Internet of things: Vision, applications and challenges

Bharti Bansal[(1)] , Shweta Rana[(2)]
Assistant Professor & Computer Science & Amity University Haryana
Gurugram , Haryana , India

ABSTRACT
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).
It aims to unify everything in our world under a common infrastructure, giving us not only control of things around us, but also keeping us informed of the state of the things. 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. However, this manuscript will give good comprehension for the new researchers, who want to do research in this field of Internet of Things and facilitate knowledge accumulation in efficiently.

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 escalating as a global computing network where everyone and everything will be connected to the Internet. IoT is continually evolving and is a hot research topic where opportunities are inestimable. 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 . IoT is an approach of converging data obtained from different kinds of things to any virtual platform on existing Internet infrastructure. The concept of IoT evolves in 1982 when a modified coke machine was connected to the Internet which was able to report about the availability of drinks contained and its temperature. Later, in 1991, a contemporary vision of IoT was first given by Mark Weiser . However in 1999, Bill Joy gave a clue about the communication among devices in his taxonomy of internet [6]. In the very same year, Kevin Ashton proposed the term ”Internet of Things” for interconnected devices. The basic idea of IoT is to allow autonomous exchange of useful information between uniquely identifiable real world devices around us. These devices are fueled by the leading technologies like Radio-Frequency IDentification (RFID) and Wireless Sensor Networks (WSNs) and further processed for decision making, on the basis of which an automated action is performed.

2. VISION

In 2005, ITU reported about a pervasive networking era in which all the networks are interconnected. Imagine you are searching for watch you lost somewhere in your house through internet. So this is the main vision of IoT, an environment where things are able to respond and their data can be processed to perform desired tasks through machine learning. A practical implementation of IoT is demonstrated by a 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.

3. ARCHITECTURE

According to CISCO more than 25 Billion things are expected to be connected by 2020.The existing architecture of Internet with TCP/IP protocols cannot handle a network as big as IoT. So a need for a new open architecture arise that could address various security and Quality of Service (QoS) issues as well as support the existing network applications using open protocols. IoT is not likely to be adopted without a proper privacy assurance. 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. A six-layered architecture was proposed based on the network hierarchical structure as shown in the Fig. 1.

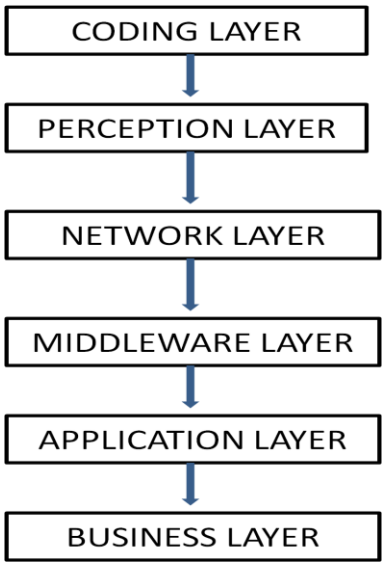

Fig. 1. Six-Layered Architecture of IoT

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: This layer receives the useful information in the form of digital signals from the Perception Layer and transmit it to the processing systems, present in the Middleware Layer through the transmission mediums like WiFi, Bluetooth, WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc .

Middlware Layer: It processes the information received from the sensor devices which includes the technologies like Cloud computing, Ubiquitous computing ensuring 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.

Application Layer This layer realizes the applications of IoT for all kinds of industry, based on the processed data. 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: It 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.

4. TECHNOLOGIES

The development of a omnipresent 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 that 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.

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. 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 Depending on the type of application, RFID frequencies are divided into four different frequencies ranges, (1) Low frequency (135 KHz or less) (2) High Frequency (13.56MHz) (3) Ultra-High Frequency (862MHz 928MHz) (4) Microwave Frequency (2.4G , 5.80). Bar Code is also an identification technology which has almost the same function as an RFID but RFID is more effective than a Bar Code due to a number of its benefits. RFID 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 unless its

reader is placed in front of it. Moreover, an RFID can work as an actuator to trigger different events and it has even modification abilities which Bar codes clearly don't have.

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 technolog However an additional unit for saving the data, named as Memory Unit which could also be a part of the sensing node has been proposed.

Cloud Computing
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 not only converges the servers but also processes on an increased processing power and analyzes the useful information obtained from the sensors and even provide good storage capacity. But this is just a beginning of unleashing the true potential 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 researches are being carried out since IoT will be totally dependent on the Cloud Computing.

