International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 6 (2018) pp. 4599-4605

Stay Connected – Internet of Things

[1] Osama Abdul Jaleel Ali, [2]Samir Qaisar Ajmi, [3] Sarmad Hmzah Ali
Al-Muthanna University, Computer Centre, Samawah, Iraq.

INTRODUCTION

Internet of things IOT [1] can be defined as interconnection of computing devices bearing identification on internet. Devices those are connected on internet can be sensed with the help of sensor and can be programmed to follow the command. There can be many devices like, Laptops, computers, mobile phone with SIM, and RFID [2] tag, a GPS chip, etc. All these electronic devices can be directly connected on the internet. One major problem of internet was of the IP addresses. For being on the internet, any device needed to have an IP address. This IP address is a universal identification number of that device that can be sensed on the internet. Till now IPv4 with 32 bit size could handle about 2^{32} i.e. 4,294,967,296 IPv4 addresses; whereas IPv6 has a 128 bit address, which could handle about 2^{128} i.e.340,282,366,920,938,463,463,374,607,431,768,211,456 addresses. On getting this figure we can analyze that these addresses are much more than total human population on earth. Approximately every human being can have about one trillion trillion addresses. It is expected that these addresses are sufficient enough and can last for around 1000 years from now before getting exhausted.

With internet it also requires some sensors for detection of devices. Sensors [2] are being used in industries since 80's. Like light sensor, CO_2 sensor, weight sensor, heat sensor, etc. with the help of electronics integrated chips IC's, these sensors became cheaply available in IC's with all its required circuitries. This leads to embedded technology [13] which gave birth to IOT. [8] In this paper we shall discuss the IOT its technology, application areas and threats.

NETWORK

Internet

Internet means network of networks. Many smart devices if connected together form a network. Smart devices are those devices those can communicate with other devices connected within a network. To be precise in communication, each device communicating with other device needs an IP address. IP is internet protocol, which enables any device to show its presence on the network. We have discussed the IP addresses in the previous section. In the network there are devices like Switches, Routers, Hubs, Servers, etc besides other devices like mobile phones, computers, laptops, etc. These devices help in making communication between different smart devices. Every entity on the network needs an IP address. When these networks are connected together they form an Internet.

