(AGUIJET) 2018, Vol. No. 7, Jul-Dec **e-ISSN: 2455-0442, p-ISSN: 2455-6734**

A Review on Internet of Things

Pratiksha Gautam
Assistant Professor
Deptt. of Computer Science and Engineering
AP Goyal University Shimla H.P
pratikshamtech20@gmail.com

ABSTRACT

This paper extants an outline of the Internet of Things (IoT) with significance on enabling technologies, application protocols and security issues. The IoT is empowered by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The essential hypothesis is to have smart sensors collaborate directly without human fascination to deliver a new class of applications. The current rebellion in mobile, machine-to-machine (M2M) and Internet technologies can be seen as the first stage of the IoT. In the coming years, the IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together in support of intelligent decision making. This paper begins by presenting a overview of the IoT. Then, we provide a summary of some technical details that concern to the IoT enabling protocols, technologies, applications and security issues. We have reviewed survey papers and compared them in the field, our aim is to give an additional comprehensive review of the most pertinent protocols, application and security threats issues to facilitate scientists and application developers to get up to speed quickly on how the different protocols fit together to deliver desired functionalities and how the security issues can be curtail. We also presents an summary of some of the key IoT challenges as security and privacy concerns presented in the recent literature and provide a summary of related research work.

Keywords— *Internet of Things; Security Issues; IoT Architecture, Applications; Protocols*

INTRODUCTION

An emergent integer of physical objects is being linked to the Internet at an unparalleled rate comprehend the design of the Internet of Things (IoT). A vital illustration of such objects comprises the HVAC (Heating, Ventilation, and Air Conditioning) monitoring and control systems that enable smart homes. There are also other domains and environments in which the IoT can play a remarkable role and improve the quality of our lives. Unquestionably, the main strength of the IoT idea is the high impact it will have on several aspects of everyday-life and behavior of potential users. From the point of view of a private user, the most obvious effects of the IoT introduction will be visible in both working and domestic fields. In this context, domotics, assisted living, e-health, enhanced learning are only a few examples of possible application scenarios in which the new paradigm will play a primary role in the near future. Similarly, from the prospect of business users, the most perceptible ramifications will be

uniformly noticeable in fields such as, automation and industrial manufacturing, logistics, business/process management, intelligent transportation of people and goods.

By starting from the considerations above, it should not be surprising that IoT is included by the US National Intelligence Council in the list of six ‘‘Disruptive Civil Technologies” with probable collisions on US national power [2]. NIC foresees that ‘‘by 2025 Internet nodes may reside in everyday things – food packages, furniture, paper documents, and more”. It focus on future probabilities that will occur, originates from the idea that ‘‘popular demand combined with technology advances could coerce extensive transmission of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development”. This paper is structures as follows. Section 2 is related to evolution, architecture and elements of Internet of Things. Section 3 presents the application of Internet of Things. Section 4 discusses the security and privacy concerns in IoT. Finally, Section 5 concludes the paper.

EVOLUTION OF IOT

Before the investigation of the IoTs in depth, it is worthwhile to look at the evolution of the Internet. As shown in figure.1 in the late 1960s, communication between two computers was made possible through a computer network. In the early 1980s, the TCP/IP stack was pioneered. Then, commercial use of the Internet started in the late 1980s. Later, the World Wide Web (WWW) became available in 1991 which made the Internet more popular and stimulate the rapid growth. Then, mobile devices connected to the Internet and produced the mobile Internet. With the emergence of social networking, users started to become connected together over the Internet. Before the investigation of the IoTs in depth, it is worthwhile to look at the evolution of the Internet. As shown in figure. 1, in the late 1960s, communication between two computers was made possible through a computer network. In the early 1980s, the TCP/IP stack was introduced. Then, commercial use of the Internet started in the late 1980s. Later, the World Wide Web (WWW) became available in 1991 which made the Internet more popular and stimulate the rapid growth. Then, mobile devices connected to the Internet and formed the mobile Internet. With the surfacing of social networking, users started to become allied together over the Internet.

