National Journal of Multidisciplinary Research and Development
ISSN: 2455-9040
Impact Factor: RJIF 5.22
www.nationaljournals.com
Volume 3; Issue 1; January 2018; Page No. 1013-1016

Internet of things: A survey on enabling technologies, application and standardization

Nitin Sharma, Shadab Ali, Deepak Choudhary
Assistant Professor, Department of Computer Science & Engineering, Institute of Engineering & Technology, Alwar, Rajasthan, India

Abstract
Internet of Thing (IoT) has been a considerable attention from last few years. The paper is an elementary survey of IoT application areas, security and privacy issues, supporting tools and standardization techniques that an end user keeps in mind while designing an IoT device.

Keywords: IoT, security, privacy, standardization

1. Introduction
In last decay, IoT has become trending through representative application (e.g. intelligent transportation, green house monitoring, telemedicine monitoring). The term internet of things refers to the network of physical devices, machine, home appliance, vehicles and other item which embedded with network and electronics, that put up the data from their sensors to the cloud and other structural representative software through a network. The IoT allows to sense or remotely access the object through network infrastructure. That give us sophisticated technology between physical world and computer system and it improve efficiency, accuracy and instance data deliver through network parameter. The term "Thing" in the IoT refers to the wide variety of devices like camera streaming and control, automobile with built in sensors, biochip, DNA analysis. Legal scholars suggest regarding "Things" as an "inextricably mixture of hardware, software, data & service". The word "The internet of things" was proposed by Kelvin Ashton of Procter & Gamble (P & G), later MIT's Auto – ID center in 1999 (Perera *et al*., 2013) [1].

2. Evolution
Before doing investigation of the IoT in depth, it is worthwhile to know the evolution of the internet. In the late 1960s the computer communication between two computer was made possible through a computer network. Later in 1980s, the TCP/IP stack comes in the light. After that commercial use of the internet came. Later the World Wide Web (WWW) became more popular in 1991 which help internet to gain more popularity and rapid growth. After uses of WWW, user went more forwarded and connect internet to mobile and form mobile internet. Later on the invention of internet, the next step to connect object around us to each other (e.g. M2M) and interchange data via internet.
IoT helps in creating the world where all object may easily connect to each other via Internet. The final goal is to create "a better world for human being" where object around us know what we like and what we need, and they act accordingly without less human interaction (Palattella *et al*., 2012) [5].

By the mid of 1990s, web servers were added in the embedded product. These manufacturers were rapidly integrating internet connected system into the high value asset tracks and fleet management. They liked it for more than 15 years. However, it is getting easier to integrate M2M machine system as more powerful processor are incorporated into the end nodes (Vermesan *et al*., 2012) [6]. These processors support high level operating systems.

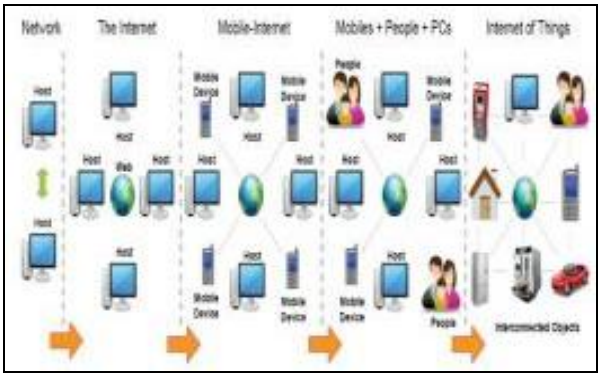

Fig 1: Evolution of internet of things

3. Applications
Later in 2010, a survey was done by IOT-I project that identified IoT's application (Vermesan *et al*., 2012) [6]. These applications were grouped in 14 domains. These are: transport, smart home (Bing *et al*., 2011) [4], smart city (Liu & Yang, 2011) [3], lifestyle, retail, agriculture, smart factory, supplychain, emergency, health care (Zhao *et al*., 2011) [7] and energy. Our survey is based on 270 responses from 31 countries.