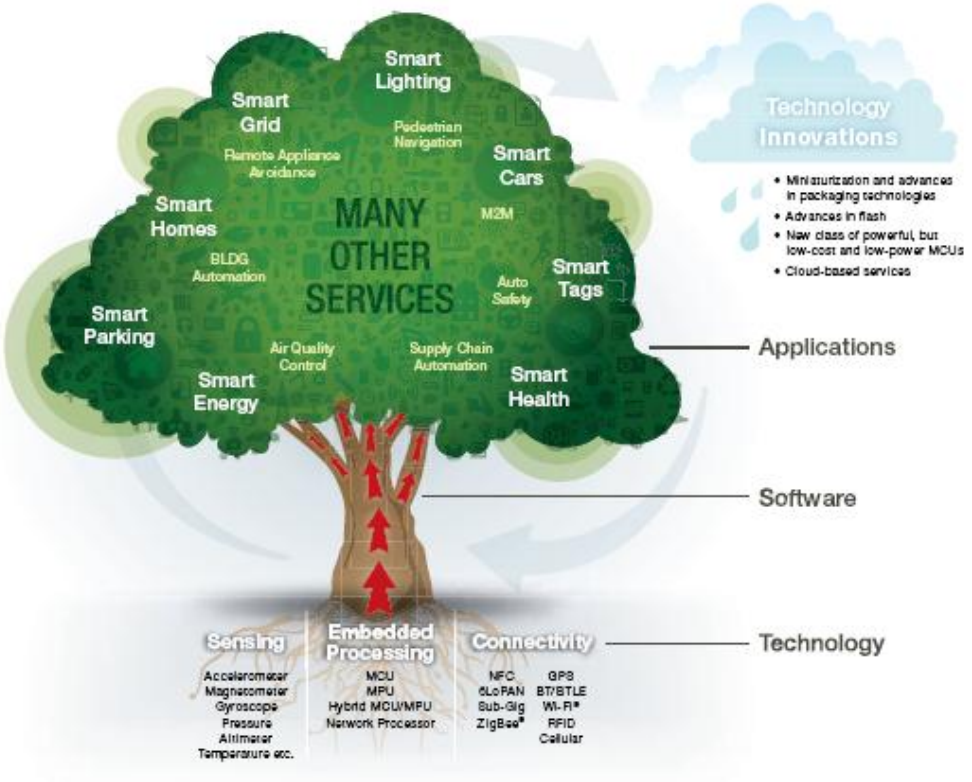

Figure 1: The Internet of Things: Different Technologies, Services & Meanings for Everyone [5]

Cloud

A small domain or private group of network which can be accessed amongst the authentic group members is known as cloud. Resources can be shared and services can be made available for the authentic group members in a cloud. Here an IP address is required to access the contents of cloud, but these IP's may not be available on internet. There is a concept of FOG, [8] which can work for a very small area in wireless sensor network WSN where communication can be made between devices with the help of Bluetooth or Wi-Fi i.e. wireless fidelity. Normally RFID i.e. radio frequency identification or NFC near field communication can be used in this area [2][12].

Wireless Sensor Network (WSN)

This is a type of network, which doesn't need internet connectivity on regular basis. Here the WSN device or sensor node is used for data acquisition and command. Here data is not directly transmitted to internet, but it is collected by one unit and that unit transfers the data. There can be even more number of hops required for controlling such WSN devices. [1][12][13]

Hardware - A node contains sensor, processing units, transceiver units and power supply. They comprise of multiple A/D converters for sensor interfacing and more modern sensor nodes have the ability to communicate using one frequency band making them more versatile.

Communication Stack - Nodes are deployed in adhoc way. It is required to design a suitable topology, routing and MAC layer for scalability and longevity of the deployed network. WSN nodes need to communicate among themselves to transmit data to base station.

Middleware - A mechanism to combine cyber infrastructure with a Service Oriented Architecture (SOA) and sensor networks to provide access to heterogeneous sensor resources in a deployment independent manner. A platform independent middleware is required for developing sensor applications, such as an Open Sensor Web Architecture (OSWA). [12][13]

Data aggregation - A method is required for extending the lifetime of the network as well as ensuring reliable data collected from sensors.

Internet of Things

Six layer architecture of IOT is as follows [12]

Coding Layer

Coding layer is the foundation of IOT which provides identification to the objects of interest. In this layer, each object is assigned a unique ID which makes it easy to discern the objects.

Perception Layer

This is the device layer of IOT which gives a physical meaning to each object. It consists of data sensors in different forms like RFID tags, IR sensors or other sensor networks which could sense the temperature, humidity, speed and location etc of the objects. This layer gathers the useful information of the objects from the sensor devices linked with them and converts the information into digital signals which is then passed onto the Network Layer for further action.\

