A Comprehensive Review on Technologies Applications of IoTs (Internet of Things)

Mrs. Meeta Prajapati
Lecture in Computer Engineering,
Government Polytechnic, Gandhinagar,
Gandhinagar, Gujarat, India

Abstract: - Recent year Internet of Things (IoT) is a technological revolution, which provides connected world vision of Things. Devices, systems and people are connected with one another in such a way that they can correspond with each other over Internet. So the form of communication from human-human is now twisted into human-human, human-things. In this paper introduces Internet of Things (IoTs), which offers capabilities to classified and connect worldwide substantial objects into a unified system. As a part of internet of things, serious concerns are raised over admittance of personal information pertaining to individual privacy and device. This review summarizes the basic introduction, Technologies and application of IoTs.

***Keyword*- Internet of Things, RFID, Wireless Sensor Network, development, cloud.**

I. INTRODUCTION

"Internet of Things" called IoT, related with the thought of "future internet" is a apparition where each object will become a part of the Internet. At this time objects can be any existing entity like animal or humans and any non-living entities on earth. Internet of Technologies is similar to a visualization in which every object that is on network can uniquely be identified, its position and status can be known, it is available to the network and intelligences and services are added to this network. Internet of Technologies will change the information world and technology world considerably to make a more comfortable world full of technology for us. Different types of prototyping hardware boards, on chip systems, RFID, sensors and ubiquitous networking capabilities are supporting candidates for Internet of Technologies evolution [1].

II INTERNET OF THINGS OVERVIEW AND BACKGROUND

What is Internet of Things?

As illustrate in Fig. 1, the Internet of Things allow people and things to be associated anytime, anyplace, with anything, ideally using any path/network and any service [2]. They are "Material objects associated to material objects in the Internet".

For paradigm, through laser scanners, RFID, global writing system, infrared sensors and other information sensing devices are associated to any object for data exchange and communication services. At preceding, to reach the smart devices to be tracked, located, monitored and to handle the network functions, to make the IT infrastructure and physical infrastructure consolidation Internet of Things is the most needed one.

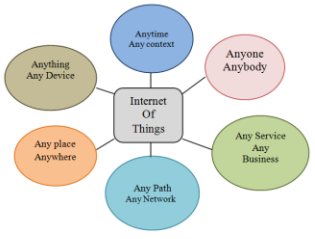

Figure 1 definition of IOT by [2]

DEFINITIONS AND ELEMENTS of IoTs

The definitions are existing here. There are various definitions of IoT are presented in the word.

- Definition by Radio Frequency identification group - The interconnected worldwide network objects exclusively addressable based on standard communication protocols
- Interconnection of actuating and sensing devices providing the capability to share information across platforms through a integrated framework. Emergent a common operating picture for enabling innovative applications [3].
- The IoTs allows people and things to be connected Anyplace, Anytime with Anything and Anyone, ideally using Any path/network and Any service [2].

Internet of Things Elements [3]:

- Radio Frequency Identification (RFID):- Application of RFID in IoTs technology is embedded communication, for designing of microchips for wireless data communication.
- Wireless Sensor Networks (WSN):- Application of WSN are efficient, low power, low cost devices so it is apply to remote sensing applications.
- Addressing Schemes:- Addressing schemes are functional to uniquely identify the "Things" i.e. smart objects.
- Data Analytics and Storage:- Internet of Things deals with storing and sharing of large amount of data. These data have to be stored and used intelligently for smart actuation and monitoring.
- Visualization:- This allows dealings of the user with the environment. Origin of meaningful information from raw data is non-trivial.

III. Architecture of IoTs

Basic of problems with the Internet of Things is that it is so enormous and such a broad concept that there is no projected, uniform architecture. In order for the scheme of IoT to work, it must consist of an sensor range, network, communications and amongst others [4]. Here, several researchers, authors and practitioners present IoT architectures or model.