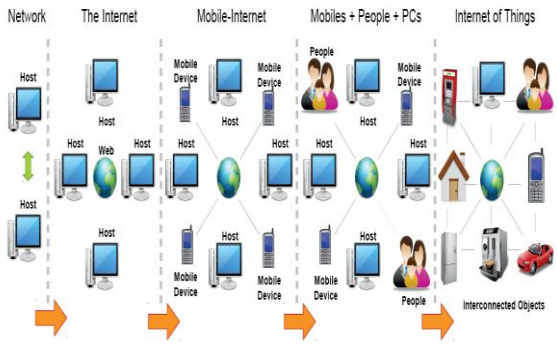

Figure.1 Evolution of Internet of Things

A. Architecture of IoT

IoTs can be classified into three significant layers such as Recognition or Perception, Network and Application. As shown in figure. 2, perception layer assembles information and recognizes

the physical world. Network layer is the middle one (also called as wireless sensor networks), which is accountable for the preliminary dispensation of information, broadcasting of data, assortment and polymerization. The uppermost application layer suggests these refurbish for all the industries. However, along with these layers, the middle one network layer is a "Central Nervous System" that guards the global services in the IoTs, since it operates the part of comprehensive with upward application layer and formulates the link sliding of perceptual layer [9, 10, 11].

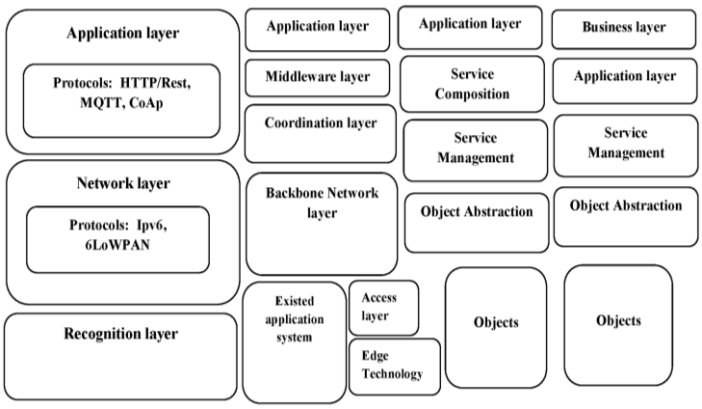

Figure. 2 A generich architecture of IoT

B. Elements of IoT

Understanding the IoT building blocks helps to gain a better insight into the real meaning and functionality of the IoT. In the following sections we discuss six main elements needed to deliver the functionality of the IoT as illustrated in figure 3.

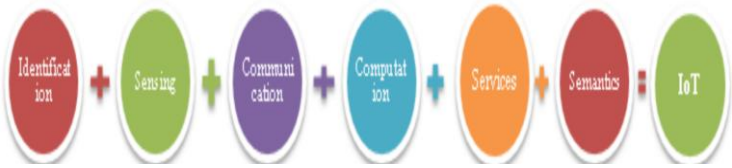

Figure. 3 Elements of IoT

Figure.3 depicts the elements of the Internet of Things such as identification (critical to identify the names and match services for IoT). Sensing means to collects information from the objects within the network. Communication (IoT communicates different objects collectively to deliver explicit services. Computation (software application and processing units signify the computational facility of IoT). Services can be classified into four types in terms of IoT as Identity-related services (to bring real world object into virtual world), Information aggregation services (to accumulate and summarize raw sensing measurements), Collaborative-Aware services and Ubiquitous services (to review some applications of IoT). Moreover, the last element of IoT is semantic (it is used to haul out knowledge information from different machines to give required services.

(AGUIJET) 2018, Vol. No. 7, Jul-Dec **e-ISSN: 2455-0442, p-ISSN: 2455-6734**

APPLICATIONS OF IOT

According to survey done by the IoT-I project in 2010 [3]indicated IoT's circumstance applications could be grouped in 14 domain as Transportation, Smart home, Smart city, Lifestyle, Retail, Agriculture, Smart factory, Supply chain, Emergency, User Interaction, Healthcare, Culture and tourism, Environment and Energy. This survey was based on 270 responses from 31 countries demonstrated the most interesting circumstance applications were: smart home, smart city, transportation and healthcare. In this paper, the focus will be briefly on the IoT's applications in transportation, healthcare, smart city or home, personal and social.

a) Assisted Driving

Today's different type of transportation such as cars, train and buses along with the road and the rails equipped with sensors, actuators and powerful processors may provide beneficial information to the driver and/or passengers (i.e. accidents, temporary and/or permanent road closures, traffic congestions) to provide better navigation and safety [4]. The numerous profit and non-profit organizations would benefit from gathered road traffic patterns information such as governmental authorities used for construction/planning purpose, freight companies used these information to perform more route optimization which allows energy saving, and so on.

b) Mobile Ticketing

Electronic posters or billboards presenting information in regard to transportation services can be assembled with the NFC tag. The user can acquire data from the web by either hovering their mobile phone over the NFC tag or pointing the mobile phone to the visual markers [5,9,10,11]. The mobile phone automatically retrieves and combines information from the related web services (stations, number of passengers, costs, available seats, departure and arrival time, and type of services) and provides the suggestion about tickets which suitable for each user.

