CHAPTER 1

INTRODUCTION

The Internet of Things (IoT) is the network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more-direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020. British entrepreneur Kevin Ashton first coined the term in 1999 while working at Auto-ID Labs (originally called Auto-ID centers - referring to a global network of Radio-frequency identification (RFID) connected objects). Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a Smart Grid, and expanding to the areas such as smart cities. "Things," in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring or field operation devices that assist firefighters in search and rescue operations. These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. Current market examples include smart thermostat systems and washer/dryers that use Wi-Fi for remote monitoring. Besides the plethora

of new application areas for Internet connected automation to expand into, IoT is also expected to generate large amounts of data from diverse locations that is aggregated very quickly, thereby increasing the need to better index, store and process such data. IoT is one of the platforms of today's Smart City and Smart Energy Management Systems.

Anyone who says that the Internet has fundamentally changed society may be right, but at the same time, the greatest transformation actually still lies ahead of us. Several new technologies are now converging in a way that means the Internet is on the brink of a substantial expansion as objects large and small get connected and assume their own web identity. Following on from the Internet of computers, when our servers and personal computers were connected to a global network, and the Internet of mobile telephones, when it was the turn of telephones and other mobile units, the next phase of development is the Internet of things, when more or less anything will be connected and managed in the virtual world. This revolution will be the Net's largest enlargement ever and will have sweeping effects on every industry — and all of our everyday lives. Smart connectivity with existing networks and context-aware computation using network resources is an indispensable part of IoT. With the growing presence of Wi-Fi and 4G-LTE wireless Internet access, the evolution towards ubiquitous information and communication networks is already evident. However, for the Internet of Things vision to successfully emerge, the computing paradigm will need to go beyond traditional mobile computing scenarios that use smart phones and portables, and evolve into connecting everyday existing objects and embedding intelligence into our environment. For technology to disappear from the consciousness of the user, the Internet of Things demands: a shared understanding of the situation of its users and their appliances, software architectures and pervasive communication networks to process and convey the contextual information to where it is relevant, and the analytics tools in the Internet of Things that aim for autonomous and smart behavior. With these three fundamental grounds in place, smart connectivity and context-aware computation can be accomplished. A radical evolution of the current Internet into a Network of interconnected objects that not only harvests information from the environment (sensing) and interacts with the physical world (actuation/ command/control), but also uses existing Internet standards to provide services for information transfer, analytics, applications, and

communications. Fueled by the prevalence of devices enabled by open wireless technology such as Bluetooth, radio frequency identification (RFID), Wi-Fi, and telephonic data services as well as embedded sensor and actuator nodes, IoT has stepped out of its infancy and is on the verge of transforming the current static Internet into a fully integrated Future Internet. The Internet revolution led to the interconnection between people at an unprecedented scale and pace. The next revolution will be the interconnection between objects to create a smart environment. Only in 2011 did the number of interconnected devices on the planet overtake the actual number of people. Currently there are 9 billion interconnected devices and it is expected to reach 24 billion devices by 2020. According to the GSMA, this amounts to $1.3 trillion revenue opportunities for mobile network operators alone spanning vertical segments such as health, automotive, utilities and consumer electronics.

DEFINITION OF INTERNET OF THINGS

Although the term “Internet of Things” first appeared in the literature in 2005,20 there is still no widely accepted definition. One participant described the IoT as the connection of “physical objects to the Internet and to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing.” Another participant described it as including “embedded intelligence” in individual items that can detect changes in their physical state.23 Yet another participant, noting the lack of an agreed-upon definition of the IoT, observed, “[w]hat all definitions of IoT have in common is that they focus on how computers, sensors, and objects interact with one another and process data.”The IoT includes consumer-facing devices, as well as products and services that are not consumer-facing, such as devices designed for businesses to enable automated communications between machines. For example, the term IoT can include the type of Radio Frequency Identification (“RFID”) tags that businesses place on products in stores to monitor inventory; sensor networks to monitor electricity use in hotels; and Internet-connected jet engines and drills on oil rigs. Moreover, the “things” in the IoT generally do not include desktop or laptop computers and their close analogs, such as smartphones and tablets, although these devices are often employed to control or communicate with other “things.”

“Today computers—and, therefore, the Internet—are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes(a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings—by typing, pressing a record button, taking a digital picture, or scanning a bar code. Conventional diagrams of the Internet … leave out the most numerous and important routers of all - people. The problem is, people have limited time, attention and accuracy—all of which means they are not very good at capturing data about things in the real world. And that's a big deal. We're physical, and so is our environment.

