ISSN:2231-0711

Rohit Tiwari et al | IJCSET(www.ijcset.net) | 2018 | Volume 8 Issue 4, 48-51

Internet of Things (IoT) – Challenges and Applications

Rohit Tiwari[#1]

[#1]*Computer Engineering & Information Technology Department,*
K.J. Institute of Engineering & Technology
Savli, Vadodara, Gujarat, India

Monika Kohli[*2]

[*2]*Information Technology & Computer Engineering Department,*
K.J. Institute of Engineering & Technology
Savli, Vadodara, Gujarat, India

***Abstract*— The Internet can be taken as a prodigious amalgamation of the powers of a system having Hardware and Software, as they say, you may like it or dislike it, but you cannot ignore the Internet. The Internet is said to be one of the most remarkable inventions of its time and it is the most used form of intercommunication, be it person to person or person to the machine. But there is one more form of intercommunication, getting popular nowadays, is Machine to Machine, wherein machines at both sides are not explicitly supervised by a person at that very time. The Internet of Things (IoT) is behind the evolution of this very form of intercommunication and also works as the backbone technology for the same. This research paper is an effort by the researchers to put some light on some of the most fundamental aspects of this phenomenal technology known in the world of technology, as the Internet of Things (IoT).**

***Keywords*— Internet of Things, IoT, Smart, Sensors, Network, Computing, Security.**

I. INTRODUCTION

The Internet of Things (IoT), with its recent advancement, is having a roaring success into the comprehensive computing network of the Ubiquitous computing around the globe. The opportunities are never-ending and, there is no end to the imaginations to what can be accomplished with, the rapid advancements in the field of the Internet of Things (IoT). As it is going to transform the way we are thinking of internet, the internet is going be now something very diverse, that we ever imagined of it could be [1]. Day by day, more and more devices are getting connected to the internet, by whatsoever means possible, making the Internet of Things (IoT) to nurture in its comprehensive arrangement towards becoming the pioneer of the new technological era of Global Computing System.

Since its inception, back in 1982, when it was first used commercially, the Internet of Things (IoT) has come this far to rule globally and still way more to bolster [2]. The fundamental thought behind the Internet of Things (IoT) is to use the existing internet infrastructure to provide a base to a special virtual platform which is capable of accepting and processing of various types of data from an enormous number of devices around the globe.

II. ARCHITECTURE

It is mid-2018 now, and according to the speculation which states that in the coming two to three years, there will be more than quarter of a billion devices in the network of the IoT, which are going to be connected through the Internet. This number is gigantic enough to cause failure to the current TCP/IP based network architecture of the Internet used for IoT. The solution to this problem is to work over the development of a new open architecture to confront numerous security problems and QoS (Quality of Service) concerns, and also the current network applications can be reinforced with the help of open protocols [4]. As the protection of user's privacy and their data are the prime concerns for IoT, and if not addressed adequately, not having a privacy assurance is certainly going to affect how IoT will be accepted by masses.

There are lot many multi-scale architectures for security are proposed for the future stages of development in the field of IoT.

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.

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.

Network Layer

The purpose of this layer is to 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.

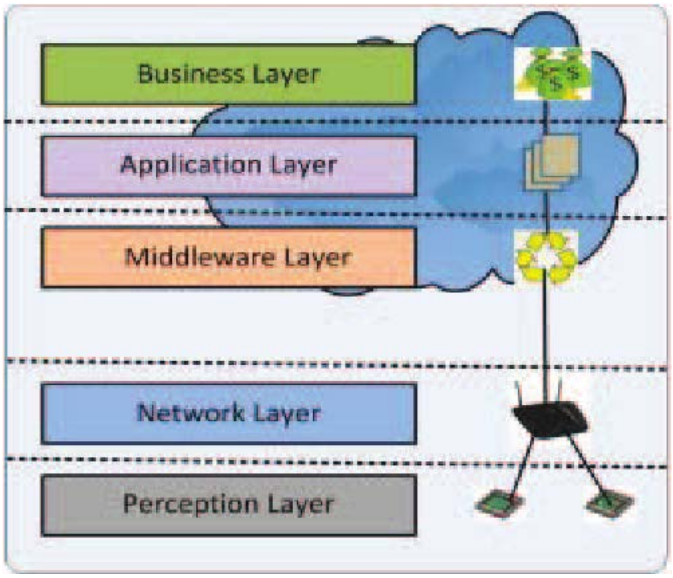

Fig. 1 IoT Architecture

Middleware Layer

This layer processes the information received from the sensor devices. 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 Pro- cessing Equipment, the information is processed and a fully auto- mated action is taken based on the processed results of the information

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

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.