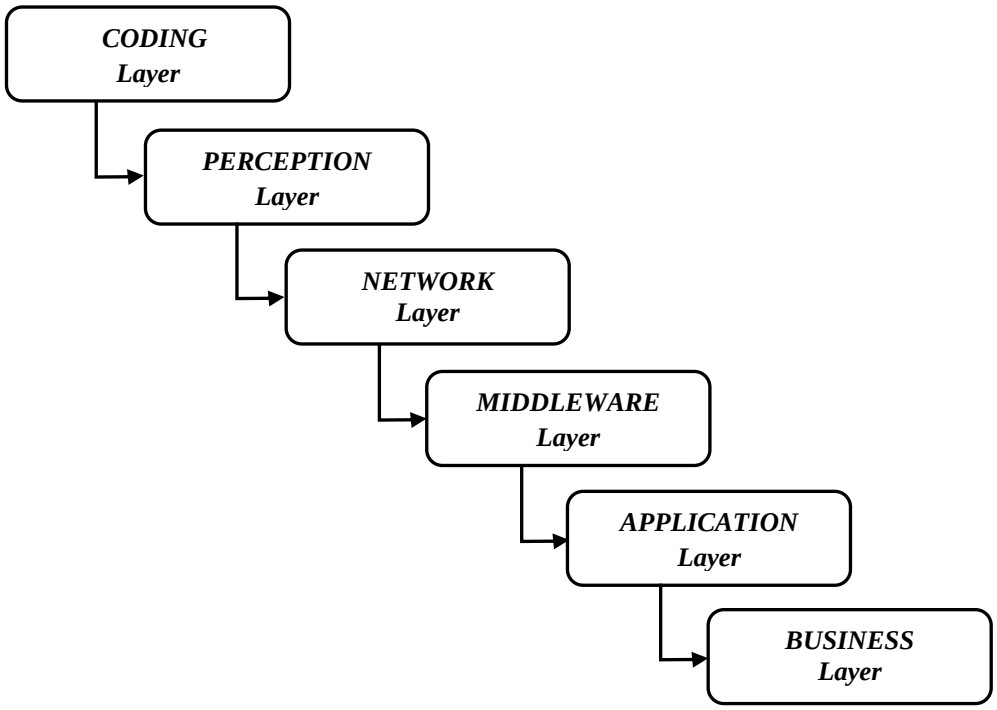

Figure 2: Six Layered Architecture of Internet of Things [12]

Network Layer

The purpose of this layer is receive the useful information in the form of digital signals from the Perception Layer and transmit it to the processing systems in the Middleware Layer through the transmission mediums likeWiFi, Bluetooth,WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc.

Middleware Layer

This layer processes the information received from the sensor devices. It includes the technologies like Cloud computing, Ubiquitous computing which ensures a direct access to the database to store all the necessary information in it. Using some Intelligent Processing Equipment, the information is processed and a fully automated action is taken based on the processed results of the information.[13]

Application Layer

This layer realizes the applications of IOT for all kinds of industry, based on the processed data. Because applications promote the development of IOT so this layer is very helpful in the large scale development of IOT network. The IOT related applications could be smart homes, smart transportation, smart planet etc.

Business Layer

This layer manages the applications and services of IOT and is responsible for all the research related to IOT. It generates different business models for effective business strategies.

SMART DEVICES

Smart Mobiles

An area in which there has been recent innovation is the capability for the remote provisioning of IOT devices. In some connected devices or equipment, the module with the SIM card needs to be inserted in the machine and hermetically sealed during the production process. Examples include tamper-proof security or alarm systems. Other pieces of connected equipment are located in remote or hazardous locations, such as weather, pipeline or geology sensors, or equipment in chemical plants, meaning it is difficult or impossible to access the module after deployment. To address these specific market segments, the mobile industry through the GSMA has produced an “Embedded SIM” specification to enable the remote ‘over the air’ provisioning and management of Embedded SIMs in such devices. The specification enables operators and their customers to activate, swap or change network subscriptions over-the-air without having to physically access the module containing the SIM..

GSM

Mobile networks already deliver connectivity to a broad range of devices, enabling the development of innovative new services and applications. This new wave of connectivity is going beyond tablets and laptops; to connected cars and buildings; TVs and game consoles; smart meters and traffic control; with the prospect of intelligently connecting almost anything and anyone. [14]

