Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 41 (2016) 135-143 EISSN 2392-2192

The Internet of Things - A survey

S. K. Anithaa, S. Arunaa, M. Dheepthika*, S. Kalaivani, M. Nagammai, M. Aasha, S. Sivakumari

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

*E-mail address: dheepthika.m@gmail.com

ABSTRACT

The Internet of Things is a new era where the day-to-day objects can be mannered with sensing, networking and processing capabilities that will allow them to get across with one another round the internet to attain divers intent.

***Keywords*:** Internet of Things, Evolution of Internet of Things, IoT

1. INTRODUCTION

With the swift proliferation of Internet technology and communications technology, our lives are gradually led into a visionary space of imaginary world. Nevertheless, human beings subsist in the real world and cannot be thoroughly implemented round the services in the imaginary space. To snuff out these constraints, a newfangled technology is required to blend imaginary space and real-world on an identical platform which is called as Internet of Things (IoTs). This survey is based on several security and privacy issues related to Internet of Things (IoTs). Then, discussion on some applications of IoTs in real world is made. The rest of the paper is organized as follows: Section 2 defines the various components of IoT such as outline, evolution and architecture. Section 3handles the applications of IoT. Section 4 includes the security and privacy interest of IoTs. Section 5 concludes survey study with references at the end.

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

2. IOT- AN OVERVIEW

2. 1. Expansion of IoT

The "I" in IoT refers to the "Internet" that corresponds to the Internet protocols (i.e.) the digital data of the real world is stored in the virtual storage drive called cloud. The "T" in "IoT" is used to define "Thing" which is actually a sensor through which the data is transmitted or controlled which is demonstrated in Fig. 1,

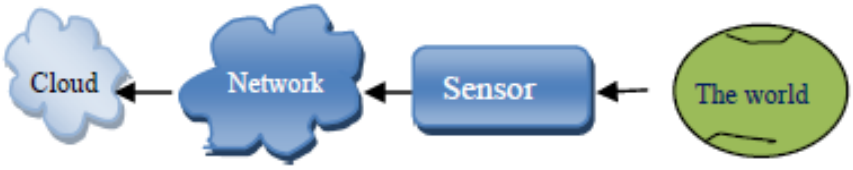

Fig. 1. Structure of Internet of Things

As shown in Fig. 2, soon everything and anything could be connected through the Internet of Everything (IoE) known as Internet of Things (IoT).

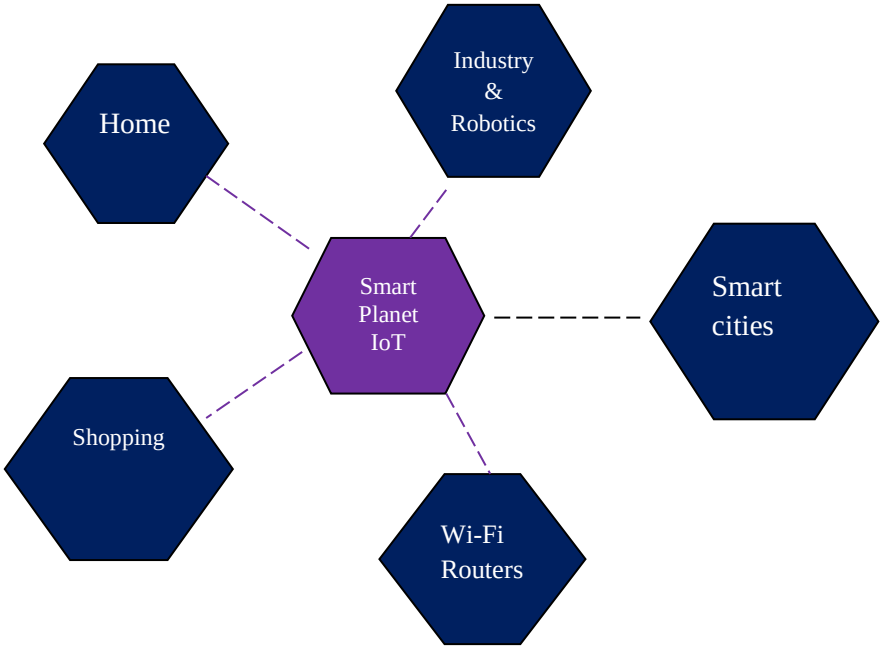

Fig. 2. Smart planet IoT

2. 2. Evolution

The Internet of Things will be the next big thing to hit the enterprise. The IoT will design a complete new data structure – something that will be leaner, cheaper networking abilities that are high-caliber to today's state-of-the art by multiple order of magnitude. Fig. 3 shows the evolution of the IoT.

