International Journal of Computer Techniques -– Volume 3 Issue 4, July - Aug 2016

RESEARCH ARTICLE OPEN ACCESS

A Review and Survey on IOT Techniques for Automating Devices

Rachel Hannah[1] ,Praveen Jayasankar[2] , Prashanth Jayaraman[3].,

1, 2,,3 Department Computer Science and Engineering
1 St.Joseph's College of Engineering, Chennai-119
2,3 Meenakshi Sundararajan Engineering College,Chennai

----------**********----------

Abstract:

Nowadays world of Internet is changing towards Internet-of-Things simply called as IoT, where all things which we use in our day to day life connects to internet and can be monitor & can be operate remotely. IoT has many applications in all domains such as industrial wireless sensor network, smart homes, agriculture, etc. IoT uses standard protocols and predefined architecture for deployment using Smart technologies such as Radio Frequency Identification, Wireless Sensors, Actuators, Zigbee, etc. for communication. Applications of IoT are increasing day by day in many domains. This paper proposed an overview on architecture of IoT and technologies used in IoT. Applications of IoT, Problems in IoT and suitable solutions are also presented in this survey paper.

Keywords— **Internet of Things (IoT), System Architecture, Radio Frequency Identification.**

----------**********----------

I. INTRODUCTION

Today's internet is changing day by day as its application getting increases and new developments in its architecture. Internet of Things (IoT) is a new revolution of the Internet. Internet of Things (IoT) is can be said the expansion of internet services. It provides a platform for communication between objects where objects can organize and manage themselves. It makes objects themselves recognizable. The internet of things allows everyone to be connected anytime and anywhere [1]. Objects can be communicated between each other by using radio frequency identification (RFID), wireless sensor network (WSN) [3], Zigbee, etc. Radio Frequency identification assigns a unique identification to the objects [3-4] [7]. RFID technology is used as more secure identification and for tracking/locating objects, things, vehicles, etc. [4].

In simple words, when the objects or things connected with each other using standard protocols and standard infrastructure so that they can communicate between each other and all these objects/things can be monitored and controlled by anywhere and anytime using internet then it can be called as Internet-of-Things (IoT). The IoT was began in the year 1998 and the term Internet of Things was first called by Kevin Ashton in 1999 [1]. System architecture of IoT is shown in figure 1. Layered architecture of IoT is also shown in figure 2 [10].

In system architecture (a) all the things such as objects in smart homes, vehicale, electronics gadets, etc. are connected to internet. To understand more clearly one another system architecture is shown in figure (b).

According to the IEEE Internet of Things journal, An IoT system is a network of networks where, typically, a massive number of objects/things/sensors/devices are connected through communications and information infrastructure to provide value-added services via intelligent data processing and management for different applications.

Fig. 1. System Architecture of Internet-of-Things (IoT)

The Internet of Things (IoT) is a computing concept where physical objects may be real or virtual will connects to the internet and they can identify themselves and organize themselves [1]. RFID, zigbee, WSN, etc are used for the communication between themselves. According to The Internet of Things European Research Cluster (IERC) definition states that IoT is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network [1].

Layer based architecture of IoT is shown below in fig.2

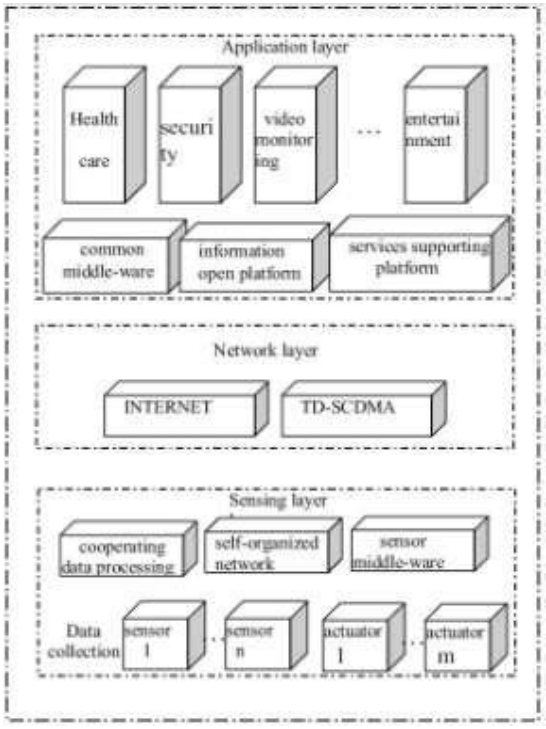

Fig. 2. Layer based Architecture of IoT [12]

Sensing Layer: Sensing layer is the first layer as shown in figure. All the data collection from the outside world done in this layer with the use of sensors, actuators, GPs terminal, etc. data get collected into the digital form and send further for the next procedure [2] [12].