c) Sensing

Sensor device enable multifunction focused on both in patient and out-patients treatment and especially on diagnosing patient conditions providing real-time information on patient health indicators. Heterogeneous wireless access-based remote patient monitoring system can be deployed to reach the patient everywhere with multiple wireless technologies integrated to support continuous bio-signal monitoring in presence of patient mobility [4] [6].

d) Identification and Authentication

Identification and authentication are two terms that described the preliminary phases of the security process in computer systems which could apply to healthcare, for instance, patient identification to reduce harmful incidents to patient, current electronic medical record maintenance and infant identification in hospitals to prevent mismatching. An identification and authentication procedure is most frequently used to manage, grant access and improve medical staff morale by addressing patient safely issues [4]. In addition, identification and authentication are essential parts to meet the requirements of security schemes and prevent thefts or losses of precious instruments and products.

e) Comfortable Homes and Offices

Sensors and actuators distributed deployment in houses and offices could make our life easier in several aspects, room heating can be adapted as predefined preferences and the weather; the room lighting can automatically change according to the time of day; hazardous incidents can be prevented with appropriate alarm and monitoring system [4] and energy cost could drastically

reduced by automatically switching off the electrical equipments such as television, air condition, kettle, fridge, light bulb and so on, when not used.

f) Social Networking

This application is involved to the automatically update of information and location about our social activities in social networking websites. We probably think of RFIDs which generate events about people and places to assist users real-time updates in their social networks [4].

SECURITY AND PRIVACY CONCERN IN IOT

The security and privacy of information and network should be equipped with these basic principles such as confidentiality, integrity, availability, authentication and authorization [4]. Unlike from the Internet, the IoT will be applied to the most significant of global economy. For instance, transportation, healthcare, smart city and home, personal and social. Therefore, the security and privacy issues are the most concerned that need to be addressed in IoT.

1. Security Concerns

Internet of Things is seamlessly combined two disparate worlds into one. In the initial stage of IoT, mostly researchers are focused on developing the M2M (Machine to Machine) communication protocol that distinct from general network communication in case of characteristics and deployment environments [7]. Though dramatically improve in IoT it creates a concerning problems which affecting security and privacy of information. Front-end Sensors and Equipment: Front-end sensors and equipment is responsible for receive data via smart sensors then transmit the data to central processing system by using M2M modules device. Through the eccentric architecture of IoT some perception sensors or devices are mostly deployed in the absence of monitoring system [7] which create vulnerabilities to attack from the outsiders such as an attacker can readily access and continuously reprogram until these devices could send data not only to registered server but also to many groups of attackers. Thus, the possible threats to front-end sensors and equipment can be assorted into three groups: eavesdropping, unauthorized access to data and denial of service attack.

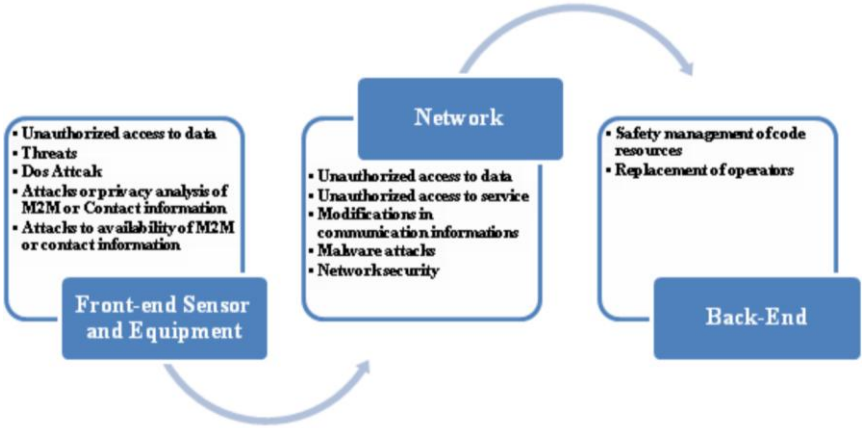

Figure. 5 Security Concerns of Internet of Things

- Network: Network in IoTs is directly responsible for overall M2M communication management as well as reliable quality of service (QoS) [7]. Since the enormous volumes of data

sending to high traffic network, large number of devices are currently connected to network may be caused of denial of service attacks.