III. TECHNOLOGIES

An amalgamation of latest and efficient technologies is required to establish a ubiquitous computing system, and it is solitarily conceivable with the help of assimilating various technologies. With the help of such technologies, the participating devices can be recognized and interconnect with one another, and it is also the fundamental requirement for a ubiquitous computing network to act as IoT as it requires all the digital devices to be distinctively recognized and also to make them capable of reasoning and interacting with the other devices in the network to accumulate the data which is essential to automate the action taken by the devices. To escalate the extensive development of IoT, we have the list of following pertinent technologies to discuss particularly in this segment.

1) *Radio Frequency IDentification (RFID)*
2) *Wireless Sensor Network (WSN)*
3) *Cloud Computing*
4) *Networking Technologies*
5) *Nano Technologies*
6) *Micro-Electro-Mechanical Systems (MEMS) Technologies*
7) *Optical Technologies*
8) *Cloud Computing*

IV. APPLICATIONS

To develop an extensive assortment of ingenious applications, it is necessary that not only almost all of the commonly used routine real-world applications must communicate with one another, but also these applications should share pragmatic information with one another. And this scenario is there, as these applications are not smart enough to interact with one another. And it is quite certain that in the coming time, to enhance the quality of a human life, such emanating applications, having capabilities which are self-governing in nature, will play a very crucial role. We already may feel the presence of such IoT based applications in the market, although such applications are still in their development stage, which includes a very phenomenal experience of having a self-driving car running in the real-time traffic without any simulation in legitimate meteorological and roadway conditions using the real-time information reciprocity. Despite the fact that the list of imminent IoT applications, which are capable of adding a great amount of comfort to the life of humans, is quite long to be discussed in a section here in this research paper, yet we have a few prominent applications of IoT to discuss as below.

1) Smart Traffic System

Traffic is an inseparable issue of a society and each and every issue related to the same must be addressed in an appropriate manner. A system should have been designed having IoT as the backbone technology, which will use the information exchange between participating objects in the traffic, to mitigate the traffic conditions to a great extent. Rather than applying general image processing approaches, IoT technologies can serve the purpose in a far better manner for an aforesaid smart traffic surveillance system

having instinctive identification of automobiles in the traffic and other many crucial aspects required in such system. It is implicit that with the aid of this smart traffic surveillance system, the jams in the traffic will be reduced and everyone will be perceiving a great experience during their transportation [5]. The other characteristics of this smart traffic surveillance system might include traffic calamities reporting, a reduced amount of environmental contamination, ascertainment of vehicle thievery and many more. Driving and walking tracks may be ameliorated in the smart city arteries having such an aforesaid system by providing alternate routes in the situations emanated due to vicissitudes in the weather, unanticipated traffic jams or natural calamities [7]. Conservation of Energy is possible by making the traffic illumination system adaptable to meteorological conditions and also all and sundry in the smart city may have access to the information showing the availability of parking spaces all over the city.

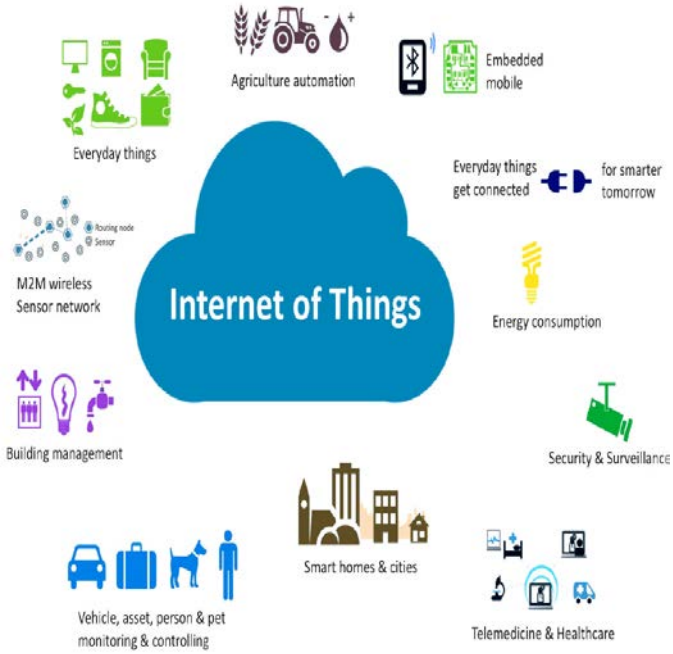

Fig. 2 IoT Applications

2) Smart Environment

The smart environment is all about having state-of-the-art ingenious IoT technologies to be used for the forecasting of natural catastrophes including tremors, deluge, wildfire and so forth [9].