3.1. IoT in medical application
Due to rapid growth of population and aging, IoT is arising of challenges to equally serve the health treatment. Since, many rural areas has no health care center. they usually suffer from big problem regarding their health issue.
There is a serious shortage problem with medical staff, specially in rural area, lack of medical instrument kit, low

level of treatment. Inadequate disease prevention & early detection capability.

The imperfect diseases prevention system cannot meet the national strategy requirements to safeguard the health of the citizen becoming heavy burden on economy, individuals, families and state.

To overcome these issue, remote monitoring & management platform of healthcare and information (RMMO-HI) (Zhao *et al*., 2011) [7] can easily monitor and manage rural lifestyle diseases. Hence, IoT can easily prevent from these disease.

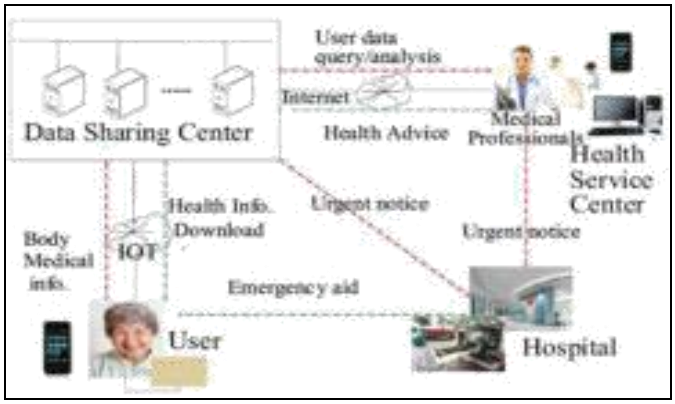

Fig 2: Framework of healthcare service

Regardless of restrictions of location, time and human activity state, RMMP-HI can collect the body medical information timely through variety of sensors which are loaded in the human body. These informative data sent to the nearby data sharing center where doctors can easily handle more than one area of people at one place. It also do analysis of these data and notify them in real time, when suspicious result is found. It is also useful to maintain the nation record of people medical information for higher research and development in medical field. Body medical sensors are responsible for register and delete, constituting Medical Body Area Network (MBAN) automatically (Zhao *et al*., 2011) [7]. As shown in Fig. 2, short-range wireless communication sensors module can easily transmit human information to mobile phone or home gateway. This medical information is uploaded to datacenter and processing timely. After that, the important result will be send back to the respective person. First-aid notification is delivered to nearby health care center and then they deliver emergency service to the patient.

3.2. IoT in smart home

In recent years, people have higher and higher requirement not only on the automation for information of housing and accommodation, but also on the flexible control of house hold appliance and the accessibility of acquiring the external information along with the rapid development of network technology, communication technology and for meeting the need of the "Well-off Society" (Bing *et al*., 2011) [4]. Thus, a well improved smart home network is in demand to establish. in the smart home system, so that home life becomes more comfortable, safer, and effective through the overall management. A smart home network is shown in Fig.3.

At present, all kind of low transmission rate data such as sensors, lighting, entrance guard, and equipment switch with a small data capacity have been maturely monitored and controlled through existing zigbee technology solution.

Fig 3: A smart home network

However, there have been no related research on the collection and the transmission solution of the voice, image and video data. In most related research at home and abroad, the advantage of applying zigbee technology to smart home network have been proven. In the domestic furniture system the application of the traditional sensors such as temperature, humidity, gas, smoke and CMOS camera, the collection of image information in the home network is mainly researched. The different control methods such as relay control, infrared control, serial port control and EIB control are mainly discussed in term of network structure. The network structure is designed as a star structure in most researches.

4. Security in IoT

The information security and privacy may be categories with some properties like identification, confidentiality, integrity and undesirability. Different from other technology, IoT deals with our private data such as health information, home camera surveillance, home light system etc. Thus security is at higher priority in availability and dependability of IoT devices.