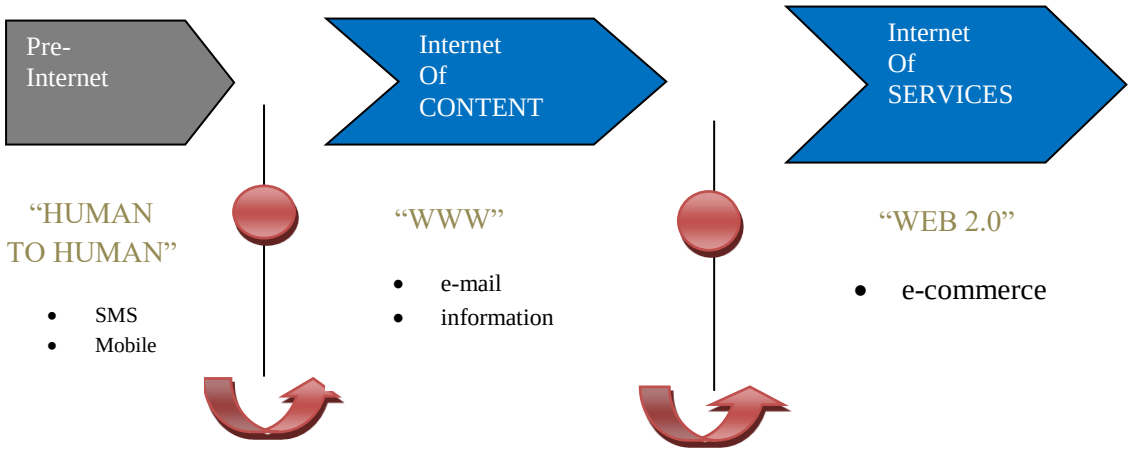

Fig. 3. Evolution of Internet of Things

2. 3. Architecture

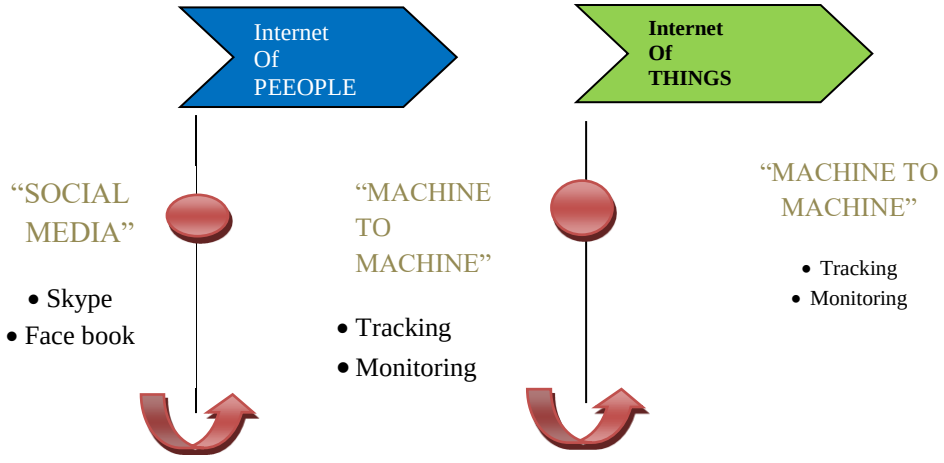

Fig. 4. Architecture of Internet of Things

The *thing* words relates to smart sensors, simple human-machine interfaces (HMIs), and so forth which conjoin in a Network of Things (NOT), to ubiquitously interact with other *thing*, the environment and people. NoT is basically a resource-challenged ecosystem, typically with medium-high time access delays, increase in error level, lower data throughput and limited time online where energy consumption must be increased to the maximum. The basic blocks of communication, computation and interaction using sensors, actuators, and HMI are distinguished in a simplified model of a *thing*. The Internet world is built around computers, centralized software infrastructures, or in the cloud. Applications and services use*thing*to provide context awareness, artificial intelligence, effective computing and so forth.

