Internet of Things (IoT) – A Survey

ANGEL HEPZIBAH R
Assistant Professor,Department of Information Technology,
Jayaraj Annapackiam CSI College of Engineering, Nazareth.
Email: rangelhepzibah@gmail.com
Dr.E.MARIAPPAN
Professor,Department of Computer Science and Engineering,
St.Mother Theresa Engineering College,Tuticorin District,Tamilnadu.
Email: mapcse.e@gmail.com

ABSTRACT

Now a days we are living in an era of Information Technology where each and every person has to become IT incumbent either intentionally or unintentionally. Technology plays a vital role in our day to day life since last few decades and somehow we all are depending on it in order to obtain maximum benefit and comfort. This new era equipped with latest advents of technology, enlightening world in the form of Internet of Things (IoT). Internet of things is such a specified and dignified domain which leads us to the real world scenarios where each object can perform some task while communicating with some other objects. The world with full of devices, sensors and other objects which will communicate and make human life far better and easier than ever. This paper provides an overview of current research work on IoT in terms of architecture, a technology used and applications. It also highlights all the issues related to technologies used for IoT, after the literature review of research work. The main purpose of this survey is to provide all the latest technologies, their corresponding trends and details in the field of IoT in systematic manner. It will be helpful for further research.

Keywords - **Internet of Things.**

1 INTRODUCTION

Internet of Things can be defined as the collection of two terms: one is Internet, which is defined as networks of networks which can connect billions of users with some standard internet protocols[2]. Internet connect several different sectors and department while using different technologies. Several devices like mobile, personal systems and business organizations are connected to Internet. The second term is Thing, this term is basically mean to these devices or objects which turn into intelligent objects[17]. Moreover this it is also a part of all objects of this real world. If we want to define IOT then we can not define it precisely and concisely but Vermesan et al. defined the Internet of Things as simply an interaction between the physical and digital worlds. The digital world interacts with the physical world using a plethora of sensors and actuators [8].

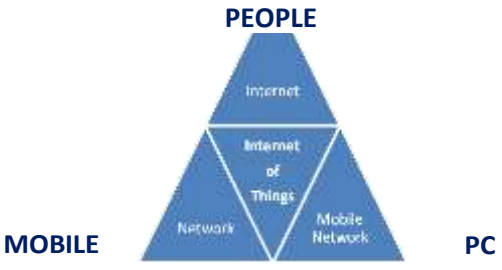

Fig. 1 – Basics of Internet of Things

IoT can also be defined as "An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment"[22].

2 HISTORY OF IOT

The IoT domain leads to world of technology and communication to a new era where objects can communicate, compute and transform the information as per the requirements. This scenario of communication has already been started but didn't get recognition. The term Internet of Things was coined by Kevin Auston, the Executive Director of Auto-ID Labs in MIT in 1999. The concept of IoT first became very popular through the Auto-ID centre in 2003 and in related market analytics and its publications [1]. When the concept of such communication came into existence, different companies focused on it and tried to recognize it's significance and began to identify its role and the correlated future aspects, then these companies started investing in the domain of IOT in different periods but at regular intervals of time[9].

Year	Industrial Participation & Involvement
2000	LG announced its first Internet of refrigerator plans
2003	RFID is deployed in US Dept of Defence
2005	UN's International Telecommunications Union (ITU) published its first report on the Internet of Things
2008	Recognition by the EU and the First European IoT conference is held. A group of companies launched the IPSO Alliance to promote the use of IP in networks of "Smart Objects" and to enable the Internet of Things. The FCC voted 5-0 to approve opening the use of the 'white space' spectrum
2009	The IoT was born according to Cisco's Business Solutions Group
2010	Chinese Premier Wen Jiabao calls the IoT a key industry for China and has plans to make major investments in Internet of Things
2011	IPv6 public launch-The new protocol allows for 340, 282, 366, 920, 938, 463, 463, 374, 607, 431,768,211, 456 (2^{128}) addresses

Table – 1 History of Internet of Things

3 ARCHITECTURE

Implementation of IoT concept is basically depends on its architecture. In the initial phase of research the **3 layer architecture** was introduced [8], which have three layers the perception, network and application layers.