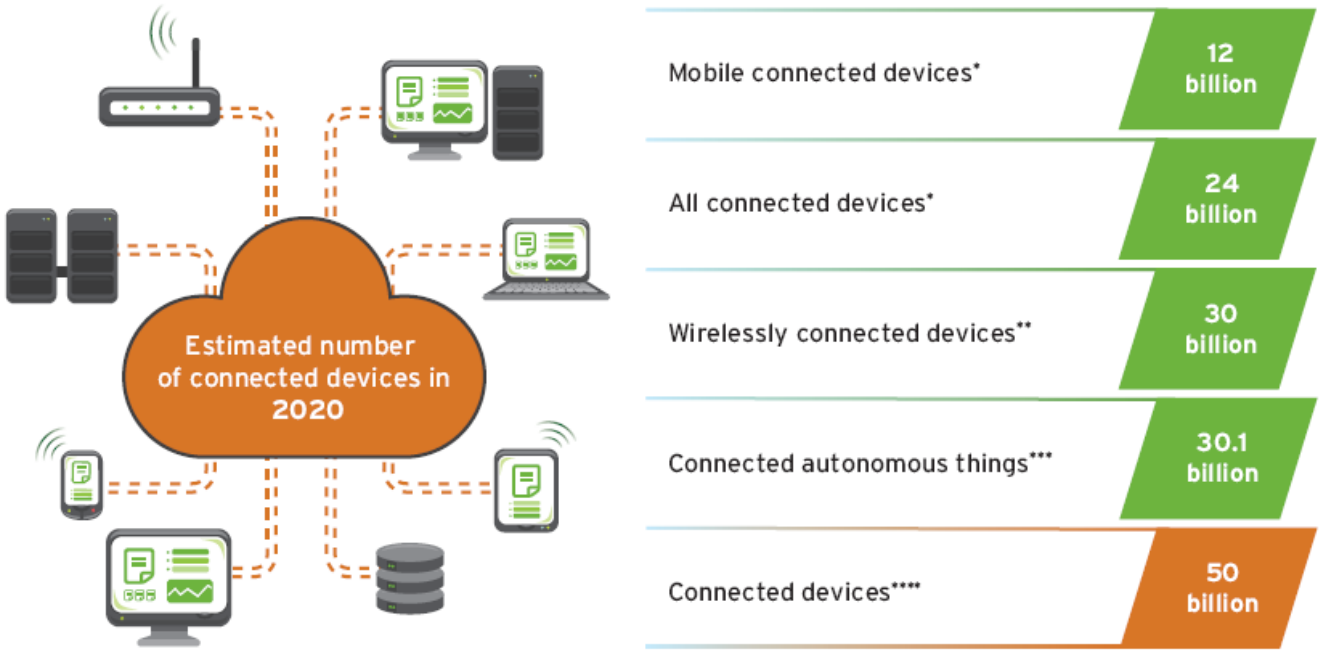

Figure 3: IOT Drivers: Exponential Growth of Smart Devices and Sensors [10]

RFID

Radio Frequency Identification (RFID) is a system that transmits the identity of an object or person wirelessly using radio waves in the form of a serial number. First use of RFID device was happened in II world war in Britain and it is used for Identify of Friend or Foe in 1948. Later RFID technology is founded at Auto-ID centre in MIT in the year 1999. RFID technology plays an important role in IOT for solving identification issues of objects around us in a cost effective manner [6]. The technology is classified into three categories based on the method of power supply provision in Tags: Active RFID, Passive RFID and Semi Passive RFID. The main components of RFID are tag, reader, antenna, access controller, software and server. It is more reliable, efficient, secured, inexpensive and accurate. RFID has an extensive range of wireless applications such as distribution, tracing, patient monitoring, military apps etc. The frequency ranges of RFID are (1) Low frequency (135 KHz or less) (2) High Frequency (13.56MHz) (3) Ultra-High Frequency (862MHz 928MHz) & (4) Microwave Frequency (2.4G, 5.80) [12]

SMART CITY

Internet of things is a recent concept that might invade almost all the objects of everyday life which will be equipped with micro-controllers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, becoming an integral part of the Internet.

Smart Parking

Crowd monitoring monitors pubic for emergency management; efficient use of public and retail spaces; workflow in commercial environments. Intelligent transportation through real-time traffic information and path optimisation [2]. Infrastructure monitoring sensors built into infrastructure to monitor structural fatigue and other maintenance; accident monitoring for incident management and emergency response coordination

Smart Health

Ways of using energy more rationally in the home by cooperating energy-aware household devices and “ambient assisted living” [2] aimed at unobtrusively supporting elderly people in their everyday lives. Patient monitoring, personnel monitoring, disease spread modelling and containment - real-time health status [8] and predictive information to assist practitioners in the field, or policy decisions in pandemic scenarios. Water quality, leakage, usage, distribution, waste management

Smart Market

Concerning the financial dimension, a clear business model is still lacking, although some initiative to fill this gap has been recently undertaken [2]. The situation is worsened by the adverse global economic situation, which has determined a general shrinking of investments on public services. This situation prevents the potentially huge Smart City market [4] from becoming reality. A possible way out of this impasse is to first develop those services that conjugate social utility with very clear return on investment, such as smart parking and smart buildings, and will hence act as catalyzers for the other added-value services.