Basically IoT have the six layers are present below:

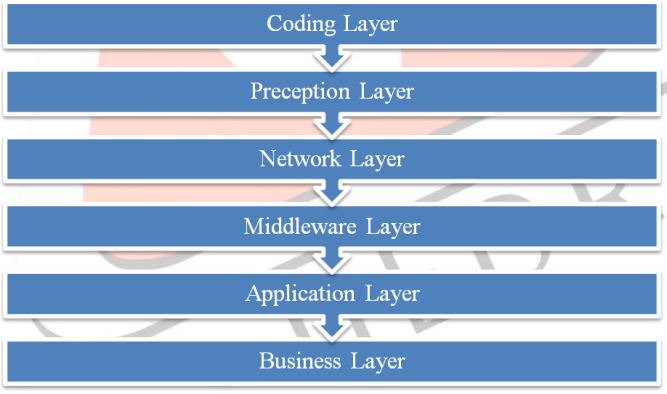

Figure 2 Six-Layered Architecture of IoT

Coding Layer

In this layer is the base of IoT, which provides identification to the objects of interest. Coding layer, every object is assigned a unique ID, which makes it easy to discern the objects [5].

Perception Layer

Perception layer is the device layer of IoT which gives a corporeal meaning to each object. It consists of data sensors in dissimilar forms like RFID tags, IR sensors or other sensor networks [6] which could sense the humidity, temperature, speed and location etc of the objects.

Perception layer gathers the useful information of the objects beginning the sensor devices connected with them and converts the information into digital signals which is then approved onto the Network Layer for further action.

Network Layer

The function of network layer is obtain the useful information in the structure of digital signals from the this Layer and transmit it to the processing systems in the Middleware Layer through the transmission mediums like Bluetooth, WiFi, WiMaX, Zigbee, GSM, 3G etc with protocols similar to IPv4, IPv6, MQTT, DDS etc [7].

- **Middleware Layer**

Middleware layer processes the information received from the sensor devices [8]. This layer includes the technologies similar to Ubiquitous computing, cloud computing which ensures a direct contact to the database to store all the essential information in it. Using some smart Processing Equipment, the information is processed and a fully automated action is taken based on the processed results of the information.

- **Application Layer**

Application layer realizes the applications of Internet of Things for all kinds of industry, based on the processed data. Since applications promote the development of Internet of Things so this layer is very useful in the large scale development of IoT network [9].

- **Business Layer**

Business layer arranges the applications and services of Internet of Things and is responsible for all the research related to IoT. It generates dissimilar business models for effective business strategies [10].

V. TECHNOLOGIES

The progress of a ubiquitous computing system where digital objects can be exceptionally identified and can be able to interact and think with other objects to accumulate data on the basis of which automated actions are taken, requires the necessitate for a combination of new and effective technologies which is only possible through an combination of different technologies which can make the objects to be identified and communicate with each other [11]. In this paper we discuss the relevant technologies that can help in the large-scale development of IoT.

- **Radio Frequency Identification (RFID)**

Radio frequency identification is the key technology for making the objects uniquely identifiable. Its reduced cost and size makes it integral into any object [13]. It has a transceiver microchip similar to an adhesive label which could be both passive and active, depending on the type of application [12]. Passive tags just get activated when they are triggered while Active tags have a battery connected to them due to which they are always active and therefore continuously emit the data signals. Active tags are more expensive than the Passive tags however they have a wide range of useful applications [2]. Radio frequency identification system is collected of readers and associated Radio frequency identification tags which emanate the identification, location or any other specifics about the object, on getting triggered by the any appropriate Radio frequency generated signal [14].

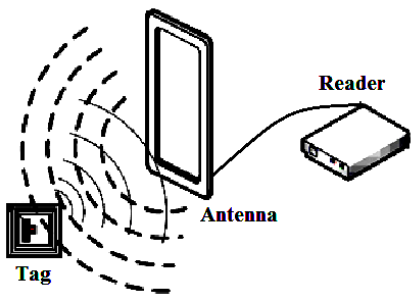

Figure 3. RFID Scenario

Depending on the category of application, Radio frequency identification frequencies are divided into four different frequencies ranges , which are specified below:

(1) Low frequency (135 KHz or less)

(2) Microwave Frequency (2.4G , 5.80)

(3) Ultra-High Frequency (862MHz 928MHz)

(4) High Frequency (13.56MHz)

Bar Code is also another an identification technology which has approximately the same function as an Radio frequency identification but Radio frequency identification is more effective than a Bar Code due to a number of its benefits. Radio frequency identification being a radio technology doesn't require the reader to be physically in its vision while Bar Code is an optical technology which cannot work except its reader is placed in front of it.

