Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 41 (2016) 99-104 EISSN 2392-2192

A Study on Technologies User for implementation of Internet of Things

K. S. Sindhu*, M. Aasha, S. Sivakumari

Department of CSE, Faculty of Engineering, Avinashilingam University, India

*Email address: sindhu22.ks@gmail.com

ABSTRACT

Internet of Things plays a major role in various areas. This paper presents a study about IOT in a wider context and describes about the various technologies involved in implementation of IOT and the application areas namely smart grid, smart home, smart security, industrial areas etc.

***Keywords*:** Internet of Things, RFID, M2M, NFC, V2V

1. INTRODUCTION

IOT is a platform in which objects and persons are given a distinctive identity and then they are used to interchange the data over a network. IOT was first named by Kevin Ashton while working at Auto-IDlabs. Over a last few decades the usage of internet came into existence .Now a day's about two billion people use internet for various purposes, and as the usage increases it gives rise to an another big area called IOT (Internet Of Things).With the help of this technology the objects around us are connected and then communication is made with the help of internet. IOT allows the objects to be sensed and controled remotely over a network. IOT creates a world where all objects, are called smart objects, and these smart objects are connected to the internet and then communicated. The main goal of IOT is used to create a better world for human beings. Internet of Things continues to be the latest, most hyped concept in the IT world and it is considered as a global network which allows the communication

(Received 01 February 2016; Accepted 10 February 2016; Date of Publication 11 February 2016)

between human-to-human, human-to-things and things-to-things. In this paper section 2 describes about the Architecture of IOT, section 3 describes about the technologies involved, section 4 describes about the future applications, finally section 5 concludes this paper.

2. ARCHITECTURE OF IOT

The structure of IOT is divided into five layers as mentioned in Fig. 1 they are,

- Device layer
- Transmission layer
- Middleware Layer
- Application Layer
- Business Layer

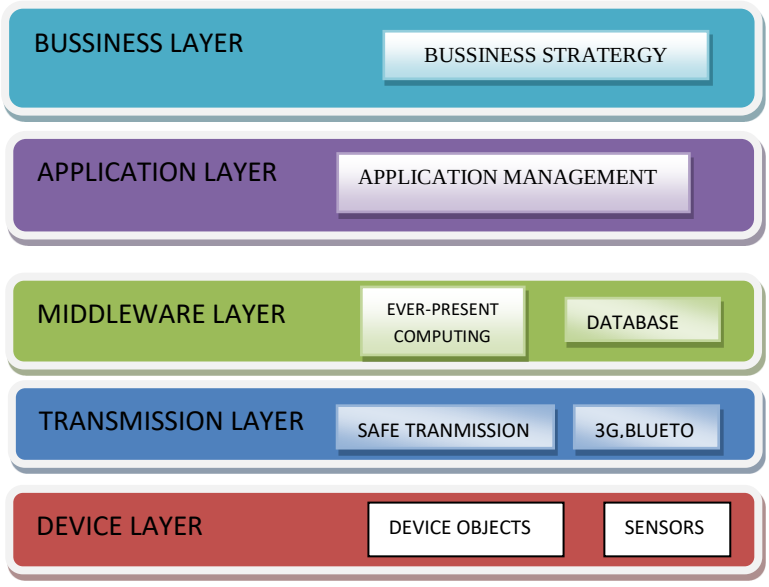

Fig. 1. Architecture overview

2. 1. Device Layer

It is also known as perception layer, it deals with identification and objects specific information by the sensor devices. Based on sensor type, the information can be about place, hotness, orientation, action trembling acceleration, moisture, chemical changes etc. The composed information is passed to transmission layer for its safe transmission.

2. 2. Transmission layer

The transmission layer can also be called ”Network Layer”. This layer firmly passes the information from sensor devices to the information dispensation system. The broadcasting standard can be wired or wireless and technology such as 3G, Bluetooth, infrared, ZigBee, etc. Thus, the transmission layer transfers the information from device layer to Middleware layer.

2. 3. Middleware Layer

Middleware layer is liable for the provision management and it maintains a relationship with the database. It receives the information from transmission layer and saved at the database.

2. 4. Application Layer

Application layer provides overall management of the function based on the substance information processed in the Middleware layer.

2. 5. Business Layer

Business Layer is accountable for overall management of IOT system which includes the applications and services [10].

3. TECHNOLOGIES INVOLVED

There are numerous technologies available to implement the concept of IOT. This paper, discusses the following technologies

- Radio Frequency Identification (RFID)
- Machine-to-Machine Communication (M2M)
- **Near Field Communication (NFC)**
- Vehicle-to-vehicle (V2V) communication

3. 1. Radio Frequency Identification (RFID)

Radio frequency identification (RFID) is described as a system which transfers the identity of an object or person wirelessly, with the help of radio waves. RFID technology gives a rise to a numerous stern issues including safety measures and privacy concerns [1]. Radio Frequency Identification is used with biometric technology for security purposes.

RFID provides identification from a distance, which is not similar to bar-code technology. RFID is used for automatic capturing of data or with the help of radio frequency. Identification is done without a line of sight. RFID systems can differentiate different tags which are present in the same general area without any human aid [2].