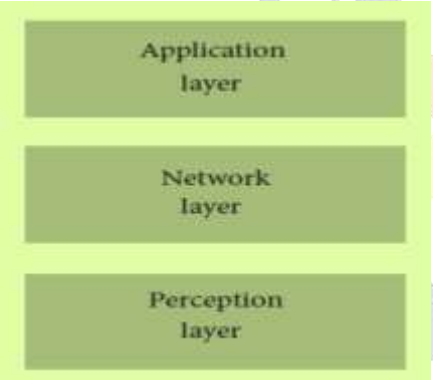

Fig. 2 - 3 Layer Architecture

1. Perception Layer – Perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment [1].

2. Network Layer - Network layer is the middle one; it establishes an interface link between application layer and perceptual layer. It is responsible for the initial processing of data, broadcasting of data and connecting devices [8].

3. Application Layer - Application layer is the implementation of IoT. The working of sensors and actuators is achieved by application layer. We can understand it as software which works on and for the sensors other virtually intelligent objects.

This three layer architecture of Internet of Things is not a sufficient for the today's technology. So a new architecture was designed to define the entire concept of it's working and development of IoT devices. The new architecture involves 5 layers and is known as 5 Layer architecture [29]. New architecture has perception, transport, processing, application and business layers:

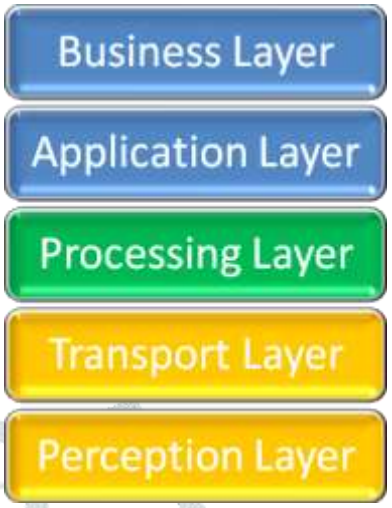

Fig. 3 - 5 Layer Architecture

1. Perception layer works in a similar manner as previously described in the 3 layer architecture. It is used to take information from the sensors and implement it.

2. Transport layer takes the data from the perception layer and pass this data to the next layer which is processing layer and vice versa. This will done with the help of networks like LAN, wireless technology, 3G, 4G, LTE, RFID etc[8].

3. Processing layer which is third layer has to perform the major task because it will process all the information gathered by the perception layer. There is a huge amount of data which will be stored with the help of some techniques like cloud computing or any DBMS. Then it will analyse how to fetch data whenever required in order to complete the desired task[1].

4. Application layer is next layer which implements the working of IoT. For this an application is required with the corresponding device in order to complete the desired task.

5. Business layer is the last layer of this architecture which manages the working of entire system along with many other features, one of them is privacy[1].

Both the architectures are defining the working of IoT system of different types but they all are following the same sort of working in order to achieve its goal. Another architecture proposed by Ning and Wang [30] is inspired by the layers of processing in the human brain. It is inspired by the intelligence and ability of human beings to think, feel, remember, make decisions, and react to the physicalenvironment.

4 TECHNOLOGIES

There are various technologies which are used to define IOT, but the four main technologies are as follows[9]:

1. Radio Frequency Identification (RFID)
2. Near Field Communication (NFC)
3. Low Power WiFi.
4. Bluetooth Low Energy

Radio Frequency Identification (RFID)

RFID is a system in which there is a reader to read many tags[4]. It uses the technology of radio waves to send the information of an object in the form of serial number which is attached to the tag. It uses the electromagnetic fields to transfer the data on the tags so that it can automatically identify and track the objects, corresponding to a particular tag[1]. RFID is an identification technology in which an RFID tag (a small chip with an antenna) carries data, which is read by a RFID reader. The tag transmits the data stored in it via radio waves. As we already mention that RFID technology is based on reader and tags, so in the initial phase of research RFID defines in three configurations:-

- Active RFID
- Passive RFID
- Active Reader Active Tag

Active RFID - (Passive Reader Active Tag), the reader receives the signal or information from the device which runs on battery and this battery is operated by a device called active tag. This information exchange will take place in limited range of the active tags and the passive readers which is from 1-2000 feet depending upon the architecture[14].