You can't eat bits, burn them to stay warm or put them in your gas tank. Ideas and information are important, but things matter much more. Yet today's information technology is so dependent on data originated by people that our computers know more about ideas than things. If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so. “ —Kevin Ashton, "That 'Internet of Things' Thing", RFID Journal, July 22, 2009 “

Things are active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information sensed about the environment, while reacting autonomously to the real/physical world events and influencing it by running processes that trigger actions and create services with or without direct human intervention.” —Cluster of European research projects on the Internet of Things “The Internet of Things represents an evolution in which objects are capable of interacting with other objects. Hospitals can monitor and regulate pacemakers long distance, factories can automatically address production line issues and hotels can adjust temperature and lighting according to a guest's preferences, to name just a few examples.” – IBM

ARCHITECTURE OF IOT

Architecture of internet of Things contains basically 4 layers:

- Application Layer
- Gateway and the network layer
- Management Service layer
- Sensor layer

1.) Application Layer:

- Lowest Abstraction Layer
- With sensors we are creating digital nervous system.
- Incorporated to measure physical quantities
- Interconnects the physical and digital world
- Collects and process the real time information

2.) Gateway and The Network Layer:

- Robust and High performance network infrastructure
- Supports the communication requirements for latency, bandwidth or security
- Allows multiple organizations to share and use the same network independently

3.) Management Layer:

- Capturing of periodic sensory data
- Data Analytics (Extracts relevant information from massive amount of raw data)
- Streaming Analytics (Process real time data)
- Ensures security and privacy of data.

4.) Sensor Layer:

- Provides a user interface for using IoT
- Different applications for various sectors like Transportation, Healthcare, Agriculture, Supply chains, Government, Retail etc.

CHAPTER 2

BACKGROUND

Technology is quickly changing the way we interact with the world around us. Today, companies are developing products for the consumer market that would have been unimaginable a decade ago: Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. These are all examples of the Internet of Things ("IoT"), an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people. The IoT explosion is already around us, in the form of wearable computers, smart health trackers, connected smoke detectors and light bulbs, and essentially any other Internet-connected device that isn't a mobile phone, tablet, or traditional computer. Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people. Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion. Some estimate that by 2020, 90% of consumer cars will have an Internet connection, up from less than 10 percent in 2013. Three and one-half billion sensors already are in the marketplace, 4 and some experts expect that number to increase to trillions within the next decade. All of these connected machines mean much more data will be generated: globally, by 2018, mobile data traffic will exceed fifteen Exabyte's – about 15 quintillion bytes – each month. By comparison, according to one estimate, an Exabyte of storage could contain 50,000 years' worth of DVD-quality video. These new developments are expected to bring enormous benefits to consumers. Connected health devices will allow consumers with serious health conditions to work with their physicians to manage their diseases. Home automation systems will enable consumers to turn off the burglar alarm, play music, and warm up dinner right before they get home from work. Connected cars will notify first responders in the event of an accident. And the Internet of Things may bring benefits that we cannot predict. However, these connected devices also will collect,

transmit, store, and potentially share vast amounts of consumer data, some of it highly personal. Given the rise in the number and types of connected devices already or soon to be on the market, the Federal Trade Commission ("FTC" or "Commission") announced in April 2013 that it would host a workshop on the privacy and security issues associated with such devices and requested public input about the issues to consider. In response to the request for comment, staff received twenty-nine public comments from a variety of consumer advocacy groups, academics, and industry representatives. The workshop – titled The Internet of Things: Privacy and Security in a Connected World – took place on November 19, 2013, and featured panels of academics, researchers, consumer advocates, and representatives from government and industry. The workshop consisted of four panels, each of which focused on a different aspect of the IoT. The first panel, "The Smart Home, "looked at an array of connected devices, such as home automation systems and smart appliances. The second panel, "Connected Health and Fitness,"14 examined the growth of increasingly connected medical devices and health and fitness products, ranging from casual wearable fitness devices to connected insulin pumps. The third panel, "Connected Cars, discussed the different technologies involved with connected cars, including Event Data Recorders ("EDRs") and other vehicle "telematics," a term that refers to data collection, transmission, and processing technologies for use in vehicles. Finally, the fourth panel, "Privacy and Security in a Connected World, "discussed the broader privacy and security issues raised by the IoT. Following the workshop, the Commission invited comments on the issues raised by the panels. In response, staff received seventeen public comments from private citizens, trade organizations, and privacy advocates. This report summarizes the workshop and provides staff's recommendations in this area. Section II of this report discusses how we define the "Internet of Things." Section III describes some of the benefits and risks of the new technologies that are part of the IoT phenomenon. Section IV examines the application of existing privacy principles to these new technologies, and Section V addresses whether legislation would be appropriate in this area. Sections IV and V begin by discussing the views of written commenters and workshop speakers (collectively, "participants"), and then set forth staff recommendations. These recommendations focus on the types of products and services consumers are likely to encounter today and in the foreseeable future. We look forward to continuing to explore privacy issues as new IoT technologies come to market.