Smart Vehicles

Navigation devices receive remote road traffic messages. This category includes cars communicating with each other to improve road safety. Tire pressure sensors that send their readings to the car’s [2]. Even though camera-based traffic monitoring systems are already available and deployed in many cities, low-power widespread communication can provide a denser source of information. Traffic monitoring may be realized by using the sensing capabilities and GPS installed on modern vehicles, but also adopting a combination of air quality and acoustic sensors along a given road. This information is of great importance for city authorities and citizens: for the former to discipline traffic and to send officers where needed, for the latter to plan in advance the route to reach the office or to better schedule a shopping trip to the city centre.

Smart Buildings

Emergency services, defence remote personnel monitoring (health, location); resource management and distribution, response planning; sensors built into building infrastructure to guide first responders in emergencies or disaster scenarios. The urban IOT [2] may provide a distributed database of building structural integrity measurements, collected by suitable sensors located in the buildings, such as vibration and deformation sensors to monitor the building stress, atmospheric agent sensors in the surrounding areas to monitor pollution levels, and temperature and humidity sensors [4] to have a complete characterization of the environmental conditions.

Smart Consumer Electronics

Examples of the second category include a virtual lost-property office, where a mobile infrastructure would pick up feeble cries for help from lost things, or property insurance where the risk can often be better assessed (and possibly even reduced) if the insured item is “smart”. This might be a dynamic car insurance that makes your premium dependent not only on how far you drive (“pay as you drive”), but also on the individual risk. Speeding, dangerous overtaking and driving in hazardous conditions would then have a direct impact on the insurance costs. In general, we can expect the Internet of Things to give rise to increasing numbers of hybrid products that provide both, a conventional physical function and information services.

Smart Energy

An urban IOT may provide a service to monitor the energy consumption of the whole city, thus enabling authorities and citizens to get a clear and detailed view of the amount of energy required by the different services (public lighting, transportation, traffic lights, control cameras, heating/cooling of public buildings, and so on). In turn, this will make it possible to identify the main energy consumption sources and to set priorities in order to optimize their behaviour. This goes in the direction indicated by the European directive for energy efficiency improvement [4] in the next years. In order to obtain such a service, power draw monitoring devices must be integrated with the power grid in the city. In addition, it will also be possible to enhance these services with active functionalities to control local power production structures (e.g., photovoltaic panels).

SMART BUSINESS

IOT has an impact on each and every type of business. We have already discussed the Internet of Things and types of devices those connected to a company's systems. Internet of Things helps in gaining efficiencies, harnessing intelligence from a large range of sensors improving operations and increasing consumer satisfaction. For public IOT will improve health care, transportation and safety. In case of ITC, IOT will make communication faster [2].

The Cs of IOT

Communication: IOT communicates information to people and systems, such as state and health of equipment and data from sensors that can monitor a person's vital signs.

Control and Automation: In this world of connectivity, a business could be controlled remotely from a distant place.

Climate of environment: IOT can be used for many consumer applications like car parking, etc.

Cost Savings: IOT helps an organization in saving money by minimizing equipment failure and allowing the business to perform planned maintenance. [2]

Smart Retailing and Supply-chain Management.

IT with RFID provides many advantages to retailers. With RFID [12] equipped products, a retailer can easily track the stocks and detect shoplifting. It can keep a track of all the items in a store and to prevent them from going out-of-stock, it places an order automatically. Moreover the retailer can even generate the sales chart and graphs for effective strategies.

Smart Agriculture.

It will monitor Soil nutrition, Light, Humidity etc and improve the green housing experience by automatic adjustment of temperature to maximize the production. Accurate watering and fertilization will help improving the water quality and saving the fertilizers respectively [12].

CHALLENGES

Privacy

Any individual has right to speak, connect, and choose in meaningful ways to express his or her thoughts. These rights and expectations are sometimes framed in terms of ethical data handling, which emphasizes the importance of respecting an individual's expectations of privacy and the fair use of their data. The Internet of Things can challenge these traditional expectations of privacy. [11] IOT often refers to a large network of sensor-enabled devices designed to collect data about their environment, which frequently includes data related to people. This data presumably provides a benefit to the device's owner, but frequently to the device's manufacturer or supplier as well. IOT data collection and use becomes a privacy consideration when the individuals who are observed by IOT devices have different privacy expectations regarding the scope and use of that data than those of the data collector.