Passive RFID - The second one is Passive RFID (Active Reader Passive Tag), most commonly used, such tag does not have any battery or onboard power supplies, so it requires energy to send the data and thus harvests the energy from the RFID reader.

Active Reader Active Tag - The last one both the reader and tags are active so it is an Active Reader Active Tag. Although both the reader and the tags are active, but tags will start sending information only when it is awoken by the reader or when it comes in the proximity of the reader[19]. So by this we can say that the main components of this technology are tag, reader, power supply, antenna, access controller, software and server.

Application - RFID has a very limited use only for identification and tracking. As we know that it works on frequency and within a limited range. So it can work for such applications like smart grocery, smart cabinet, smart fridge, smart appliances, smart currency etc[14]. In these scenarios there is a tag on product and a reader to scan the tag. In a grocery shop we put tags on the products and when the product passes through that reader, the reader will catch it. In this way it can be tracked that which Product is moving out of the shop and what inventory is left for that corresponding product. In the same way if a fridge can sense what is putting in it and what is taking out from it, it can also be done by RFID. One another very useful and common application of this technology is on airport where the baggages are tagged and read at another place.

Issues - There are several issues with RFID. It works on specific range of frequencies; if these frequencies differ at different places then it will create a problem in reading a tag at different locations. It is also difficult to read more than one tag simultaneously [15]. There are methods to overcome this problem but very costly. Tags have to be implemented on the product and all the tags are different and unique, which includes some cost. The inclusion of cost is not comfortable all the time when comparing and concerning with the cost of product [4].

Near Field Communication (NFC)

Near Field Communication is somehow little bit similar to RFID, it combines a RFID reader in a mobile phone, which makes it better, reliable and efficient for the users. Near Field Communication is a short-range wireless technology with the frequency of 13.56 MHz, typically work for very small distance up to 4 cm[3]. Allows intuitive initialization of wireless networks and NFC is complementary to Bluetooth and 802.11 with their long distance capabilities at a distance circa up to 10 cm. It is first developed by Philips and Sony companies. Data exchange was approximately 424 kbps. Power consumption during data reading in NFC is under 15ma[2]. There are two modes in NFC technology:

- Active
- Passive

Active Mode - In active mode both the devices are active and communicate with each other by sending the signals.

Passive Mode - In passive mode one of the device sends the signal rather other just receiving it[28].

NFC doesn't need pairing, it cannot work from a long distance and in this way this technology is secure and use for mobile payments.

Application - NFC works in a very short range so the devices must be kept nearby. It has several applications, the most important one is **Payment App**. Today, we have several applications (apps) by which one can pay without using a card, in this scenario the device works as a virtual card and the transaction will take place. One can exchange their business card with the help of their devices. They just touch their devices and their business cards will be exchanged. If a information is required than use the device with the smart poster and get all the information with a single touch[21]. It can also work while travelling; a person can book a travel ticket or a room in a hotel. While booking keys are given to the person, when person touch the device on the appropriate devices, the work is done and the person will move in.

Issues - These devices will work on a very small range, so this is one of the major issues. Two devices of two different manufacturers can create some compatibility issue in their

communication. Due to this reason a monopoly may exist in market[3].

Low Power WiFi

The WiFi alliance has recently developed "WiFi HaLow," which is based on the IEEE 802.11ah standard. It consumes lower power than a traditional WiFi device and also has a longer range.This is why this protocol is suitable for Internet of Things applications. The range of WiFiHaLow is nearly twice that of traditional WiFi.

Like other WiFi devices, devices supporting WiFi HaLow also support IP connectivity, which is important for IoT applications. Let us look at the specifications of the IEEE 802.11ah standard [31, 32]. This standard was developed to deal with wireless sensor network scenarios, where devices are energy constrained and require relatively long range communication. IEEE 802.11ah operates in the sub-gigahertz band (900MHz).

Issues - Because of the relatively lower frequency, the range is longer since higher frequency waves suffer from higher attenuation. We can extend the range (currently 1 km) by lowering the frequency further; however, the data rate will also be lower and thus the tradeoff is not justified.