CHAPTER 3

IOT TECHNOLOGIES

IOT TECHNOLOGIES

The Internet of Things [22]was initially inspired by members of the RFID community, who referred to the possibility of discovering information about a tagged object by browsing an internet address or database entry that corresponds to a particular RFID or Near Field Communication technologies[23]. In the research paper “Research and application on the smart home based on component technologies and Internet of Things”, the included key technologies of IoT are RFID, the sensor technology, nano technology and intelligence embedded technology. Among them, RFID is the foundation and networking core of the construction of Internet of Things [24]. The Internet of Things (IoT) enabled users to bring physical objects into the sphere of cyber world. This was made possible by different tagging technologies like NFC, RFID and 2D barcode which allowed physical objects to be identified and referred over the internet [25]. IoT, which is integrated with Sensor Technology and Radio Frequency Technology, is the ubiquitous network based on the omnipresent hardware resources of Internet, is the Internet contents objects together. It is also a new wave of IT industry since the application of computing fields, communication network and global roaming technology had been applied. It involves in addition to sophisticated technologies of computer and communication network outside, still including many new supporting technologies of Internet of Things, such as collecting Information Technology, Remote Communication Technology, Remote Information Transmission Technology, Sea Measures Information Intelligence Analyzes and Controlling Technology etc.[26]

1) Radio Frequency Identification (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 2nd world war in Brittan and it is used for Identify of Friend or Foe in 1948. Later RFID technology is founded at Auto-ID center 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 [28]. 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[29].

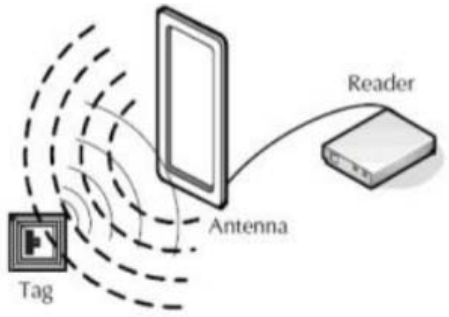

Fig 3.1 RFID

2.) Internet Protocol (IP)

Internet Protocol (IP) is the primary network protocol used on the Internet, developed in 1970s. IP is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. The two versions of Internet Protocol (IP) are in use: IPv4 and IPv6. Each version defines an IP address differently. Because of its prevalence, the generic term IP address typically still refers to the addresses defined by IPv4. There are five classes of available IP ranges in IPv4: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. The actual protocol provides for 4.3 billion IPv4 addresses while the IPv6 will significantly augment the availability to 85,000 trillion addresses . IPv6 is the 21st century Internet Protocol. This supports around for 2128 addresses.

3.) Electronic Product Code (EPC)

Internet Electronic Product Code (EPC) is a 64 bit or 98 bit code electronically recorded on an RFID tag and intended to design an improvement in the EPC barcode system. EPC code can store information about the type of EPC, unique serial number

of product, its specifications, manufacturer information etc. EPC was developed by Auto-ID center in MIT in 1999. EPCglobal Organization [Wikipedia, “EPCglobal”, 2010] which is responsible for standardization of Electronic Product Code (EPC) technology, created EPCglobal Network [Wikipedia, “EPCglobal Network”, 2010] for sharing RFID information. It has four components namely Object Naming Service (ONS), EPC Discovery Service (EPCDS), EPC Information Services (EPCIS) and EPC Security Services (EPCSS).

4.) Barcode

Barcode is just a different way of encoding numbers and letters by using combination of bars and spaces of varying width. Behind Bars serves its original intent to be descriptive but is not critical. In The Bar Code Book, Palmer (1995) acknowledges that there are alternative methods of data entry techniques. Quick Response (QR) Codes the trademark for a type of matrix barcode first designed for the automotive industry in Japan. Bar codes are optical machine readable labels attached to items that record information related to the item. Recently, the QR Code system has become popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard. There are 3 types of barcodes of Alpha Numeric, Numeric and 2 Dimensional. Barcodes are designed to be machine readable. Usually they are read by laser scanners, they can also be read using a cameras.