4.1 1secure Architecture

IoT have been categorized in four key layers (Gang *et al*., 2011) [2]. The support layer gives the support platform for the application layer as shown in Fig. 4.

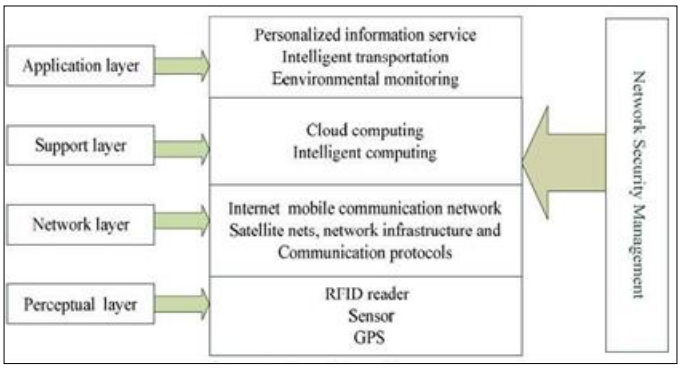

Fig 4: Security Architecture

Through this support platform all data will be organized through network grid and cloud. It combines application layer upward and network layer downward. The terminal level is application layer which is at the top most of the IoT security architecture. This layer helps user to customize services according to their need. User can access internet of things through application layer interface using television, personal computer or mobile device.

4.2 Security and Privacy Issues

Internet of things is a virtual network between real world and computer with real-time interaction. Initial stage of development of IoT is M2M, having deployment contexts and subscription. Unapproachable operation is done without human interaction by the wireless area network (WAN) or WLAN. Due to improvements in social efficiency new concerns of security and privacy breach started arising (Palattella *et al*., 2012) [5] shown in Fig.5.

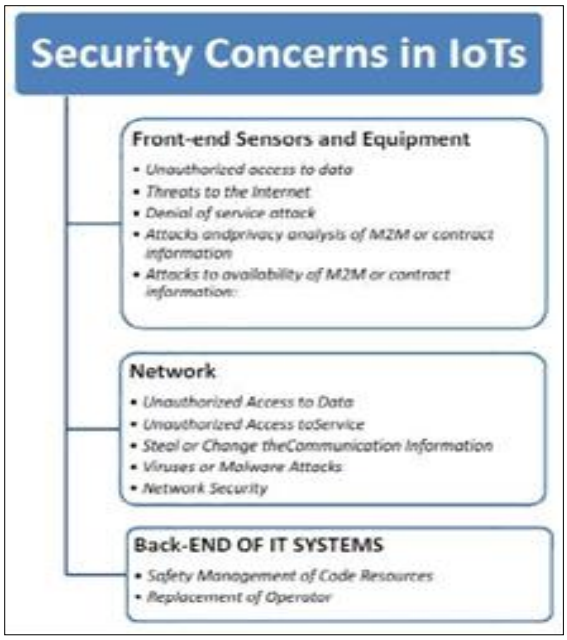

Fig 5: Security concerns in (Fig source – internet)

4.2.1 Front-End Sensors and Equipment

Front end perceptual layer sends data from different sensors and RFID reader to different modules of M2M device. This methodology involves the machines security with business implementation & node connectivity (Zhao *et al*., 2011) [7]. Perception nodes are general categories in the absence of monitoring sensors. An intruder may get easy access and damage these devices and their data. This results in denial of services attack.

4.2.2 Network

Network plays an important role because it provides a more comprehensive interconnection capability, effectualness, thriftiness of connection and an authentic quality of service in IoTs. Large number of machines in network sends enormous data that leads to network congestion, large number of nodes and groups in lOTs results in denial of service attacks (Gang *et al*., 2011) [2].