Networking Technologies
These technologies 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.

\
Nano Technologies
This technology is useful for 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.

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 advantages like size reduction of sensors and actuators, integrated ubiquitous computing devices and higher range of frequencies etc.

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 objects interconnected on the concept of IoT. Similarly Bi-Directional (BiDi) technology gives a 40G ethernet for a big data from multifarious devices of IoT.

5. APPLICATIONS

Most of the daily life applications that we normally see are already smart but they are unable to communicate with each other and to make them communicating and sharing useful information will create a wide range of innovative applications. These emerging applications with some autonomous capabilities would certainly improve the quality of our lives.There are a number of possible future applications that can be of great advantage are :

Smart Traffic System: Traffic is an important part of a society 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 system, 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 traffic lighting system will be weather adaptive to save energy. Availability of parking spaces throughout the city will be accessible by everyone.

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

Smart Home: IoT will also provide DIY solutions for Home Automation with which we will be able to remotely control our appliances as per our needs. Proper monitoring of utility meters, energy and water supply will help saving resources and detecting unexpected overloading, water leakage etc. There will be proper encroachment detection system which will prevent burglaries. 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.

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 Ambulances 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.

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

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 shoplifting. 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 effective 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:

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. Some of the real life threats of RFID which includes RFID Virus, Side Channel Attack with a cell-phone and SpeedPass Hack.

Sensor-Nodes Security Breach WSNs are vulnerable to several types of attacks because sensor nodes are the part of a bi-directional sensor network, which means other than the transmission of data, acquisition of data is also possible. Some of the possible 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.

Cloud Computing Abuse Cloud Computing is a big network of converged servers which allow sharing of resources between each other. These shared resources 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 Monstrous 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 manipulating.
(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 mushrooming of the emerging IoT technologies, the concept of Internet of Things will soon be unavoidably 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. 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 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

[6] Jason Pontin, "Bill Joy's Six Webs," MIT Technology Review, 29 September 2005

[7] Kevin Ashton, "That 'Internet of Things' Thing", RFID Journal, 22 June 2009

[8] H.D. Ma, "Internet of things: Objectives and scientific challenge," in Journal of Computer Science and Technology, 2011, pp. 919-924

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

[10] 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

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

[12] "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

[13] 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

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

[15] "The Internet of Things," ITU Report, Nov 2005

[16] Wang Chen, "AN IBE BASED SECURITY SCHEME OF INTERNET OF THINGS," in Cloud Computing and Intelligent Systems (CCIS), 2012, pp. 1046, 1049

[17] Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, "Security in the Internet of Things: A Review," in Computer Science and Electronics Engineering (ICCSEE), 2012, pp. 648-651

[18] 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

[19] 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 Intelligence and Design, pp. 294-297, 2012

[20] 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

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

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

[23] L.Atzori, A.Iera, G. Morabito, "The Internet of Things: A survey," in Computer Networks - Science Direct

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

[25] 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

[26] Sohraby, K., Minoli, D., Znati, T. "Wireless sensor networks: technology, protocols, and applications", John Wiley and Sons, 2007 ISBN 978-0-471-74300-2, pp. 15-18

[27] E. M. Tapia, S. S. Intille, and K. Larson, "Portable wireless sensors for object usage sensing in the home: Challenges and practicalities," in Proceedings of the European Ambient Intelligence Conference. vol. LNCS 4794 Berlin Heidelberg: Springer-Verlag 2007

[28] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks"

[29] 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, 2011, pp. 147-159
[30] B.B.P. Rao, P.Saluia, N.Sharma, A.Mittal, S.V.Sharma, "Cloud computing for Internet of Things & sensing based applications," in Sensing Technology (ICST), 2012 Sixth International Conference, IEEE
[31] X.Xiaohui, "Study on Security Problems and Key Technologies of The Internet of Things," Computational and Information Sciences (ICCIS), 2013, pp. 407-410
[32] O.Vermesan, P.Friess, "Internet of Things ? From Research and Innovation to Market Deployment," River Publishers, pp. 74-75
[33] I.Akyildiz and J.Jornet, "THE INTERNET OF NANOTHINGS," IEEE Wireless Communications, Volume: 17 Issue: 6, 2010, pp. 58-63
[34] V.M. Lubecke, Jung-Chih Chiao, "MEMS technologies for enabling high frequency communications circuits," in Telecommunications in Modern Satellite, Cable and Broadcasting Services, 1999, Volume: 2, pp. 382-389