5.) Wireless Fidelity (Wi-Fi)

Wireless Fidelity (Wi-Fi) is a networking technology that allows computers and other devices to communicate over a wireless signal. Vic Hayes has been named as father of Wireless Fidelity. The precursor to Wi-Fi was invented in 1991 by NCR Corporation in Nieuwege in the Netherland. The first wireless products were brought on the market under the name WaveLAN with speeds of 1 Mbps to 2 Mbps. Today, there are nearly pervasive Wi-Fi that delivers the high speed Wireless Local Area Network (WLAN) connectivity to millions of offices, homes, and public locations such as hotels, cafes, and airports. The integration of Wi-Fi into notebooks, handhelds and Consumer Electronics (CE) devices has accelerated the adoption of Wi-Fi to the point where it is nearly a default in these devices [32]. Technology contains any type of WLAN product support any of the IEEE 802.11 together with dual-band, 802.11a,

802.11b, 802.11g and International Journal of Computer Applications (0975 – 8887) Volume 169 – No.4, July 2017 13 802.11n. Nowadays entire cities are becoming Wi-Fi corridors through wireless APs.

6.) Bluetooth

Bluetooth wireless technology is an inexpensive, short-range radio technology that eliminates the need for proprietary cabling between devices such as notebook PCs, handheld PCs, PDAs, cameras, and printers and effective range of 10 - 100 meters. And generally communicate at less than 1 Mbps and Bluetooth uses specification of IEEE 802.15.1 standard[33]. At first in 1994 Ericson Mobile Communication company started project named “Bluetooth”. It is used for creation of Personal Area Networks (PAN). A set of Bluetooth devices sharing a common channel for communication is called Piconet. This Piconet is capable of 2 - 8 devices at a time for data sharing, and that data may be text, picture, video and sound. The Bluetooth Special Interest Group comprises more than 1000 companies with Intel, Cisco, HP, Aruba, Intel, Ericson, IBM, Motorola and Toshiba.

7.) ZigBee

ZigBee is one of the protocols developed for enhancing the features of wireless sensor networks. ZigBee technology is created by the ZigBee Alliance which is founded in the year 2001. Characteristics of ZigBee are low cost, low data rate, relatively short transmission range, scalability, reliability, flexible protocol design. It is a low power wireless network protocol based on the IEEE 802.15.4 standard . ZigBee has range of around 100 meters and a bandwidth of 250 kbps and the topologies that it works are star, cluster tree and mesh. It is widely used in home automation, digital agriculture, industrial controls, medical monitoring & power systems.

8.) Near Filed Communication (NFC)

Near Field Communication (NFC) is a set of short-range wireless technology at 13.56 MHz, typically requiring a distance of 4 cm. NFC technology makes life easier and more convenient for consumers around the world by making it simpler to make transactions, exchange digital content, and connect electronic devices with a touch. Allows intuitive initialization of wireless networks and NFC is complementary to

Bluetooth and 802.11 with their long distance capabilities at a distance circa up to 10 cm. It also works in dirty environment, does not require line of sight, easy and simple connection method. It is first developed by Philips and Sony companies. Data exchange rate now days approximately 424 kbps. Power consumption during data reading in NFC is under 15ma.

9.) Actuators

An actuator is something that converts energy into motion, which means actuators drive motions into mechanical systems. It takes hydraulic fluid, electric current or some other source of power. Actuators can create a linear motion, rotary motion or oscillatory motion. Cover short distances, typically up to 30 feet and generally communicate at less than 1 Mbps. Actuators typically are used in manufacturing or industrial applications. There are three types of actuators are Electrical: ac and dc motors, stepper motors, solenoids Hydraulic: use hydraulic fluid to actuate motion Pneumatic: use compressed air to actuate motion. All these three types of actuators are very much in use today. Among these, electric actuators are the most commonly used type. Hydraulic and pneumatic systems allow for increased force and torque from smaller motor.

10.) Wireless Sensor Networks (WSN)

A WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations (Wikipedia). Formed by hundreds or thousands of motes that communicate with each other and pass data along from one to another. A wireless sensor network is an important element in IoT paradigm. Sensor nodes may not have global ID because of the large amount of overhead and large number of sensors. WSN based on IoT has received remarkable attention in many areas, such as military, homeland security, healthcare, precision agriculture monitoring, manufacturing, habitat monitoring, forest fire and flood detection and so on . Sensors mounted to a patient’s body are monitoring the responses to the medication, so that doctors can measure the effects of the medicines[35] .

