International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

A Comprehensive Study on IoT

K.Radhika Reddy
Assoc .Prof,Dept. of ECE
Jyothishmathi Institute Of Technology And Science, Karimnagar

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 communication is machine-machine (M2M). This paper aims to provide a comprehensive overview of the IoT scenario and reviews its enabling technologies and the sensor networks. Also, it describes a six-layered architecture of IoT and points out the related key challenges.

Keywords:

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

1. INTRODUCTION

With the continuous advancements in technology a potential innovation, IoT is coming down the road which is burgeoning as an ubiquitous global computing network where everyone and everything will be connected to the Internet [1]. IoT is continually evolving and is a hot research topic where opportunities are infinite. Imaginations are boundless which have put it on the verge of reshaping the current form of internet into a modified and integrated version. The number of devices availing internet services is increasing every day and having all of them connected by wire or wireless will put a powerful source of information at our finger tips. The concept of enabling interaction between intelligent machines is a cutting-edge technology but the technologies composing the IoT are not something new for us [2]. IoT, as you can guess by its name, is the approach of converging data obtained from different kinds of things to any virtual platform on existing Internet infrastructurThe basic idea of IoT is to allow autonomous exchange of useful information between invisibly embedded different uniquely identifiable real world devices around us, fueled by the leading technologies like Radio-Frequency IDentification (RFID) and Wireless Sensor Networks (WSNs) [2] which are sensed by the sensor devices and further processed for decision making, on the basis of which an automated action is performed [1].

2. ARCHITECTURE

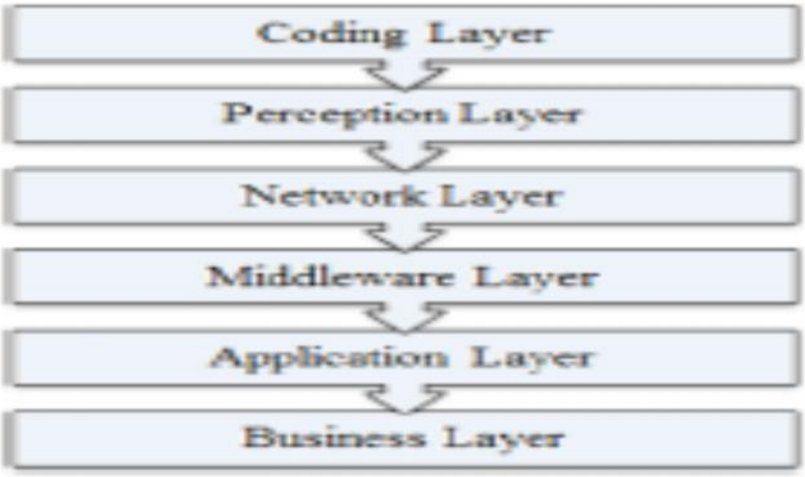
More than 25 Billion things are expected to be connected by 2020 which is a huge number so the existing architecture of Internet with TCP/IP protocols, adopted in 1980 , cannot handle a network as big as IoT which caused a need for a new open architecture that could address various security and Quality of Service (QoS) issues as well as it could support the existing network applications using open protocols [16].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 architecture of IoT while [20] 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. Similarly a six-layered architecture was also proposed based on the network hierarchical structure . So generally it's divided into six layers as shown in the Fig. 2.

The six layers of IoT are described below:

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

2.1 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



2.2Perception 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.

2.3 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 transmission mediums likeWiFi, Bluetooth,WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc [24].

2.4 Middlware Layer

This layer processes the information received from the sensor devices [2]. It includes the technologies like Cloud computing, Ubiquitous computing which ensures a direct access to the database to store all the necessary information in it. Using some Intelligent Processing Equipment, the information is processed and a fully automated action is taken based on the processed results of the information.

2.5 Application Layer

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

2.6 Business Layer

This layer manages the applications and services of IoT and is responsible for all the research related to IoT. It generates different business models for effective business strategies [1].