Network Layer: The use of internet layer is to set up the internet connection and save the logs of the connections. Multiplexing and demultiplexing of the data held in this layer.

Application Layer: Application layer creates the Internet of things and makes interface with wide and achieves the intelligent application of Internet of things. All the applications of IoT cover into this layer. Software developer should make the software and applications user friendly with the knowledge of application layer [2].

II. APPLICATION DOMAINS

Applications of IoT are very diversify. Applications of IoT are increasing every day in many domains. Every day human changes his needs and as per need he use the internet and hence Internet-of-Things. As explained in [1] all applications of IoT which are developed so far and which are yet to be developed comes in three broad domains which are Society, Environment, and Industry as shown in table 1.

Domain	Description	Applications
Society	Activities related to the betterment and development of society, cities and people	Smart Cities, Smart Animal Farming, Smart Agriculture, Healthcare, Domestic and Home automation, Independent Living, Telecommunications, Energy, Defense, Medical technology, Ticketing, Smart Buildings
Environment	Activities related to the protection, monitoring and development of all natural resources	Smart Environment, Smart Metering, Smart Water Recycling, Disaster Alerting
Industry	Activities related to financial, commercial transactions between companies, organizations and other entities	Retail, Logistics, Supply Chain Management Automotive, Industrial Control, Aerospace and Aviation

Table 1. IoT Application Domains [1]

IoT can be used for web business applications on large scale. The Web of Things Service Environment (WoTSE) concept has been already developed [2].

Wireless sensors have many uses in every field. For Internet of Things wireless sensors have many applications on large field. Wireless sensor networks are used in industries as well. In particular, Wireless Sensor Networks (WSNs) are connecting things to the Internet through a gateway that interfaces the WSN to the Internet [3].

Smart Homes system using IoT is the application which has more demand for our homes. A smart home is the home or that living environment having technology to allow all the household devices/home appliances to be controlled automatically and can be controlled remotely [12]. In Smart homes user can easily monitor and control all home devices/home appliances through internet. Home appliances connect in predefined proper network architecture and using standard protocols. Basic idea for Smart Homes using IoT is shown in figure 3 [13].

The whole system can be divided into two parts: in one part consist all the home devices and switch modules and RF transmitter receiver and in second part include all the interface device, processor, data collector, GPRS module that will communicate with the internet.

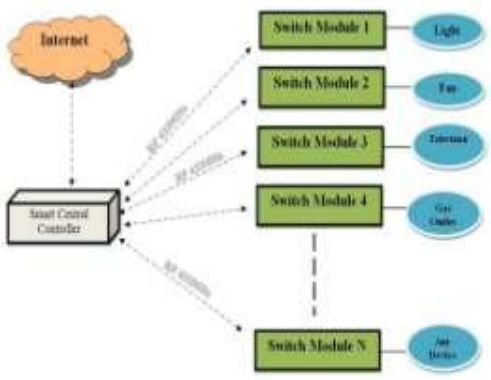

Fig. 3. Basic idea for Smart Home System using IoT [13]

In this we have shown only four households devices: Light, Fan, Television, Gas outlet are shown. But user can connects number of devices to the system. These all household devices will connect to the switch modules. Switch module may contain any type of module which changes its state as it received signal. Switch module connected to the device in such a way that when it change the state, the state of household device connects to it will also change [12] [13]. Relays can be used as a switch module. It is an electromagnetic device or normally called as relay switch. It isolates two circuits electrically and connects them magnetically [14]. Switch modules will connect to the smart central controller through RF transceiver. Each switch module and device will be identified by assigning a unique identity to them. One RF transceiver will connects at the smart central controller. RF modules communicate between themselves at 433MHz. 433MHZ spectrum is specially made for the RF communication [4] [6] [10] [13]. Smart central controller will act as interface device between household devices and internet server. It will be the set of devices like microcontroller, CPLD processor, RF transceiver, GPRS or Zigbee module, etc. Microcontroller can be used as a main controller and for data processing. Data acquisition can be easily done by microcontroller hence it can be act as interface device [12].

RELATED WORK AND TECHNOLOGIES USED

The different applications which are adopted and the technologies used so far for IoT are presented by Dr. V. Bhuvaneswari and Dr. R Porkodi in [1]. The overview of sensors and their standards are also explained in [1].