Wireless Sensor Network (WSN)

Wireless sensor network is a bi-directional wirelessly linked network of sensors in a multi-hop fashion, built from numerous nodes scattered in a sensor landscape each linked to one or more than a few sensors which can accumulate the object specific data such as humidity, temperature speed etc and then pass on to the processing equipment [13]. The sensing nodes converse in multi-hop all sensor is a transceiver having an antenna, a micro-controller and an interfacing circuit for the sensors as a actuation, communication and sensing unit correspondingly along with a power source which could be both battery or any energy harvesting technology [2]. However, it has projected 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 illustrating in the figure below:

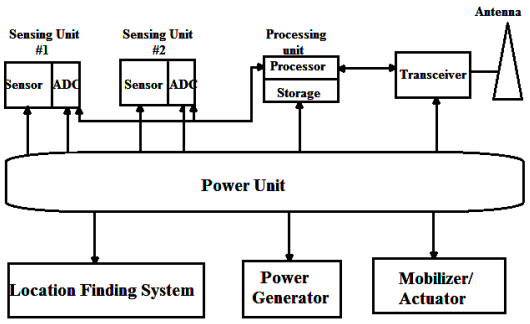

Figure 4 A typical sensing node

Both Wireless sensor network and Radio frequency identification sensor networks have their own advantages but radio frequency identification Sensor Networks have a low range and their communication is asymmetric while Wireless sensor networks have a comparatively longer range and their communication is Peer-to- Peer. Additionally, most of the wireless sensor network is based on the IEEE 802.15.4 standard [13], which specifies the Physical and MAC layer of Low- Rate Wireless Personal Area Networks (LR-WPANs) [14].

Cloud Computing

With numbers of devices projected to come by 2020, the cloud seems to be the only technology that can evaluate and store all the data effectively. It is the most important part of Internet of Things, which not only converges the servers but also processes on an improved processing power and analyzes the useful information obtained from the sensors and even provide good storage capacity [11]. But cloud computing is just a beginning of unleashing the true potential of this technology. It interfaced with smart objects using potentially numbers of sensors can be of massive benefits and can help internet of things for a very large scale development so researches are being carried out since internet of things will be totally dependent on the Cloud Computing.

Figure 5 A typical Cloud Computing Scenario

Networking Technologies

Networking technologies have an essential role in the success of internet of things since they are responsible for the association 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 usually use 3G, 4G etc. but As we know, mobile traffic is so much conventional since it only has to perform the common tasks like making a sending a text message, call 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.

- **Nano Technologies**

Nano technology realizes improved and smaller version of the things that are interconnected. This technology 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 similar to a normal device. Such a nano device is made from nano components and the consequential network defines a new networking standard, which is Internet of nano-Things [15].

- **Micro-Electro-Mechanical Systems (MEMS)**

Technologies of Micro electro mechanical systems are a combination of electric and mechanical components working together to present several applications including sensing and actuating which are already being commercially used in many field in the form of accelerometers and transducers etc. Micro electro mechanical systems combined with nano technologies are a commercial solution for improvising the communication system of Internet of things and other advantages akin to size reduction of sensors and actuators, integrated ubiquitous computing devices and higher range of frequencies etc.

- **Optical Technologies**

Recent year developments in the field of Optical technologies in the form of technologies like Cisco's Bi-Direction and Li-Fi optical technology could be a major get through in the Internet of things development. Li-Fi, an epoch-making Visible Light Communication technology, will afford a great connectivity on a higher bandwidth for the objects interrelated on the concept of IoT.

VI. Application of IoTs

IoTs system is designed for a shopping complex mall but it can be also used in numerous organizations like, Bus stand and Air-port to display the information and notification, educational Notice board system or at Railway station. A few areas where Internet of things frequently used:

i. Smart Cities: -

To construct the city as a smart city to connect with the data exhaust produced from your city and neighbourhood.

ii. Security & Emergencies: -

- Perimeter Access Control is a detection and control of people in non-authorized and restricted.
- Liquid Presence is liquid detection in data centres, sensitive building grounds and warehouses to prevent breakdowns and corrosion.

iii. Smart agriculture: -

- Wine Quality Enhancing is a monitoring soil moisture and trunk diameter in vineyards to organize the amount of sugar in grapes and grapevine health.
- Green Houses is control microclimate conditions to maximize the production of vegetables and fruits and its quality.

iv. Home & Domestic Automation:- In home and domestic by using the internet of things system remotely manage and monitor our home appliances and reduce on your monthly bills and resource usage.

v. Medical field:-

• All detections support for disabled or elderly people living independent.