Bluetooth Low Energy

Bluetooth Low Energy, also known as "Bluetooth Smart," was developed by the Bluetooth Journal of Electrical and Computer Engineering 13 Special Interest Group. It has a relatively shorter range and consumes lower energy as compared to competing protocols. The BLE protocol stack is similar to the stack used in classic Bluetooth technology. It has two parts: controller and host. The physical and link layer are implemented in the controller. The controller is typically a SOC (System on Chip) with a radio. The functionalities of upper layers are included in the host [62]. BLE is not compatible with classic Bluetooth. Let us look at the differences between classic Bluetooth and BLE [63, 64]. It supports quick transfer of small packets of data (packet size is small) with a data rate of 1Mbps.. There are two types of devices in BLE:

- Master
- Slave

Master - The master acts as a central device that can connect to various slaves. Let us consider an IoT scenario where a phone or PC serve as the master and mobile devices such as a thermostat, fitness tracker, smart watch, or any monitoring device act as slaves.

Slaves - In such cases, slaves must be very power efficient. Therefore, to save energy, slaves are by default in sleep mode and wake up periodically to receive packets from the master.

Issues - BLE does not support data streaming.

5. COMMUNICATION

As the Internet of Things is growing very rapidly, there are a large number of heterogeneous smart devices connecting to the Internet. IoT devices are battery powered, with minimal compute and storage resources.

1. Machine to Machine Communication (MtoM)
2. Vehicle to Vehicle Communication (VtoV)

Machine to Machine Communication (M2M)

Machine-to-Machine (M2M) refers to the communications between computers, embedded processors, smart sensors, actuators and mobile devices (DYE, 2008). The use of M2M communication is increasing in the scenario at a fast pace. For instance, researchers predicted that, by 2014, there will be 1.5 billion wirelessly connected devices excluding mobile phones[5]. Now a days, there are approx 2 billion wirelessly connected devices which can gather information from the sensors, analyse this data and send the information to other devices to perform some task. Machine receives the information and perform the operation with the help of actuators, sensors, embedded processors and application software[12].

Application - In industrial work, a machine can sense the work efficiency of the machine and work accordingly for maximum output. Smart homes where objects can communicate with each other like when there is no one in the home and unfortunately the owner forgot to lock the home then smart home will sense that there is no motion in the home and it will lock the home and send the unlock key to the owner[13]. The same application is smart water supply, if there is a leakage then the machine sensor will sense this and send the information to the server. It will help to stop the wastage of water[24].

Issues - The key issues in M2M are -
In M2M technology, devices or groups can use different naming process. Devices can use different names for their working or same name can be assigned different devices, objects or groups. They can also use some temporary id, names and URIs for their communication. IP addresses are also used to make communication among the devices or connected groups. These addresses may be of individual device or multicast address for group of connected devicesor some other address schemes to make connectivity and communication[26].

In this way we can say that M2M devices are unnamed and have very less security. So it has several securityissues and threats like hacking, unauthorized access, tampering etc. Some moving devices have problems of monitoring and linking with their base stations, geographical change may cause some effects on the network and it may get disconnected for some time or fora long time. It is a major security issue and some sort of attack can be encountered. These devices also require timely updates so that it will become aware from security threats. M2M devices are moving or stationary, so there are lots of devices which need to be operate and update butsome of them are wireless and some are not, so it has not been easy to access each and every device manually. This will lead more vulnerabilities to these devices. [5]

Vehicle to Vehicle Communication (V2V)

In this technology the objects are vehicles, which can communicate with another vehicle or the sensors around them. The main aspect of concern here is, there is no proper method to define the protocols because the object is moving and communicating with another moving

object or with the sensors on the roadside[6]. So we are not able to define any routing protocol. This communication can work for a long distance and make an efficient communication among objects. This technology was designed primarily with the aims of traffic control, safety and accident avoidance.

Application - Smart cars are the application of M2M, a car which is driverless or a car which have sensors and sense the speed of the nearby car who is getting slow uncertainly. So the car can also be slow down to avoid accident[10].

Issues – The key issue in V2V are -
The main concern of V2V is the loss of connectivity when any other object comes in between the communicating devices. If they are not in a proper distance and proper line of sight then they will not be able to continue in connectedstate[10].