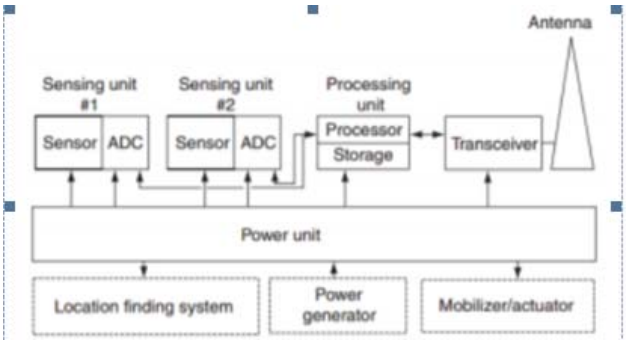

Fig 3.2 A typical sensing node

11.) Artificial Intelligence (AI)

Artificial Intelligence refers to electronic environments that are sensitive and responsive to the presence of people. In an ambient intelligence world, devices work in concert to support people in carrying out their everyday life activities in easy, natural way using Information and Intelligence that is hidden in the network connected devices. It is characterized by the following systems of characteristics Embedded: Many Net- worked devices are integrated in to the environment Context Aware: These devices can recognize you and your situational context Personalized: They can be tailored to your needs Adaptive: They can change in response to you Anticipatory: They can anticipate your desires without conscious mediation.

CHAPTER 4

ARCHITECTURE OF IOT

More than 25 Billion things are expected to be connected by 2020 which is a huge number so the existing architecture of Internet with TCP/IP protocols, adopted in 1980, cannot handle a network as big as IoT which caused a need for a new open architecture that could address various security and Quality of Service (QoS) issues as well as it could support the existing network applications using open protocols. Without a proper privacy assurance, IoT is not likely to be adopted by many. Therefore protection of data and privacy of users are key challenges for IoT. For further development of IoT, a number of multi-layered security architectures are proposed i.e. a three key level architecture of IoT while described a four key level architecture. proposed a five layered architecture using the best features of the architectures of Internet and Telecommunication management networks based on TCP/IP and TMN models respectively. Similarly a six-layered architecture was also proposed based on the network hierarchical structure. So, generally it's divided into six layers as shown in the Fig. 1 . The six layers of IoT are described below:

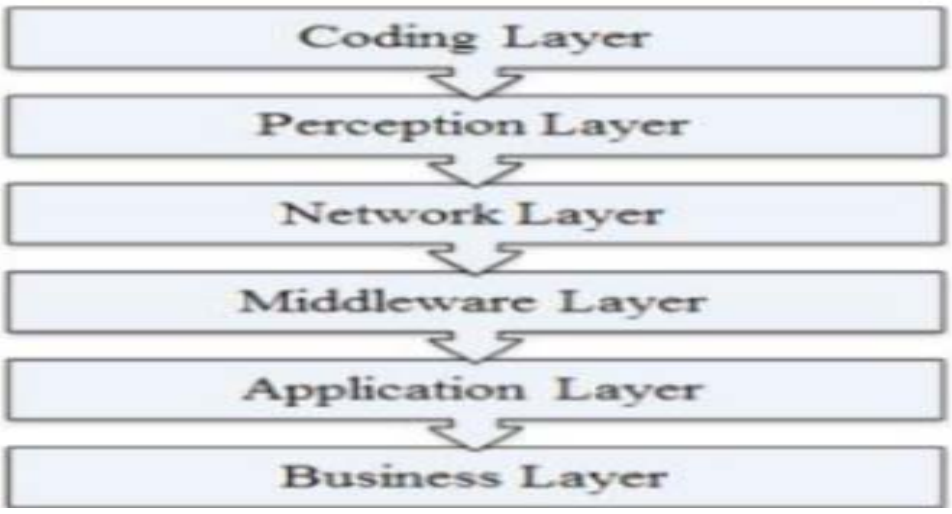

Fig 4.1 Six-Layered Architecture of IoT

3.1 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[18].

3.2 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[19] 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.

3.3 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 like Wi-Fi, Bluetooth, WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc.

3.4 Middleware Layer

This layer processes the information received from the sensor devices[2] . 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.

3.5 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[21]. The IoT related applications could be smart homes, smart transportation, smart planet etc.

3.6 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 [1].