The application based architecture of IoT is explained with their importance and applications such as smart homes by Nan LIN, Weihang SHI in [2].Web of Internet business environment and its architecture with key technologies is given in [2].

Wireless sensors can also be used for IoT. Wireless sensors can be connected into the network and sensors can be operated from the web. Nacer Khalil, Mohamed Riduan Abid, Driss Benhaddou and Michael Gerndt presented the integration of wireless sensor network in IoT [3].

Radio Frequency Identification is already used for internet of things. But it has been seen that there are many

problems occurs when RF ID is used for IoT. Dietmar P.F. Möller and Hamid Vakilzadian have proposed an architecture of IoT and use of RF ID, Problems comes in use of RF ID and solutions on the problem in [4]. As the use of Radio frequency is getting more the problems of collision of signals would occur. Hence, For anti-collision in RFID scheme, WANG Shoufeng, ZHANG Dongchen, XU Xiaoyan, SHI Shumeng and WANG Tinglan proposed A novel anti-collision scheme for RFID systems in [6].

When physical devices get connected to the internet we have to deal with security problems. Jose L. Hernandez-Ramos, Marcin P. Pawlowski, Antonio J. Jara, Antonio F. Skarmeta and Latif Ladid have proposed a set of lightweight authentication and authorization mechanisms in order to support smart objects during their life cycle [5]. For secure authorization Simone Cirani, Marco Picone, Pietro Gonizzi, Luca Veltri, and Gianluigi Ferrari have proposed IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios in [7].

Charith Perera, Chi Harold Liu, Srimal Jayawardena, and Min Chen have given a full survey on a variety of popular and innovative IoT solutions in terms of context-aware technology perspectives and they evaluate these IoT solutions using a framework that they built around well-known context aware computing theories. They presented a guideline and a conceptual framework for context-aware product development and research in the IoT paradigm [8].

As the applications of IoT are increasing and IoT is expanding on large scale there may be problem in expansion on IoT and handling the devices connected into the IoT network will get difficult [9]. Chayan Sarkar, Akshay Uttama Nambi S. N., R. Venkatesha Prasad, Abdur Rahim, Ricardo Neisse, and Gianmarco Baldini have proposed a Distributed Internet-like Architecture for Things (DIAT), which will overcome most of the obstacles in the process of large scale expansion of IoT. It specifically addresses heterogeneity of IoT devices, and enables seamless addition of new devices across applications. They have proposed a layered architecture that provides various levels of abstraction to tackle the issues such as, scalability, heterogeneity, security and interoperability. This architecture would increase the security in the system [9].

The customer domain of the smart grid naturally blends with smart home and smart building systems, but typical proposed approaches are “distributor-centric” rather than

“customer-centric,” undermining user acceptance, and are often poorly scalable. To solve this problem, Elisa Spanò, Luca Niccolini, Stefano Di Pascoli, and Giuseppe Iannaccone proposed a detailed architecture and an implementation of a “last-meter” smart grid—the portion of the smart grid on customer premises—embedded in an internet-of-things (IoT) platform. Their approach has four aspects of novelty and advantages with respect to the state of the art: 1) seamless integration of smart grid with smart home applications in the same infrastructure; 2) data gathering from heterogeneous sensor communication protocols; 3) secure and customized data access; and 4) univocal sensor and actuator mapping to a common abstraction layer on which additional concurrent applications can be built. They demonstrated this system with the use of zigbee technology [11].

As we discussed Smart homes system is one of the expanding applications of IoT. New implementation with the use of new technologies is going on for smart homes system. Kang Bing, Liu Fu, Yun Zhuo, and Liang Yanlei have given the implemented smart homes system using IoT in [12] and they have eliminated the previous bugs in the same such as poor portability, weak updating capability, and personal computer dependence [12].

IV. PROBLEMS IN IOT

In this paper we have seen that many new technologies have been implemented and many drawbacks have been overcome for IoT. But still there are some problems would come in the future when the Internet of Things will get expand on large scale. Some of the major problems that could come are presented below:

Network architecture: Network architecture of IoT varies for different applications and with the change in communication modules [1] [9].

Privacy and Security: When many things get connected to internet definitely there will be the issues in data privacy and security. Applications of IoT are increasing rapidly, hence there is need to secure the communication and privacy of data. There are many types of attacks and there are many ways the whole system could be attacked [1] [7].