Moving vehicles will also create several difficulties during establishment of communication. There may be change in topology when there is a change in the network. Sometimes device will not have the network or have little range of network, so the data will not be send or receive properly and device will not work accurately. This will lead to great problem.[6]

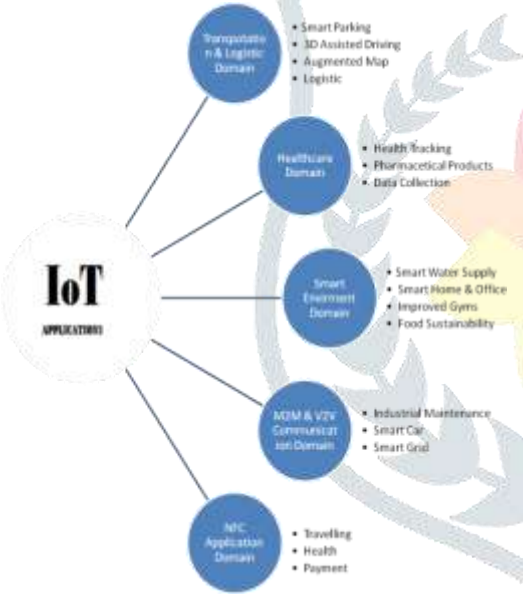

Fig. 4 – Applications of IoT

5 CONCLUSION

Internet of Things depends on Internet, sensors technology which makes the communication possible among devices by implementing different protocols.
After doing the literature survey some major issues are observed, like the interrupted connectivity among devices effecting the communication. Also there is compatibility issue in devices. Security of devices during communication process and security of communication channel or link is also a major issue. Lots of work is to be done for the betterment and progress of this field; still there is more work to do, more standardization of technology, protocols and hardware are required to make completely reliable and secure domain of Internet of Thing. Some global guidelines should be used for this purpose. The future is totally depends on Internet of Thing, so lot of thing to do at implementation level. In order to resolve security issues in IoT domain we propose to implement the concept of Block Chain in IoT. We will have deep discussion on principals and implementation of Block Chain in our further works.

ACKNOWLEDGEMENTS

The authors are thankful for all the experts who contribute to prepare this research paper directly or indirectly.

REFERENCES

[1] Pallavi Sethi and Smruti R. Sarangi, " Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering Volume 2017, Article ID 9324035, 25 pages

[2] Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, "Internet of Things (IoT): A Literature Review," *Journal of Computer and Communications, 2015, 3, 164-173*

[3] Gerald, Josef,Christian and Josef Scharinger, "NFC Devices: Security and Privacy", *ARES 08 proceedings of the 2008 Third International Conference on Availability, Reliability and Security, IEEE Computing Society, Washington, DC, USA, 2008*

[4] Want, R. (2006) An Introduction to RFID Technology. *IEEE Pervasive Computing, 5, 25-33*.

[5] H. C. Chen, M. A. A. Faruque and P. H. Chou, "Security and privacy challenges in IoT-based machine-to-machine collaborative scenarios," *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*, Pittsburgh, PA, 2016, pp. 1-2.

[6] Y.Usha Devi, Dr. M.S.S.Rukmini, "IoT in Connected Vehicles: Challenges andIssues- A Review," *International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016.*

[7] A. Juels, "RFID security and privacy: a research survey," in *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394, Feb. 2006.

[8] Miao W., Ting L., Fei L., ling S., Hui D., 2010. Research on the architecture of Internet of things. *IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE), Sichuan province, China, Pages: 484-487*.

[9] Luigi A., Antonio I., Giacomo M. 2010.The Internet of Things: A survey. *Science Direct journal of Computer Networks, Volume 54, Pages: 2787–2805*.

[10] G. Burnham, J. Seo G. Bekey, A. Identification of Human Driver Models in Car Following. *IEEE Transactions on Automatic Control 19, 6, 1974, pp. 911–915.*

[11] J. Deng, R. Han, and S. Mishra, Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks, *Proc. of ACM/IEEE IPSN, 2006. pp. 292-300.*

[12] J. Stankovic, A Vision of a Smart City in the Future, Smart Cities, *Vol. 1, Issue 10, Oct. 2013*.

[13] Anvari-Moghaddam, A., Monsef, H. and Rahimi-Kian, A. (2015) Optima Smart Home Energy Management Consi- dering Energy Saving and a Comfortable Lifestyle. *IEEE Transactions on Smart Grid, 6, 324-332. http://dx.doi.org/10.1109/TSG.2014.2349352*.