3. TECHNOLOGIES

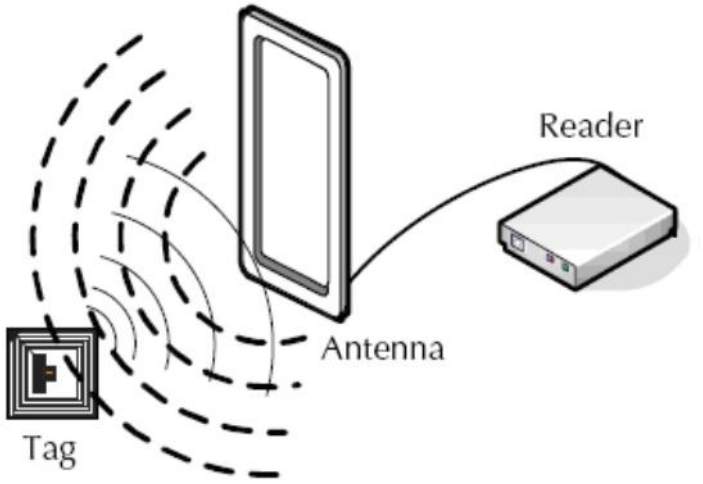
The development of a ubiquitous computing system where digital objects can be uniquely identified and can be able to think and interact with other objects to collect data on the basis of which automated actions are taken, requires the need for a combination of new and effective technologies which is only possible through an integration of different technologies which can make the objects to be identified and communicate with each other . In this section

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

we discuss the relevant technologies that can help in the large-scale development of IoT.

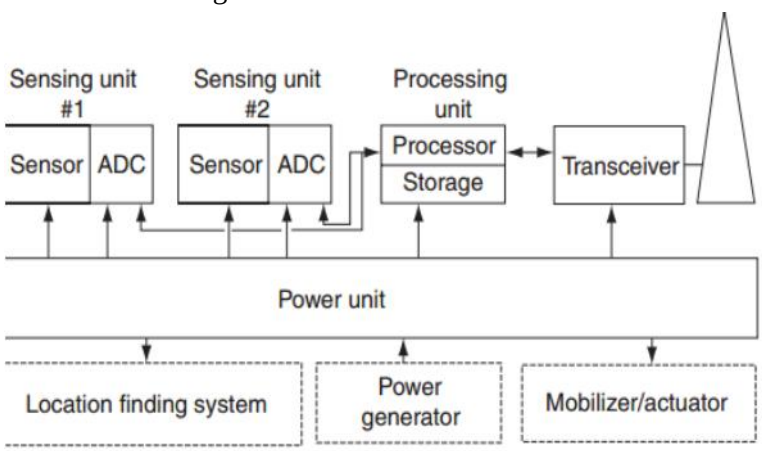
3.1 Radio Frequency IDentification (RFID)

RFID is the key technology for making the objects uniquely identifiable. Its reduced size and cost makes it integrable into any object . It is a transceiver microchip similar to an adhesive sticker which could be both active and passive, depending on the type of application . Active tags have a battery attached to them due to which they are always active and therefore continuously emit the data signals while Passive tags just get activated when they are triggered. Active tags are more costly than the Passive tags however they have a wide range of useful applications [2]. RFID system is composed of readers and associated RFID tags which emit the identification, location or any other specifics about the object, on getting triggered by the generation of any appropriate signal . The emitted object related data signals are transmitted to the Readers using radio frequencies which are then passed onto the processors to analyze the data.



3.2 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 [2] 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:



International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

Wireless Sensors Network technology and RFID technology when combined together opens up possibilities for even more smart devices, for which a number of solutions have been proposed . An example solution is provided by the Intel Research Labs in the form ofWireless 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 [26], which specifies the Physical and MAC layer of Low- Rate Wireless Personal Area Networks (LR-WPANs) [32].

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 [33], that allows IPv6 packets to be transmitted through the networks that are computationally restricted. Also there's ROLL routing standard for end-to-end routing solutions .

3.4 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 commonly 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 wireless system which could offer a lot more bandwidth . Similarly for a short-range communication network we use technologies like Bluetooth, WiFi etc.

3.5 Nano Technologies

This technology realizes smaller and improved version of the things that are interconnected. It can decrease the consumption of a system 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

3.6 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. MEMScombined with Nano technologies are a cost-effective solution for improvising the communication system of IoT and other advantages like size reduction of sensors and actuators, integrated ubiquitous computing devices and higher range of frequencies etc

4. 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 [47]. So for its ubiquitous adoption, IoT must have a strong security infrastructure. Some of the possible IoT related issues are as followed:

5. CONCLUSION

With the incessant burgeoning of the emerging IoT technologies, the concept of Internet of Things will soon be inexorably developing 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 carried 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.

6. REFERENCES

[1] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer and Shahid Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in Proceedings 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] M. Weiser, "The computer for the 21st century", Sci. Amer., 1991, pp.66 -75