Depending on their specifications both tablets and smart phones can be used. Nevertheless, due to their power (battery, lifetime) we find it more appropriate to consider them more related to the world of computers and Internet than when compared to the world of *things*. Currently, Internet provides the basic infrastructure for the interchange of information. However, in order to have access, it has several constraints such as the need for unique identifier, to have a change of communication, and adopting the Internet Protocols. Nowadays, this "IP wall" is looped through an IoT gateway. In order to provide services to end users the Internet is used as it is the global interconnection method in which a web of services and applications make use of the information extracted by the IoT. On each of them, needs are virtual representations of the *things* of the IoT in order to enable interaction. Once the "IP wall" is saved, thanks to the connectivity provided by the Internet services one can access the information. But, for the information to be useful, it must be understood and this results in the origin of the "understanding wall" [1].

2. 3. 1. Protocols

By implementing the communication between the devices (D2D) the functionality of the IoT is initiated. And then the device data is collected and given to the infrastructure of the server (D2S), which then shares the device data (S2S), possibly providing it back to the devices, or to people.

***MQTT*:** In short it is a protocol for collecting device data and communicating with the servers (D2S). But is defined as a publish-subscribe based "light weight" messaging protocol. In the real world application the MQTT is used by the face book messenger. Its components are,

- MQTT Broker
- MQTT methods

***XMPP*:** It is a protocol best for connecting devices with people which is a special case of the D2S pattern, since people are connected to servers. It is based on the XML (Extensible Markup Language).

***DDS*:** A fast bus for integrating intelligent machines (D2D).

***AQMP*:** A queuing system designed to connect servers to each other (S2S).

3. APPLICATIONS

IoT touches every facet of our life. It is widely used in many applications like building and home automation over wearable.

3. 1. Building & Home Automation

From enhancing security to reducing energy and maintenance costs, TI offers a variety of innovative IoT technologies for monitoring and controlling intelligent buildings and smart homes. As in Fig. 5, the IoT consists of different sensors like temperature, gas, motion and LDR. Initially the Intel Galileo got connected to the Internet by using Wi-Fi. The parameters of sensors like p1, p2, p3, etc. will be read when the connection is made. The threshold levels for the required sensors are set as t1, t2, t3, etc. The sensor data are stored in cloud by sending

the required data to the web server. The data can be analyzed anywhere any time. If the threshold level is lesser than the sensor parameter then the respective alarm a1, a2, a3, etc. will be raised and in order to control the parameters the required actuation is done. In this model the temperature, gas leakage and movement in the house is monitored. The temperature and the movement detectionis stored in cloud for analyzing. If the temperature exceeds the threshold then the cooler will turn on automatically, similarly the alert sound is produced for the gas leakage.