[14] E. Welbourne, l. Battle, g. Cole, k. Gould, k. Rector, s. Raymer, et al., building the internet of things using rfid the rfid ecosystem experience, *ieee internet comput. 13 (2009) 48–55*.

[15] A. Juels, rfid security and privacy: a research survey,

ieee j sel areacomm. 24 (2006) 381–394.

[16] Ruchi Parashar, Abid Khan, Neha, "A SURVEY: THE INTERNET OF THINGS," *International Journal of Technical Research and Applications e-ISSN: 2320-8163, Volume 4, Issue 3 (May-June, 2016).*

[17] Shashank Agrawal, Dario Vieira, "A survey on Internet of Things," *Abakós, Belo Horizonte,v. 1, n. 2, p. 78 – 95, maio 2013 – ISSN:2316–9451*.

[18] Yinghui H., Guanyu L., 2010. Descriptive Models for Internet of Things. *IEEE International Conference on Intelligent Control and Information Processing, Dalian, China, Pages: 483- 486.*

[19] Tongzhu Z., Xueping W., Jiangwei C., Xianghai L., Pengfei C., 2010 .Automotive recycling information management based on the internet of things and RFID technology. *IEEE International Conference on Advanced Management Science (ICAMS), Changchun, China, page(s):620 – 622.*

[20] Muriel D., Juan F., 2010. Expanding the learning environment: combining physicality and virtuality The Internet of Things for eLearning. *IEEE International Conference on Advanced Learning Technologies (ICALT), Sousse, Tunisia, Pages: 730-731.*

[21] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, *Springer, 2010. ISBN: 978-1-4419-1673-0.*

[22] Ms.Neha Kamdar, Vinita Sharma, Sudhanshu Nayak, "A Survey paper on RFID Technology, its Applications and Classification of Security/Privacy Attacks and Solutions," *IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol.6, No4, July-August 2016*

[23] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials, vol. 17, pp. 2347-2376, 2015*.

[24] Prajakta Pande and Anand R. Padwalkar, "Internet of Things –A Future of Internet: A Survey", *International Journal of Advance Research in Computer Science and Management Studies Research Article / Paper / Case Study Volume 2 , Issue 2 , February 2014 pg . 354 - 361*

[25] Salonie Vyas, Umang Chaudhari, V. Chinmay Nandini, Bhushan Thakare, "State of the Art Literature Survey 2015 on RFID," *International Journal of Computer Applications (0975 – 8887) Volume 131 – No.8, December2015*

[26] White Paper on "Machine-to-Machine Communication (M2M)"

[27] S. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE Access, vol. 3, pp. 678-708, 2015.*

[28] Anusha Rahul, Gokul Krishnan G, Unni Krishnan H and Sethuraman Rao, "NEAR FIELD COMMUNICATION (NFC) TECHNOLOGY: A SURVEY," *International Journal on Cybernetics & Informatics (IJCI) Vol. 4, No. 2, April 2015*

[29] Handong Zhang and Lin Zhu, "Internet of Things: Key technology, architecture and challenging problems," *2011 IEEE International Conference on Computer Science and Automation Engineering*, Shanghai, 2011, pp. 507-512.

[30] H. Ning and Z. Wang, "Future internet of things architecture:like mankind neural systemor social organization framework?"*IEEE Communications Letters*, vol. 15, no. 4, pp. 461–463, 2011.

[31] B. Shanmuga Sundaram, "A quantitative analysis of 802.11ah wireless standard," *International Journal of Latest Research inEngineering and Technology*, vol. 2, 2016.

[32] W. Sun, M. Choi, and S. Choi, "Ieee 802.11 ah: a long range 802.11 wlan at sub 1 ghz," *Journal of ICT Standardization*, vol. 1, no. 1,pp. 83–108, 2013

AUTHORS BIOGRAPHY

Mrs. Angel Hepzibah R is presently working as Assistant Professor in Department of Information Technology at Jayaraj Annapackiam CSI College of Engineering and having 15 years experience of teaching UG students. She obtained M.E. degree from Anna University, Trichy and B.E. degree from Anna University, Chennai. She works in the field of Wireless Sensor Networks, Cloud Computing and Internet of Things.