. Some of the possible IoT related issues are as followed:

6.1 Unauthorized Access to RFID

An unauthorized access to tags that contains the identification data is a major issue of IoT which can expose any kind of confidential information about the user so it needs to be addressed. Not just the tag can be read by a miscreant reader but it can even be modified or possibly be damaged. In this context, summarized some of the real life threats of RFID which includes RFID Virus, Side Channel Attack with a cell-phone and SpeedPass Hack.

6.2 Sensor-Nodes Security Breach

WSNs are vulnerable to several types of attacks because sensor nodes are the part of a bi-directional sensor network as discussed in Section 4.2, which means other than the transmission of data, ac- quisition of data is also possible. described some of the possi- ble attacks that includes Jamming, tampering, Sybil, Flooding and some other kinds of attacks, which are summarized as followed:

(1) Jamming obstructs the entire network by interfering with the frequencies of sensor nodes.

(2) Tampering is the form of attack in which the node data can be extracted or altered by the attacker to make a controllable node.

(3) Sybil attack claims multiple pseudonymous identities for a node which gives it a big influence.

(4) Flooding is a kind of a DOS attack caused by a large amount of traffic that results in memory exhaustion.

6.3 Cloud Computing Abuse

Cloud Computing is a big network of converged servers which allow sharing of resources between each other. These shared re- sources can face a lot of security threats like Man-in-the-middle attack (MITM), Phishing etc. Steps must be taken to ensure the complete security of the clouding platform . Cloud Security Alliance (CSA) proposed some possible threats among which few are Malicious Insider, Data Loss, Accounts Hijacking and Mon- strous use of Shared Computers etc which are summarized as followed:

(1) Malicious Insider is a threat that someone from the inside who have an access to the user's data could be involved in data ma- nipulating. (2) Data Loss is a threat in which any miscreant user who has an unauthorized access to the network can modify or delete the existing data. (3) Man-in-the-middle (MITM) is a kind of Account Hijacking threat in which the attacker can alter or intercept messages in the communication between two parties. (4) Cloud computing could be used in a monstrous ways because if the attacker gets to upload any malicious software in the server e.g. using a zombie-army (botnet), it could get the attacker a control of many other connected devices.

7. CONCLUSION

With the incessant burgeoning of the emerging IoT technologies, the concept of Internet of Things will soon be inexorably develop- ing on a very large scale. This emerging paradigm of networking will influence every part of our lives ranging from the automated houses to smart health and environment monitoring by

embedding intelligence into the objects around us. In this paper we discussed the vision of IoT and presented a well-defined architecture for its deployment. Then we highlighted various enabling technologies and few of the related security threats. And finally we discussed a number of applications resulting from the IoT that are expected to facilitate us in our daily lives. Researches are already being car- ried out for its wide range adoption, however without addressing the challenges in its development and providing confidentiality of the privacy and security to the user, it's highly unlikely for it to be an omni-present technology. The deployment of IoT requires strenuous efforts to tackle and present solutions for its security and privacy threats.

8. REFERENCES

[1] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer and Shahid Khan, "Future Internet: The Internet of Things Archi- tecture, Possible Applications and Key Challenges," in Pro- ceedings of Frontiers of Information Technology (FIT), 2012, pp. 257-260

[2] Guicheng Shen and Bingwu Liu, "The visions, technologies, applications and security issues of Internet of Things," in E -Business and E -Government (ICEE), 2011, pp. 1-4

[3] Ling-yuan Zeng, "A Security Framework for Internet of Things Based on 4G Communication," in Computer Science and Network Technology (ICCSNT), 2012, pp. 1715-1718

[4] "The "Only" Coke Machine on the Internet," Carnegie Mellon University, School of Computer Science.

[5] Nich Heath, "What the Internet of Things means for you". It can be accessed at: http://www.techrepublic.com/blog/european- technology/what-the-internet-of-things-means-for-you

[6] "Twine" by Supermechanical. It can be accessed at: http://supermechanical.com/twine

[7] Bob Violino, "Top IT Vendors reveal their IOT strategies". It can be accessed at: http://www.networkworld.com/article/2604766/internet-of- things/top-it-vendors-reveal-their-iot-strategies.html

[8] Harald Sundmaeker, Patrick Guillemin, Peter Friess, Sylvie Woelffl, "Vision and challenges for realising the Internet of Things," Publications Office of the European Union, 2010

[9] Gartner, Inc. It can be accessed at: http://www.gartner.com/newsroom/id/2905717

[10] "From the ARPANET to the Internet" by Ronda Hauben - TCP Digest (UUCP). Retrieved 2007-07-05 It can be accessed at: http://www.columbia.edu/ rh120/other/tcpdigest paper.txt

[11] Jian An, Xiao-Lin Gui, Xin He, "Study on the Architecture and Key Technologies for Internet of Things," in Advances in Biomedical Engineering, Vol.11, IERI-2012, pp. 329-335

[12] Lan Li, "Study of Security Architecture in the Internet of Things," in Measurement, Information and Control (MIC), 2012, Volume: 1, pp. 374-377