• Medical fridges is control and monitoring of conditions inside freezers storing medicines, vaccines, and organic elements.

vi. Industrial Control:-

• Machine to Machine Applications: Machine is used auto-diagnosis the problem and control.

• Indoor Air Quality: Monitoring of toxic gas and oxygen levels inside chemical plants to ensure workers and goods safety.

VII. Conclusion

With the continual growing of the emerging Internet of things technologies, the concept of Internet of things will soon be inevitably developing on a very large scale. This rising paradigm of networking will control every part of our lives ranging from the automated houses to smart environment monitoring and health by embedding intelligence into the objects around us. In this paper present the architecture of IoTs and also highlighted various enabling technologies and few of the related applications.

IoTs is numerous usefulness of IoT applications into all the domains including medical, industrial, manufacturing, transportation, education, governance, mining, habitat etc. However, IoT has rich its benefits, there are some flaws in the IoT implementation level and governance. The key observations to IoTs are that (1) Worldwide there is no standard definition (2) in architectural level universal standardizations are required (3) For better global governance, we require to build standard protocols.

REFERENCES

[1] L. Coetzee, J. Eksteen, "The Internet of Things Promise for the Future an Introduction", IST Africa Conference Proceedings, pp. 1- 9, 2011.

[2] C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey", IEEE Communications Surveys & Tutorials, 2013, pp. 1-41

[3] S. Raza, L.Wallgren, T. Voigt, "SVELTE: Real-Time Intrusion Detection in the InternetofThings", Ad Hoc Networks, Elsevier, pp 2661–2674, May 2013.

[4] Gigli, M., Koo S. "Internet of Things, Services and Applications Categorization Advances in Internet of Things", **1**, 27-31, 2011. http://dx.doi.org/10.4236/ait.2011.12004

[5] Xu Cheng, Minghui Zhang, Fuquan Sun, "Architecture of internet of things and its key technology integration based-on RFID", in Fifth International Symposium on Computational

[6] Intelligence and Design, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy in Internet of Things (iThings/CPSCom)", pp. 294-297, 2012

[7] Ying Zhang, "Technology Framework of the Internet of things and Its Application," in Electrical and Control Engineering (ICECE), pp. 4109-4112, 2011.

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

[9] MiaoWu, Ting-lie Lu, Fei-Yang Ling, ling Sun, Hui-Ying Du, "Research on the architecture of Internet of things", in Advanced Computer Theory and Engineering (ICACTE), pp. 484-487, 2010

[10] 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), pp. 257-260, 2012

[11] Benjamin Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy" Internet of Things (iThings/CPSCom), pp. 709-712, 2011

[12] L.Atzori, A.Iera, G. Morabito, "AN IBE BASED SECURITY SCHEME OF INTERNET OF THINGS", The Internet of Things: A survey, in Computer Networks - Science Direct Wang Chen, in Cloud Computing and Intelligent Systems (CCIS), pp. 1046, 1049, 2012

[13] H. Zhang, L. Zhu, "Internet of Things: Key technology, architecture and challenging problems", in Computer Science and Automation Engineering (CSAE), Volume: 4, pp. 507-512, 2011.

[14] R. Roman, C. ALcaraz, J.Lopez, N. Sklavos, "Key Management Systems for Sensor Networks in the Context of the Internet of Things", Computers & Electrical Engineering, Volume: 37, Issue: 2, pp. 147-159, 2011.

[15] I.Akyildiz, J.Jornet, "THE INTERNET OF NANOTHINGS," IEEE Wireless Communications, Volume: 17 Issue: 6, pp. 58-63, 2010

[16] S. Sicari, A. Rizzardi, L.A Grieco, A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead", Comput. Netw. 76, 146–164, 2015.

[17] Alcaide, E. Palomar, J. Montero-Castillo and A. Ribagorda, "Anonymous authentication for privacy-preserving IoTs target driven applications", Comput. Secur. 37, 111–123, 2013.

[18] S. Papadopoulos, Y. Yang, D. Papadias, "Cads: continuous authentication on data streams", in: Proceedings of the 33rd International Conference on Very Large Data Bases, VLDB 07, Vienna, Austria, pp. 135–146,2007.