From a technical point of view, the Internet of Things is not the result of a single novel technology; instead, several complementary technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world. These capabilities include:

- Communication and cooperation: Objects have the ability to network with Internet resources or even with each other, to make use of data and services and update their state. Wireless technologies such as GSM and UMTS, Wi-Fi, Bluetooth, ZigBee and various other wireless networking standards currently under development, particularly those relating to Wireless Personal Area Networks (WPANs), are of primary relevance here.

- Addressability: Within an Internet of Things, objects can be located and addressed via discovery, look-up or name services, and hence remotely interrogated or configured.

- Identification: Objects are uniquely identifiable. RFID, NFC (Near Field Communication) and optically readable bar codes are examples of technologies with which even passive objects which do not have built-in energy resources can be identified (with the aid of a “mediator” such as an RFID reader or mobile phone). Identification enables objects to be linked to information associated with the particular object and that can be retrieved from a server, provided the mediator is connected to the network

- Sensing: Objects collect information about their surroundings with sensors, record it, forward it or react directly to it.

- Actuation: Objects contain actuators to manipulate their environment (for example by converting electrical signals into mechanical movement). Such actuators can be

used to remotely control real world processes via the Internet. International Research Journal of Engineering and Technology (IRJET)

- Embedded information processing: Smart objects feature a processor or microcontroller, plus storage capacity. These resources can be used, for example, to process and interpret sensor information, or to give products a “memory” of how they have been used.

- Localization: Smart things are aware of their physical location, or can be located. GPS or the mobile phone network are suitable technologies to achieve this, as well as ultrasound time measurements, UWB (Ultra-Wide Band), radio beacons (e.g. neighboring WLAN base stations or RFID readers with known coordinates) and optical technologies.

- User interfaces: Smart objects can communicate with people in an appropriate manner (either directly or indirectly, for example via a smartphone). Innovative interaction paradigms are relevant here, such as tangible user interfaces, flexible polymer-based displays and voice, image or gesture recognition methods . The smartphone as a mediator between people, things and the Internet . Most specific applications only need a subset of these capabilities, particularly since implementing all of them is often expensive and requires significant technical effort. Logistics applications, for example, are currently concentrating on the approximate localization (i.e. the position of the last read point) and relatively low-cost identification of objects using RFID or bar codes. Sensor data (e.g. to monitor cool chains) or embedded processors are limited to those logistics applications where such information is essential such as the temperature-controlled transport of vaccines. Forerunners of communicating everyday objects are already apparent, particularly in connection with RFID – for example the short-range communication of key cards with the doors of hotel rooms, or ski passes that talk to lift turnstiles. More futuristic scenarios include a smart playing card table, where the course of play is monitored using RFID-equipped playing cards. However, all of these applications still involve dedicated systems in a local deployment; we are not talking about an “Internet” in this ensue of an open, scalable and standardized system .

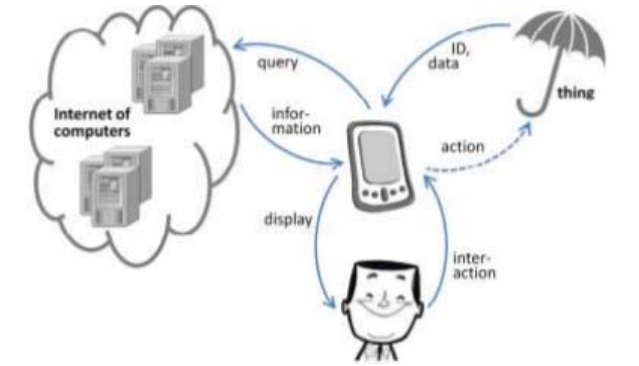

Fig 4.2 The Smartphone as a mediator between people, things and the Internet

CHAPTER 5

CHALLENGES IN IOT

We address the key challenges for IoT from several viewpoints, namely: technical, security, privacy, and trust, societal, business challenges, and challenges specifically important for Finland.