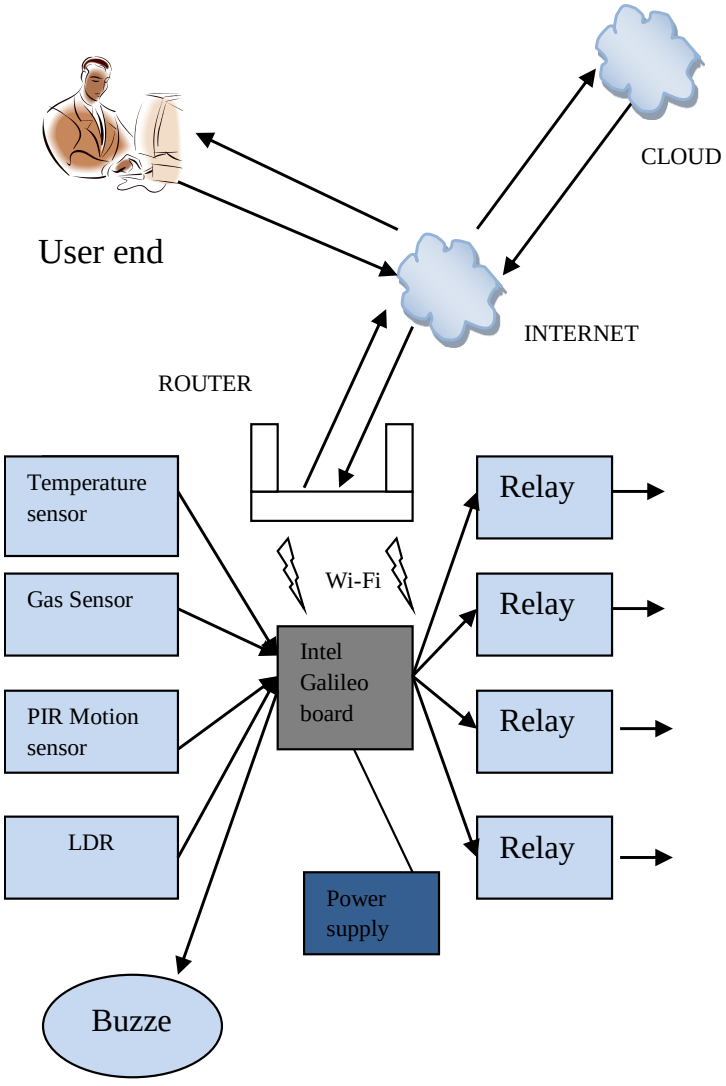

Fig. 5. IoT model of Home Automation System

3. 2. Smart cities

The IoT brings together the People, Process, Data and Things necessary to make Networked Connections that are more relevant and valuable as seen in Fig. 6.

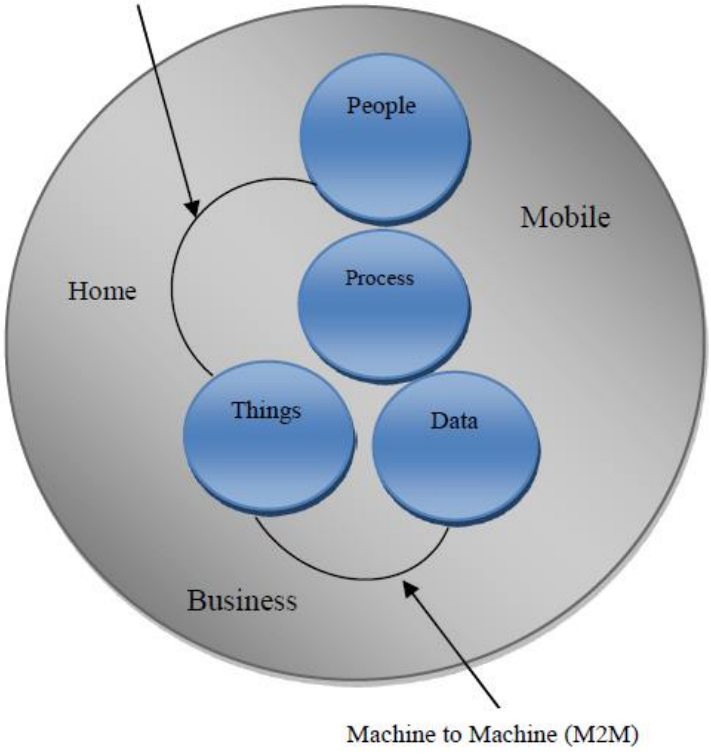

Fig. 6. IoT in smart cities

3. 2. 1. People

In IoT, people will be able to get connected to the Internet in multitude ways. In today's world people have a very close connection to the internet through their devices such as PCs, tablets, TVs, and smart phones also to social networks such as Face Book, Twitter, LinkedIn and Pinterest. Everything will get connected in immeasurable ways as technology and people evolve towards the path of using IoT. [2]

3. 2. 2. Data

Using IoT data is gathered and streamed over the internet to a central source to be analyzed and processed. As the number of things connected to the Internet increase rapidly, they will become more intelligent by converting data into more useful information. Instead of sending raw information, when things are connected they send higher standards of data back to machines, computers and to people for further evaluation and decision making.