4.2.3 Back-End

Back-end of IoT systems form the gateway and middleware. It requires high security requirements, gathering, examining sensor data in real time to increase business intelligence. The security of IoT system has seven major standards viz; privacy protection, access control, user authentication, communication layer security, data integrity, data confidentiality and availability at any time.

5. IoT Standardization

To make communication between object and system a good standardization should be implanted. For the standardization of IoT, the simplified application collaborates through standardized interface of the application development ecosystem. It should have smart behavior through analytics capability and carries standardized data exchange format and interface.

Standardizing properly ensure that the processes, procedures and interfaces should be private and confidentiality of user is maintained. There should be expandability in applicable device ecosystem and reduction in deployment time with standards compliant devices executing applications requiring little or no customization. The system should provide an ecosystem that readily allows applications to share information and experiences.

5.1 Standardization Techniques

For making communication between object and system a good standardization should be proper implanted. Organizations like Wi-Fi alliance, the Bluetooth special interest group (SIG) & Zig Bee alliance ensures the interoperability of devices with wireless connectivity.

5.1.1 ZigBee

ZigBee (IEEE 802.15.4) is operated in 2.4GHz ISM band Perera *et al*., 2013) [1], but it supports the 868MHz and 916MHz ISM bands. ZigBee can reach a data of up to 250kbps while short active phases separated by long power down intervals enable several years of operation with a single coin cell.

According to ZigBee, the protocol layer above the 802.15.4 data link layer provides application profile. It is successful in smart grid applications.

5.1.2 Wi-Fi

Wi-Fi is basically based on the IEEE 802.11 standard (Perera *et al*., 2013) [1]. The standard was designed as a wireless replacement for the widely used, cable-based IEEE 802.3 Ethernet standard. It deals with the data link layer of a LAN and can be integrated into the TCP/IP stack. In Wi-Fi, TCP/IP is used for Internet connectivity.

5.1.3 Bluetooth SIG

The Bluetooth SIG has introduced a new architecture that supports a set of educational tools. These tools help developers to quickly create Internet gateways for Bluetooth products. Bluetooth gateway allows Bluetooth sensor to transmit data to the cloud and retransmit back again. Bluetooth architecture extends the potential functionality of the IoT. In this a person has the ability to monitor and control

fixed Bluetooth sensors from a remote location. For example like turning off our home lights while we are on vacation or unlocking our front door for a pet sitter.

6. Conclusion

Paper discusses invention and significance of IoT. An extensive survey is done to explain IoT application areas. Paper focuses on standardization techniques implanted to maintain privacy and confidentiality of IoT device user. Security and privacy concerns along with supporting tools are addressed so that manufacturer makes best secure platform to make IoT highly secure.

7. References

1. Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context Aware Computing for The Internet of Things: A Survey IEEE Communications Surveys & Tutorials, 2013, 1-41.
2. Gang G, Zeyong L, Jun J. Internet of Things Security Analysis, International Conference on Internet Technology and Applications, 2011, 1-4.
3. Liu J, Yang L. Application of Internet of Things in the Community Security Management, Computational Intelligence, Communication Systems and Networks, Third International Conference on IEEE, 2011, 314-318.
4. Bing K, Fu L, Zhuo Y, Yanlei L. Design of an Internet of Things-based Smart Home System, 2nd International Conference on Intelligent Control and Information Processing, 2011, 921-924.
5. Palattella M, Accettura N, Vilajosana X, Watteyne T, Grieco L, Boggia G, Dohler M. Standardized protocol stack for the internet of (important) things, Proceedings of IEEE, 2012, 1-18.
6. Vermesan O, Friess P, Furness A. The Internet of Things by New Horizons, 2012. [Online]. Available: http:// www.internet-of-things-research.eu/pdf/IERC_Cluster_ Book_2012_WEB.pdf
7. Zhao W, Wang C, Nakahira Y. Medical Application On IoT, International Conference on Computer Theory and Applications (ICCTA), 2011, 660-665.