Technical Challenges

We present four groups of technical challenges for IoT. The first group relates to scalability and energy constraints. Scalability refers to the ability of networks to sustain a very large number of devices. We believe that one order of magnitude increase in the size of the current networks is easily achieved, but there are issues for going beyond this. These issues relate to the sheer number of devices to address and hold the state for, but also for simultaneous events such as devices coming online simultaneously after a large power or network outage. The sheer number of objects present and the kinds of active/passive wireless technologies used would create substantial challenges for routing/signaling, naming, collaboration, information/data processing and networking. Therefore traditional methods based on L2/L3 technologies (addressing and discovery) may simply not be feasible for information retrieval and complex computations, and become structurally too inflexible in terms of scalability. In contrast, from the point of view of an individual device it is important to scale down, to limit the complexity of a device and its power usage. Often such scaling down is not merely important to keep the cost of the device down, they can be crucial for enabling the entire application. For instance, sufficient battery lifetime for an application with hundreds of devices can be surprisingly large. A home with a hundred devices with ten-year battery lifetimes will result in a battery change operation every month. Or the size of the sensor may be very important, for instance to make devices embedded in our clothing practical. The practical challenge is to increase battery lifetimes of small devices by several orders of magnitude. Another class of challenges relate to interoperability. As the Internet has evolved, interoperability has always been a major concern, in terms of protocol design and extensibility, building products that in practice work well together with other devices,

and setting standards. Some of the requirements and expected usage patterns in the IoT will cause interoperability challenges. Moreover, like the present day Internet has evolved significantly over the past decades, we expect an IoT to evolve over time, with new uses and new requirements coming up. Evolution incurs another interoperability challenge: of different versions over time. One further element of interoperability is testing: it is well-known today that Internet-scale testing is hard, if not impossible; the increase in scale toward IoT and the expected limited capabilities of IoT devices are going to push the demands on testing even further. Much of the current focus in the IoT is also on the lower parts of the stack: designing the wireless networks and running IP and transport protocols over them. While tremendously useful, an IoT transport network is not enough for true interoperability. For instance, it would not be enough for a light switch from one vendor to control lights from another. For true interoperability we need semantic interoperability, the ability of the devices to unambiguously convey the meaning of data they communicate. The third group of challenges relates to shared infrastructure. The success of the IoT and the feasibility of many business models will depend heavily on architectures that utilize horizontal service components that are generic across different vertical industries. High efficiency can only be reached if multiple vertical applications can share common infrastructure, data, and resources. One challenge is identifying the parts of the IoT middleware platform that are common across the vertical industries. A further challenge is systems integration - how to build a coherent vertical application out of a large collection of software modules and horizontal components. Yet another challenge is defining generic interfaces that are attractive to application developers, meet the needs of diverse vertical applications, and abstract away the specifics of heterogeneous things, resources, and networks. The fourth group of challenges relates to managing large numbers of devices. Many of the potential applications are in environments where active management or even substantial installation expertise cannot be assumed, for instance, homes. In addition, in many applications active, human-run management or any per-device manual work is economically infeasible. This calls for self-management solutions. While this has been an active research area for some time, there is little to show in terms of solutions that have actually become adopted by consumers or the industry. Self-management is particularly challenging with regards to setting up security and application-relevant data such as locations of indoor sensors or their real-world relevance.

Security, Privacy and Trust Challenges

Security, privacy and trust challenges have an impact on all other topics of IoT. Moreover, smart solutions for these challenges are clearly strong business enablers. The IoT will create a dynamic network of a large number of identifiable things communicating with each other. Although the IoT will provide help in many areas, it will create its own set of security, privacy and trust challenges. At the heart of the IoT vision lays a contradiction: On the one hand, the environment must be highly knowledgeable about a user to match his or her needs without explicit interaction. On the other hand, a system that is truly ubiquitous will encompass numerous users, and systems. However, perfect trust among all parties is unattainable. The security, privacy and trust solutions for the IoT need to consider devices with huge variation in their capabilities as well as applications with different needs. For example, when utilizing sensors for medical applications, security solutions must be triple-checked against the stringent requirements; potential privacy issues must be addressed; protocol messages and cryptographic mechanisms must be adopted to wireless sensor standards. Although bearing high risks of provable security and patient faith, remote monitoring of health appliances could create breakthroughs in healthcare cost reduction and bring great benefits for individuals and society. A further complication relevant to large networks such as IoT is that security and privacy risks are often very dynamic in their nature. Obviously, there is plenty of room for adequate effective, adaptive, risk-driven and evidence-based security, privacy and trust solutions mitigating these challenges. In IoT, sensors and small devices are embedded all around our environment; inside buildings, under our skin, in wide-area environments, and even in highly critical environments such as industrial automation. During an attack, unplugging them from the network is often not an option. Shutting down the network infrastructure might not be sufficient either, as many of these devices will be able to form their own autonomous networks and via multichip routing still be reachable from the Internet. In addition, one basic security problem is that it is very hard to design systems that can be deployed securely without requiring a manual action for setting up a key for the device. However, critical applications must be secure enough. Examples are medical applications or applications that control potentially dangerous processes. Existing problems of the current Internet, such as