This conversion of raw information to useful data using IoT is important as it has the capacity to make faster and more intelligent decisions, also allowing us to control our environment more effectively [3].

3. 2. 3. Things

Things such as sensors, consumer devices and enterprise assets are physical items that are connected with the Internet and with each other. In IoT, these things will help sense more data,

become context-aware, and provide more experimental information to help people and machines make more relevant and valuable decisions.

3. 2. 4. Process

Process is vital to understand how people, data and things work with each other to give a better result in the connected world of IoT. With the correct process, connections become vital as they add value to IoT because information is delivered at the right time to the right person in the most secure and reliable way possible [4].

3. 3. Wearables

Wearable devices are now the most trending discussion related to the Internet of Things (IoT). Using lower end applications one could support connections to simple sensors, security and low-speed wireless access all from a low-cost battery. MCUs can operate for a long period of time on very low current. Hence they can be used in wearable applications where storing, processing and sensing are needed at the biometric frequency time intervals. These sensor oriented devices use some periodic processing power; however, minimizing wireless data transmission time will offer power saving for the largest system [5].

3. 4. Healthcare

The Internet of Things (IoT) could be a game changer for the healthcare industry. It transforms the healthcare industry by increasing efficiency, lowering cost and focusing better on patient care. It provides the major advancement in three main fields, such as

3. 4. 1. Cloud-based hospital hygiene system

Hospital-Acquired Infections (HAI) are devastating from the perspective of both the clinical and economic point of view, also implementing a heavy toll on patients and contributing to rising healthcare costs. Unfortunately, 20% to 40% of HAI patients are transmitted to hospital employees, and it has been discovered that proper hand hygiene only occurs approximately to about 55% of the time by hospital care providers. So this lead to recording of the individual staff interactions with the hand sanitizer dispenser using real- time location system (RLTS) technology that is attached to the employee badges and sanitizers dispensers. This data was then utilized to accurately understand the intact levels of hospital staff [6].

3. 4. 2. Solution for the functionality of core practice

This IoT solution helped maintain a central record of all the patient files and real time monitoring, thus helping physicians to devote more time to treat patients. These solutions are capable of collecting and analyzing the data of different modules.

3. 5. Protein research and analytics tool

This solution focuses mainly on protein research and protein composition analysis. It ensures the reliability and accuracy of the equipment and provides researchers evident access to appropriate computing power for testing [7].

4. SECURITY AND PRIVACY

IoT security is the area of endeavor that is concerned with safeguarding connected devices and networks in the Internet of things. The Internet of Things involves the increasing support for objects and entities- known, in this context as things that are provided with unique identifiers and the ability to automatically transfer data through a network. Much of the increase in the usage of IoT communication comes from computing embedded sensor systems that are used in industrial machine-to-machine (M2M) communication, home and building automation and wearable computing devices.