Data Intelligence: IoT is expanding every day. In future there will be lots of things get connected to

the IoT network, hence the huge of data collection will be done. The data handling, data processing, etc. we will need to develop intelligence algorithms so that these algorithms will achieve automated decision making [1].

Integration and Scalability: The main challenge with IoT will be to integrate applications in IoT environment

[11].

Identification: Identification is required for each device so that each device can identify uniquely whether we used RF ID, Zigbee or any communication module. [1]

[10].

Use of RFID: Radio frequency is used for many applications. Hence the collision can occur when the huge of applications will use radio frequency [4] [6].

Standards: Standardization is very essential for IoT environment as it is expanding globally. Challenges are comes related which standard should be used, which will provide secure medium, how it will make system more reliable.

CONCLUSION

Applications of Internet are increasing day by day. In most of the domain we need Internet for use. Internet-of-Things can be said as the application of internet and use of some hardware parts. In this paper the system architecture of IoT is presented. We have shown many domains where internet of things is used in this paper. But this is not limited only for the above domain. The use of internet of things is increasing rapidly. We presented most of the application domains where IoT is used. We have presented the technologies used for internet of things and the problems would come in the same.

REFERENCES

Dr. V. Bhuvaneswari, Dr. R Porkodi, “The Internet of

Things (IoT) Applications and Communication

Enabling Technology Standards: An Overview”, International Conference on Intelligent Computing Applications, 2014, pp. 324-329

Nan LIN, Weihang SHI, “The Research on Internet of Things Application Architecture Based on Web”, IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA), 2014, pp. 184-187

Nacer Khalil, Mohamed Riduan Abid, Driss

Benhaddou, Michael Gerndt, “Wireless Sensors Networks for Internet of Things”, IEEE Ninth

International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) Symposium on Public Internet of Things, Singapore, 21–24 April 2014, pp. 1-6

Dietmar P.F. Möller, Hamid Vakilzadian, “Wireless

Communication in Aviation Through the Internet of

Things and RFID”, 2014, pp. 602-607

Jos´e L. Hern´andez-Ramos, Marcin P. Pawlowski, Antonio J. Jara, Antonio F. Skarmeta and Latif Ladid,

“Towards a Lightweight Authentication and Authorization Framework for Smart Objects”, IEEE 2015, pp. 1-14

WANG Shoufeng, ZHANG Dongchen, XU Xiaoyan,

SHI Shumeng, WANG Tinglan, “A Novel Anti-collision Scheme for RFID Systems”, IEEE World

Forum on Internet of Things (WF-IoT), 2014, pp. 458-461

Simone Cirani, Marco Picone, Pietro Gonizzi, Luca

Veltri, and Gianluigi Ferrari, “IoT-OAS: An

OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios", IEEE Sensors Journal, vol. 15, NO. 2, February 2015, pp. 1224-1234

Charith Perera, Chi Harold Liu, Srimal Jayawardena, And Min Chen, "A Survey on Internet of Things From Industrial Market Perspective", IEEE access The journal for rapid open access publishing, volume 2, 2014, pp. 1660-1679

Chayan Sarkar, Akshay Uttama Nambi S. N., R. Venkatesha Prasad, Abdur Rahim, Ricardo Neisse, and Gianmarco Baldini, "DIAT: A Scalable Distributed

Architecture for IoT", IEEE Internet of Things journal, vol. x, no. x, 2014, pp. 1-10

Roy Want, Bill N. Schilit, and Scott Jenson, "Enabling the Internet of Things", IEEE computer society, 2015,

28-35

Elisa Spanò, Luca Niccolini, Stefano Di Pascoli, and Giuseppe Iannaccone, "Last-Meter Smart Grid Embedded in an Internet-of-Things Platform", IEEE Transactions on smart grid, vol. 6, no. 1, January 2015,

468-476

Kang Bing, Liu Fu, Yun Zhuo, and Liang Yanlei,

"Design of an Internet of Things-based Smart Home System", The 2nd International Conference on Intelligent Control and Information Processing, July 2011, pp. 921-924.

[13] Ming Wang, Guiqing Zhang, Chenghui Zhang, Jianbin Zhang, and Chengdong Li,"An IoT-based Appliance

Control System for Smart Homes", Fourth International Conference on Intelligent Control and Information Processing (ICICIP) June 9 – 11, 2013, pp. 744-747

[14] Vladimir Gurevich, "Electric Relays Principles and Applications", Taylor and Francis Group, 2006, pp. 1-52