When individual data streams are combined or correlated, often a more invasive digital portrait is painted of the individual than can be realized from an individual IOT data stream.

For example, a user's Internet-enabled toothbrush might capture and transmit innocuous data about a person's tooth-brushing habits. But if the user's refrigerator reports the inventory of the foods he eats and his fitness-tracking device reports his activity data, the combination of these data streams paint a much more detailed and private description of the person's overall health. This data-aggregation effect can be particularly potent with respect to IOT devices because many produce additional metadata like time stamps and geo location information, which adds even more specificity about the user. [7]

In other situations, the user might not be aware that an IOT device is collecting data about the individual and potentially sharing it with third parties. This type of data collection is becoming more prevalent in consumer devices like smart televisions and video game devices. These kinds of products have voice recognition or vision features that continuously listen to conversations or watch for activity in a room and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. A person might be in the presence of these kinds of devices without knowing their conversation or activities are being monitored and their data captured. These kinds of features may provide a benefit to an informed user, but can pose a privacy problem for those who are unaware of the presence of the devices and have no meaningful influence over how that collected information is used.

Independent of whether the user is aware of and consents to having their IOT data collected and analyzed, these situations highlight the value of these personalized data streams to companies and organizations seeking to collect and capitalize on IOT information. The demand for this information exposes

the legal and regulatory challenges facing data protection and privacy laws. [7]

These kinds of privacy problems are critical to address because they have implications on our basic rights and our collective ability to trust the Internet. From a broad perspective, people recognize their privacy is intrinsically valuable, and they have expectations of what data can be collected about them and how other parties can use that data. [9] This general notion about privacy holds true for data collected by Internet of Things devices, but those devices can undermine the user's ability to express and enforce privacy preferences. If users lose confidence in the Internet because their privacy preferences aren't being respected in the Internet of Things, then the greater value of the Internet may be diminished. [11]

Security

We can't trust on Internet, that we or our data are secure. We need to protect data on the internet. The Internet of Things is not a different concept in this regard, and security in IOT is attached to the ability of users to believe in their environment. If users don't believe the connected devices and their information to be secured from misuse or harm, this may result in a reluctance to use the Internet. [11] Therefore, security in IOT products and services should be considered a top priority for the sector. As we increasingly connect devices to the Internet, new opportunities to exploit potential security vulnerabilities grow. Poorly secured IOT devices could serve as entry points for cyber attack by allowing malicious individuals to re-program a device or cause it to malfunction. Poorly designed devices can expose user data to theft by leaving data streams inadequately protected. Failing or malfunctioning devices also can create security vulnerabilities. These problems are just as large or larger for the small, cheap, and ubiquitous smart devices in the Internet of Things as they are for the computers that have traditionally been the endpoints of Internet connectivity. [11] Competitive cost and technical constraints on IOT devices challenge manufacturers to adequately design security features into these devices, potentially creating security and long-term maintainability vulnerabilities greater than their traditional computer counterparts. Along with potential security design deficiencies, the sheer increase in the number and nature of IOT devices could increase the opportunities of attack. When coupled with the highly interconnected nature of IOT devices, every poorly secured device that is connected online potentially affects the security and resilience of the Internet *globally*, not just locally. For example, an unprotected refrigerator or television in the US that is infected with malware might send thousands of harmful spam emails to recipients worldwide using the owner's home Wi-Fi Internet connection. [7]

To complicate matters, our ability to function in our daily activities without using devices or systems that are Internet-enabled is likely to decrease in a hyper connected world. In fact, it is increasingly difficult to purchase some devices that are *not* Internet-connected because certain vendors only make connected products. [11] Day by day, we become more connected and dependent on IOT devices for essential services, and we need the devices to be secure, while recognizing that no device can be absolutely secure. This increasing level of dependence on IOT devices and the Internet services they interact with also increases the pathways for wrongdoers to gain access to devices. Perhaps we could unplug our Internet-connected TVs if they get compromised in a cyber attack, but we can't so easily turn off a smart utility power meter or a traffic control system or a person's implanted pacemaker if they fall victim to malicious behaviour. [9] This is why security of IOT devices and services is a major discussion point and should be considered a critical issue. We increasingly depend on these devices for essential services, and their behaviour may have global reach and impact. [7]