3) Smart Home

In the concept of Smart Home, one can control and operate the home appliances remotely as per the requirements. To descry unforeseen water leakages, overloading etc. and to conserve the resources, there is a requirement of legitimate monitoring of water supply system, utility meters and power resources [13]. Larceny can also be restrained with the help of an appropriate infringement ascertainment system. There is certainly a possibility of having a smart gardening system in the smart home wherein the measurement of the clamminess, precipitation, climate temperature, light and additional horticultural vitals can be taken proficiently and also it is going to provide automated water supply to the plants in the garden as and when required as per the necessity of the plants.

4) Smart Hospitals

Each and every patient in the hospital will be wearing a smart RFID embedded tag, which is a flexible wearable gadget and will be allotted to the patient on their advent into the hospital. The crucial vital signs of the patients, e.g. temperature, blood pressure, heart rate etc., can be observed not only by the doctors but by the nurses as well, disregarding of the location of the patient, within or away from the hospital establishment. A normal ambulance might not be able to reach to the patients in extreme medical contingencies at distant locations, whereas a Drone ambulance (a component of the Smart Hospital Solution) is capable enough to reach over the patient's location through air travel with a contingency kit, which will enable the doctors to not only to receive the tracking of the patient but to provide a medicinal aid till the normal ambulance reaches the patient's location.

5) Smart Cultivation

Smart Cultivation is quite helpful to multi-fold the production of an agronomic land by appropriate observation of Light, Clamminess, Soil Nutrition etc. and by monitoring of temperature for an automated climate control to make the experience of green housing better. To improve the water quality, accurate watering will help and the fertilizers can be saved by accurate fertilization as well.

6) Smart Retailing and Supply-chain Management

IoT with RFID can be proven to be of a great help, as the products with RFID implantation can provide tracking information of the stocks and it can be used to detect and prevent shoplifts. One of the major problems, having items going out-of-stoke, can be resolved by placing the order autonomously as soon as the product quantity in the stores goes to the minimum level. Sales charts and graphical representation for the data in the system can be generated to help the retailers to work upon the effective strategies.

V. Security and Privacy Challenges

The IoT has gained its popularity by making a human life much more comfortable than it was earlier, as with the help of IoT one can locate anyone and can be addressed as well [10]. But until and unless we as the users are not sure enough or not confident enough regarding the privacy and security of our data, the adoptability of IoT will remain constrained. To be adopted globally, there is a need of a robust security infrastructure for IoT. Out of many, some of the IoT security problems are discussed below:

1) Accessing the RFID Tag illegitimately

The RFID tags used in IoT applications can be accessed by the intruders not having enough privileges and the secret information in these RFID tags about the user can be passed

on to the fraternity trying to harm the user and/or application. There is even a possibility of not only alteration of the information in the RFID tags but the same information can be impaired as well. The RFID may also be injected with an RFID virus also, to attack over the complete application technological architecture.

2) Security Infringement in Sensor Nodes

IoT has Wireless Sensor Network (WSN) as the backbone technology for proper and accurate functioning. The WSN is composed of innumerable sensor nodes which are not only transmitting the data present over these nodes, but also allowing the acquisition of data as well. And by having this bi-directional mode of communication, these nodes are making the whole Wireless Sensor Network susceptible to various types of attacks, out of which some are Sybil Attack, Jamming, Flooding and Tempering and discussed as under:

In the case of Sybil attack the sensor node, in the WSN of an IoT application, is affected very much by numerous anonymous identities claimed by the attackers.

The Jamming is all about intervening with the operating frequencies of sensor nodes to impede the entire network.

Flooding falls in the category of Denial of Services attacks, and it is held responsible for causing the problem of memory exhaustion by increasing the traffic.

On the other hand, in the case of Tempering, the assailant can make the existing sensor node to a controllable one by extracting and/or modifying the confidential data present over the sensor node.