3. 1. 1. RFID principles

Number of RFID's is available at the highest level of Radio Frequency Identification devices are classified into two types they are,

1. Active RFID (it requires an power infrastructure)
2. Passive RFID (it does not require any batteries) [2]

3. 2. Machine-to-Machine Communication (M2M)

The major objective of M2M communications is to assist the sharing of information between electronic systems originally."M2M architecture" can exactly consign to any number of machines communicating, it is usually accepted that M2M principles concern mainly well to networks where a huge number of machines are used, flat up to the 1.5 billion wireless devices

[3]. M2M communication is branded by linking a huge number of low power intelligent objects partaking the data and making concerted decisions without person intervention [4]. Five primary M2M concepts that have been reported are,

1. The hold up for large-scale exploitation of devices,
2. Cross-platform networking,
3. Autonomous monitoring and control,
4. Visualization of the structure, and
5. Safety measures [3]

3. 3. Near Field Communication (NFC)

The most important feature of NFC is that it is a wireless communication interface with a functioning space restricted to about 10 cm. This interface can work in several modes. The modes are notable whether a device creates its own RF field or it retrieves power from the RF field generated by another device. If device generates its own field it is called an active device or if a device does not produce power from RF field is called a passive device.

Active devices have power supply, where passive devices don't. NFC is based on the concept of message and reply [5]. It is a short-range half-duplex communication protocol which provides simple and safe communication between various devices. The two parts of NFC communication is branded as initiator and target devices. The Initiator initiates and guides the information exchange between the parties. The target responds to the requests made by initiator [6].

3. 4. Vehicle-to-vehicle (V2V) communication

In V2V Communication lots research has to be done. In this, vehicles act as a node in a set of connections and commune with each other with the help of sensors connected in an ad-hoc network. The structure of V2V network is a complex as there is no predetermined topology to be followed as vehicles are moving from one place to another. Applications for vehicular networks is classified into four major categories, namely security and crash forestalling, traffic infrastructure organization, vehicle telematics, and activity services and network connectivity Vehicles converse with each other inside a range of 1000 m. Two different types of communication are possible; first is vehicle-to-vehicle and the other is vehicle with the kerb infrastructure. Vehicular statement system is developed as a part of Intelligent Transport System (ITS). From a network architecture attitude, focus is primarily positioned on routing protocols; Physical layer (PHY), Medium Access Control (MAC) layer, and data lines [7].

4. FUTURE APPLICATIONS

4. 1. Prediction of natural disasters

The grouping of sensors and their independent synchronization and simulation will help us to project the occurrence of land-slides or other natural disasters and to take proper actions in prior:

4. 2. Smart Security

IOT can also be used to determine its applications in the field of safety and supervision e.g., supervision of spaces, tracking of persons and resources, infrastructure, etc.

4. 3. Design of smart homes

IOT can help in invent of smart homes e.g., power utilization management, interface with appliances, detecting emergencies, residence security and discovery of things easily, etc. [8].

4. 4. Using IOT for safer mining production

Mine safety is a big apprehension for most of the countries due to the functioning condition in the subversive mines. To stop and decrease disasters in the mining production, IOT technologies are need to be used to make prior warning, calamity forecasting, and security improvement of subversive production [9].

4. 5. Smart grid

The progress of most aspects of the smart grid would be improved by the application of the IOT technology. The structural design of IOT for the smart grid was initiated in China, which is of three layers: the sensitivity layer, the system layer and the function layer [10].

5. CONCLUSION

The IOT has the capability to append a new dimension to this process by establishing a communication among smart objects. The internet has significantly transformed the manner we live, as in situation all the communications are done via the internet. This paper presents a study about the architecture of IOT and also about the various technologies involved in implementation of Internet of Things. This paper also lists some of the applications of IOT.

References

[1] B. Khoo, RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 2011, pp. 709-712, doi: 10.1109/iThings/CPSCom.2011.83

[2] Mandeep Kaur, Manjeet Sandhu, Neeraj Mohan and Parvinder S. Sandhu, RFID Technology Principles, Advantages, Limitations & Its Applications. *International Journal of Computer and Electrical Engineering*, Vol. 3, No. 1, February - 2011.

[3] M. J. Booysen, S. Gilmore, S. Zeadally, G. J. van Rooyen. Machine-to-Machine (M2M) Communications in Vehicular MIH Media Lab. *KSSI transactions on internet and information systems* Vol. 6, no. 2, February - 2012.

[4] R. Lu, X. Li, X. Liang, X. Shen and X. Lin, GRS: The green, reliability, and security of emerging machine to machine communications, in *IEEE Communications Magazine*, vol. 49, no. 4, pp. 28-35, April 2011, doi: 10.1109/MCOM.2011.5741143

[5] Ernst Haselsteiner and Klemens Breitfu. Security in Near Field Communication (NFC) Strengths and Weaknesses, 2011. Corpus ID: 12748070

[6] Y. Lin, D. Sylvester and D. Blaauw. Near-field communication using phase-locking and pulse signaling for millimeter-scale systems. *2009 IEEE Custom Integrated Circuits Conference*, 2009, pp. 563-566, doi: 10.1109/CICC.2009.5280769

[7] Mrs D. K. Bhole, A review of emerging technologies under Internet of Things. *International Research Journal of Engineering and Technology* 02, 08, (2015) 1612-1615

[8] R. Khan, S. U. Khan, R. Zaheer and S. Khan. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. *2012 10th International Conference on Frontiers of Information Technology*, 2012, pp. 257-260, doi: 10.1109/FIT.2012.53

[9] Wei Qiuping, Zhu Shunbing, Du Chunquan, Study On Key Technologies Of Internet Of Things Perceiving Mine, *Procedia Engineering*, Volume 26, 2011, Pages 2326-2333, https://doi.org/10.1016/j.proeng.2011.11.2442

[10] Xiang Zhen Li; Xi Chen; Yan Zhen, Applications of Internet of Things on smart grid in China. State Grid Inf. & Telecommun. Co. Ltd, Beijing, China - 2011.