CONCLUSION

The Internet of Things promises to deliver a step change in individuals' quality of life and enterprises' productivity. Through a widely distributed, locally intelligent network of smart devices, the IOT has the potential to enable extensions and enhancements to fundamental services in transportation, logistics, security, utilities, education, healthcare and other areas, while providing a new ecosystem for application development. A concerted effort is required to move the industry beyond the early stages of market development towards maturity, driven by common understanding of the distinct nature of the opportunity. This market has distinct characteristics in the areas of service distribution, business and charging models, capabilities required to deliver IOT services, and the differing demands these services will place on mobile networks. It is hoped that a common understanding of the characteristics of IOT will enable industry stakeholders to collaborate more effectively in order to propel the market forward for the benefit of consumers and society. This paper throws light to the need for a detailed analysis of privacy threats and challenges in the Internet of Things. It provided a formal basis for discussing privacy in the IOT by concisely framing our notion of privacy and security. It was then acknowledged that the Internet of Things is constantly evolving and cannot be reduced to the sum of the technologies it builds on. The threats of privacy-violating interactions and presentations & attacks on information linkage arise later in the IOT were discussed. It also discussed the technical challenges in context of threat to privacy and security of an individual.

REFERENCES

[1] Friedemann Mattern and Christian Floerkemeier, "From the Internet of Computers to the Internet of Things", Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich

[2] Team Lopez (2013), "An Introduction of Internet of Things (IOT)", part 1 of the IOT series, Lopez Research LLC.

[3] Jayavardhana Gubbi, Rajkumar Buyya, Slaven

Marusic,a Marimuthu Palaniswamia, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions"

[4] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, Michele Zorzi, "Internet of Things for Smart Cities", paper published in IEEE Internet of Things Journal, vol. 1, no. 1, year 2014.

[5] White paper developed in collaboration with Global Strategy and Business Development, Freescale and Emerging Technologies, ARM, "What the Internet of Things (IOT) Needs to Become a Reality", published for FreeScale & Arm, bearing Document Number: INTOTHNGSWP REV 2, May 2014

[6] Madakam, S., Ramaswamy, R. and Tripathi, S.,"Internet of Things (IOT): A Literature Review" published in Journal of Computer and Communications, 3, 164-173. (2015)

[7] Editor Carolyn Marsan and Internet Society Community Members, "The Internet of Things: An Overview", published by Internet Society, October 2015

[8] Moeen Hassanalieragh, Alex Page, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo Mateos, Burak Kantarci, Silvana Andreescu, "Health Monitoring and Management Using Internet-of-Things (IOT) Sensing with Cloud-based Processing: Opportunities and Challenges", published in 2015 IEEE International Conference on Services Computing for IEE Computer Society, bearing no. 978-1-4673-7281-7/15 2015 IEEE DOI 10.1109/SCC.2015.47, pp 285-292

[9] Jan Henrik Ziegeldorf, Oscar Garcia Morchon and Klaus Wehrle, "Privacy in the Internet of Things: Threats and Challenges", Security and Communication Networks 2013, DOI: 10.1002/sec.795, John Wiley & Sons, Ltd.

[10] Aala Santhosh Reddy, Kevin Benedict, Harleen Bhatia, "Reaping the Benefits of the Internet of Things", published by Cognizant report May 2014

[11] John A. Stankovic, "Research Directions for the Internet of Things", published for IEEE, 2014

[12] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal, "A Review on Internet of Things (IOT)", published in International Journal of Computer Applications bearing no. 0975 8887, Volume 113 - No. 1, March 2015

[13] Pedro Castillejo, Jose-Fernan Martinez, Lourdes Lopez, and Gregorio Rubio, "An Internet of Things Approach for Managing Smart Services Provided by Wearable Devices", published in Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, Volume 2013, Article ID 190813,