- Back-end: Back-end is the most important part of IoT system which has high security requirements and efficient sensor data analysis and management unit inside to enable real-time data processing. The typical security of IoT system can be classified into seven major domains as follows: privacy protection, access control, user authentication, communication security, data integrity, data confidentiality and availability at any time [7].

2. Privacy Concerns

Generally, the IoT standard communication, the distributed environmental sensor devices are connected to the Internet or network then signal the specific information which gathered from sensor devices toward the central server via Mobile or fixed communication. Privacy issues should be concerned in entire process of wireless communication since in the device, in storage, during communication and even during processing process [7] which helps to conceal the sensitive information. Thus, the privacy of users and personal information are one of the key challenges in IoTs which have to cope with.

- Privacy in Device: The unsecure devices always have at least one or more vulnerabilities which probably caused to leak out of confidential information in case of inappropriate hardware and software design. For instance, the attackers can directly remote access to victim's device then change the destination account name and number while doing an online transaction. Hence, reliability and robustness are the essential features for devices that gather sensitive data [7]. Nowadays, there are numerous privacy issues in the device that need to be addressed such as hiding the folder containing personal information (i.e. login name and password, registered phone number, citizen ID number, etc.) when the device theft or loss, concealing the current or recorded location information of device holder, encrypting the communication links both wired and wireless in order to prevent unwanted third parties eavesdrop on your conversations.

- Privacy during Communication: One of the most useful and effective approaches to maintain data confidentiality during the data transmission process is encryption. However, some encryption algorithms may provide an easier way to attackers for tracing data and analysis of linking packets. Hence, secure communication protocols should be suitable approach to address this issue.

- Privacy in Storage: The common procedures to keep information privacy in storage devices or databases is stored only frequently used data for routine tasks but excluding personal and specific information. To conceal the stored data not only a Pseudonymization and Anonymization technique could be a suitable approach [7] but also hide any specific record and force the database could display only statistical data to ensure the output is not related to particular record.

- Privacy at Processing: This problem generally consist of two issues, first, sensitive data must be treated in an appropriate way as desired purpose. Secondly, Mostly data owner are inadequate of information privacy knowledge and cause of their personal data explicitly disclosed or transferred to third party. Thus, the most effective technique that could deal with those crucial problems is Digital Right Management (DRM). The DRM could control and protect against illegally used and re-distribution [7] of commercial media through define a set of privacy policies for each personal data during the data processing procedure. However, for effective and efficient operations of DRM essentially require trusted and powerful devices.

(AGUIJET) 2018, Vol. No. 7, Jul-Dec **e-ISSN: 2455-0442, p-ISSN: 2455-6734**

CONCLUSION

The Internet has changed drastically the way we live, moving interactions between people at a virtual level in
several contexts spanning from the professional life to social relationships. The IoT has the potential to add a
new dimension to this process by enabling communications with and among smart objects, thus leading to the vision of ‘‘anytime, anywhere, any media, anything” communications. To this purpose, we observe that the IoT should be considered as part of the overall Internet of the
future, which is likely to be dramatically different from the Internet we use today. In this paper, we have presented a comprehensive review on Internet of Things which covers , IoT application elements, protocols and discuss the security issues in Internet of Things.

REFERENCES

1) National Intelligence Council, Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests Out to 2025 – Conference Report CR 2008-07, April 2008, <http://www.dni.gov/nic/NIC_home.html>.

2) Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context aware computing for the internet of things: A survey. IEEE Communications Surveys & Tutorials. 2014 Jan 1;16(1):414-54.
3) Smith IG, editor. The Internet of things 2012: new horizons. CASAGRAS2; 2012.
4) Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer networks. 2010 Oct 28;54(15):2787-805.
5) Bing K, Fu L, Zhuo Y, Yanlei L. Design of an Internet of things-based Smart Home System. InIntelligent Control and Information Processing (ICICIP), 2011 2nd International Conference on 2011 Jul 25 (Vol. 2, pp. 921-924). IEEE.
6) Niyato D, Hossain E, Camorlinga S. Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization. IEEE Journal on Selected Areas in Communications. 2009 May;27(4).
7) Kumar JS, Patel DR. A survey on internet of things: Security and privacy issues. International Journal of Computer Applications. 2014 Jan 1;90(11).
8) M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.
9) Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer networks. 2010 Oct 28;54(15):2787-805.
10) Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials. 2015 Nov 18;17(4):2347-76.
11) Kumar JS, Patel DR. A survey on internet of things: Security and privacy issues. International Journal of Computer Applications. 2014 Jan 1;90(11).