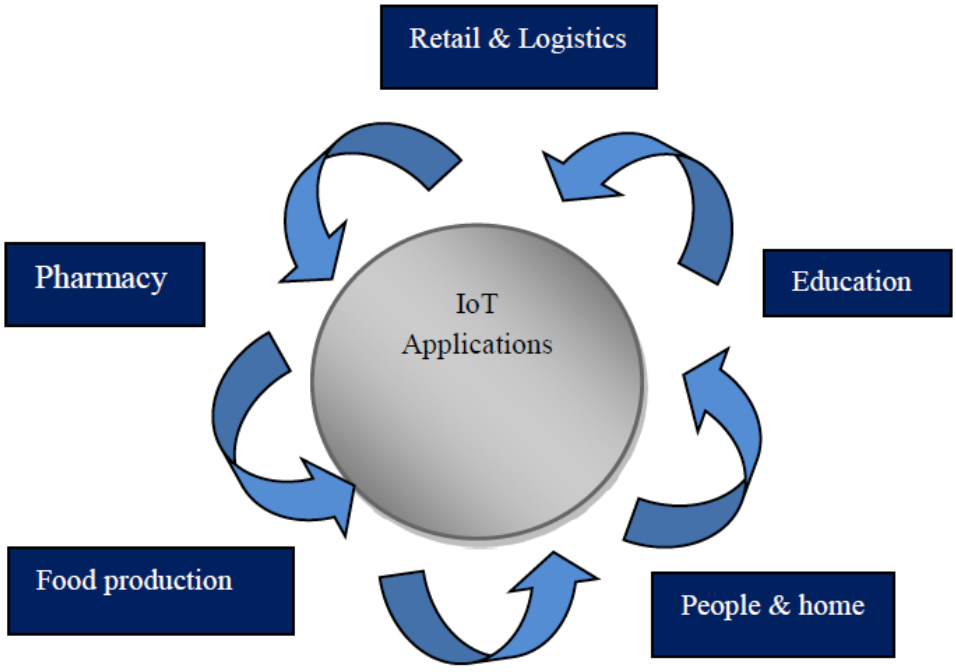

Fig. 7. IoT applications

IoT devices are typically wireless and are located in public places. Wireless communication in today's Internet is made more secure through encryption. Encryption is also a key to ensure that information is secure in the IoT. However, in order to support robust encryption many of the present IoT devices are not powerful enough. To facilitate encryption on the IoT, algorithms need to be designed more efficient and consume less energy and efficient key distribution schemes are required.

In addition to encryption, identity management is a vital component of any security model and unique identifiers are essential to the IoT devices. Using these identifiers personal identities at financial institutions, identify illegal activity and other functions can be established. Thus, they ensure that smart objects are who they say they are which is essential to the success of IoT.

The customer privacy is a very important issue. To achieve this many technologies are developedand still the developing process continues. VIRTUAL PRIVATE NETWORK (VPN) and TRANSPORT LAYER SECURITY (TLS) are the currently enhancing technologies for privacy goals [8].

5. CONCLUSION

In conclusion, the IoT connects the virtual world of things to the real world things. The main technology of IoT is RFID and sensors. Nowadays the sensors plays a major role and makes the human life more sophisticated. The IoT will provide highest security and privacy. To develop the application companies provide more importance to privacy and security. So IoT service to the world today is inevitable.

References

[1] Andrew Whitmore, Anurag Agarwal & Li Da Xu. The Internet of Things-A Survey of Topics and Trends and Business Media, NY, USA, 2014.

[2] Dhiren R. Patel & J. Sathish Kumar. A Survey on Internet of Things: Security and Privacy Issues *International Journal of Computer Applications* Volume 90, No: 11, March 2014.

[3] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista and Michele Zorzi. Internet of Things for Smart Cities, *IEEE Internet of Things Journal,* Vol. 1, No. 1, February 2014

[4] Joe Folkens. Building a Gateway To The Internet of Things. Texas, December 2014.

[5] L. Atzori, A. Lera, and G. Morabito. The Internet of Things: A Survey. *Comput. Netw.* 54(15) (2010) 2787-2805

[6] J. M. Hernandez-Munoz, J. B. Vercher, L. Munoz, J. A. Galache, M. Presser, L. A. Hemandez Gomez, and J. Petterson. Smart Cities at the Forefront of the Future Internet. *The Future Internet, Lect. Notes Comput. Sci.* 6656 (2011) 447-462

[7] R. Bonetto, N. Bui, V. Lakkundi, A. Sebanati, and M. Rossi, Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples," in *Proc. IEEEIoT - SoS,* San Francisco, CA, USA, 2012, pp. 1-7

[8] A. Laya, V. I. Bratu, and J. Markhendahl, Who is investing in machine-to-machine communications? in *Proc. 24th Eur. Reg. ITS Conf.,* Florence, Italy, Oct. 2013, pp. 20-23