3) Misuse of Cloud Computing

Resources can be shared among the congregated servers in a very well-planned network architecture known as cloud Computing. Resource sharing, that too over internet, obviously it is open to a lot many security threats including Data Loss, Malicious Insider, Man in the Middle, Monstrous use etc. discussed below:

The confidential data present in the network can be extracted as well as altered or deleted by the attacker and this threat is Data Loss.

The confidential data can be manipulated by the Malicious Insider by accessing it and this insider has all authorized access to the system.

The communicating messages between two participating entities can be intercepted and/or altered by this man in the middle by hijacking of account.

There is monstrous way to use the cloud computing by injecting a malicious software into the server to get all over control of the server and its connected peripherals.

VI. CONCLUSIONS

It is inevitable that the development in the field of Internet of Things (IoT) is going to increase exponentially with the nonstop growing of the upcoming IoT technologies. By entrenching brilliance into the gadgets around humans, this imminent networking architype is certainly going to put a great positive effect on every aspect of human life including smart health, automated homes and atmosphere monitoring. This research paper talks about basic fundamental aspects IoT with the explanation of a definite architecture needed for the deployment. The discussion further progresses towards the elucidation of IoTs prominent applications which are ultimately going to make human life easier. Although the IoT is considered to be an extensively accepted technology in near future, still it becomes mandatory to deliberate the security and privacy aspects related to the user. That is the reason why the privacy and security issues of IoT necessitates adequate handling efforts.

ACKNOWLEDGMENT

This work was supported by Dr. Ashok Kumar Jetawat, the authors thank to, for his kind guidance in the research and as reviewer to this research paper. The author would also thank the KJIT management for their astonishing support in the research.

REFERENCES

[1] Saranya C. M., Nitha K. P., Analysis of Security methods in Internet of Things. International Journal on Recent and Innovation Trends in Computing and Communication, Volume 3, Issue 4; April 2015.

[2] De-Li Yang, Feng Liu and Yi-Duo Liang, "A Survey of the Internet of Things", in International Conference on E-Business Intelligence (ICEBI), 2010.

[3] M. A. Ezechina, K. K. Okwara, C. A. U. Ugboaja. The Internet of Things (IoT): A Scalable Approach to Connecting Everything. The International Journal of Engineering and Science 4(1) (2015) 09-12.

[4] Patrick Guillemin et al., Internet of Things standardization - Status, Requirements, Initiatives and Organizations. Conference: Internet of Things - Converging Technologies for Smart Environments and Integrated Ecosystems 2013.

[5] L.Xiao, Z.Wang, "Internet of Things: A New Application for Intelligent Traffic Monitoring System," in Journal of Networks, 2011.

[6] Miao Wu, 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), 2010, pp. 484-487.

[7] Farheen Fatima, at el., Internet of things: A Survey on Architecture, Applications, Security, Enabling Technologies, Advantages & Disadvantages. International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 12, December 2015.

[8] L.G. Guo, Y.R. Huang, J. Cai, L.G. QU, "Investigation of Architecture, Key Technology and Application Strategy for the Internet of Things," in Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011, Volume: 2, pp. 1196-1199.

[9] P. Susmitha, G. Sowmyabala. Design and Implementation of Weather Monitoring and Controlling System. International Journal of Computer Applications Volume 97, No. 3, July 2014.

[10] S. Misra et al., Security Challenges and Approaches in Internet of Things. Springer Briefs in Electrical and Computer Engineering, 2016.

[13] D. Bhattacharjee and R. Bera. Development of smart detachable wireless sensing system for environmental monitoring. International journal on smart sensing and intelligent systems Vol.. 7, No. 3, September 2014.

[14] P. Saichaitanya1, N. Karthik, D. Surender. Recent trends in IoT. International Journal of Electrical and Electronics Engineering, Vol. 8, Issue 2, December 2016.

[15] Amrita Sajja, D. K. Kharde, Chandana Pandey. A Survey on efficient way to Live: Smart Home - It's an Internet of Things. ISAR International Journal of Electronics and Communication Ethics, Volume 1. Issue 1, 2016.

[16] Debasis Bandyopadhyay, Jaydip Sen, "Internet of Things - Applications and Challenges in Technology and Standardization" in Wireless Personal Communications, Volume 58, Issue 1, pp. 49-69.