unwanted traffic and different kinds of denial of service attacks, are also amplified in the IoT. For instance, battery-powered devices should avoid having to receive any unwanted messages for power saving and also minimize the overhead created by overplaying security. Overplaying security can be minimized by systematical trade-off analysis of security effectiveness, usability, and performance dimensions. Feasible design methodologies and tools for this are needed. Another basic problem is that by its nature, the IoT produces information that can identify persons through the devices that they carry, and collect sensitive information. The privacy problems of the IoT are largely unsolved today in the general case, even if specific solutions exist for applications that handle sensitive data. Better solutions are needed in order to preserve the basic human right to privacy and to comply with relevant legislation. Security, privacy and trust considerations are crosscutting in IoT: they have an impact on IoT at all levels from technical details to human behavior. For example, IoT concepts might redefine the traditional view of end-to-end security as intermediate devices play increasingly important roles for the essential functioning of an application. They should be considered as early as possible during the IoT architecture design, business analysis and should be adequately managed and built-in in all activities. This horizontality is a remarkable challenge in itself, and postulates contribution from security professionals as well as security-oriented thinking from all developers, service providers and end-users.

Societal Challenges

It is important to note that the IoT is not just about networking technology. All systems involve user interaction, and finding good ways to deal with large amount of possibly conflicting data is not trivial. Good user interfaces for managing different types of IoT networks are still being researched. Moreover, IoT enables interacting with physical objects directly (i.e. tangible user interfaces) in addition to interacting through the conventional user interface devices (i.e. graphical user interfaces). What are the right abstractions to present information to human users? How to advertise the tangible interaction possibilities to users? What is a good user interaction model to begin with? Much of our current interaction with technology revolves around the limitations of older designs. For instance, light switches were born out of the way electrical wiring needed to be done. If there were no wiring limitations, what would

be a good user interface from the user's perspective? Development tools should be revised as well – with the right kind of tools users could build IoT applications themselves. One view on this set of challenges is how to fully exploit new physical interaction options between the digital and physical world that become possible with IoT technology? What is more, the future will bring a Social Internet of Things. This requires a new perspective of device and system interoperability. Starting from User interface Designs of Social Internet to Social Internet of Things, designs must be interoperable on the application and service level with the devices that provide IoT data. When the research work is ongoing the crossroads of both of these aspects provide an intriguing new field of study.

Business Challenges

While there are many technical challenges, the challenges at the business level seem even bigger. In most cases, the (businesses and) business models are still being developed. For some cases, such as delivering general-purpose networking solutions the IoT is just additional business within the same business framework. In many other cases, it is still unclear what customers are being targeted, with what partners, and with what kind of economic parameters. There is a large number of perceived and real obstacles for starting an IoT business. For instance, utility companies complain about undesirable long-term lock-ins to operators providing a service, enterprise customers complain about the lack of interoperable solutions where vendors can be put in competition against each other, and application vendors complain about the lack of infrastructure and communications solutions that can be readily used. Many products still have a very small number of units sold, which keeps the prices high. It is clear that today's solutions for the IoT are fragmented. They are in many cases running in silos of legacy networks. Even if some applications may run over general-purpose Internet networks, there's little or no interoperability between applications. Middleware solutions exist, but no appreciable business on top of them. Today's applications are different depending on the specific vertical industry, enterprise, and geographical location, among other things. Existing solutions are typically dedicated to single applications such as fleet management, remote meter reading, or vending machines. In the future, economies of scale will make the reduction of the fragmentation a key success factor. Similarly, consumer adoption requires

standardization in many cases. Traditional electrical installations in homes allowed any light control to work with any light switch, for instance. This has yet to be replicated for the IoT-based lighting controls. Today the M2M market is very fragmented with different protocols, lots of device vendors and products. Interoperability between M2M products from different vendors and also between M2M networks is a challenge. It is also a challenge to define the level of generalization of M2M solutions so that they support use cases from various industries but are still useful.

Challenges in Finland

The above issues are global. There are, however, specific local challenges within our industry and society. As a country, Finland has some challenges that are not unique in the Western world but are perhaps a bit more pronounced here than elsewhere. An aging population and high labor costs are two examples. On the other hand, there is also a high desire to invest in the school system, high quality health care, and environmentally friendly solutions. Carbon emission agreements are particularly difficult for a country with a cold climate, and energy-saving applications are clearly a priority. All of these areas would benefit from IoT applications, and in some cases technology developed elsewhere in the world is not readily applicable for the specific Finnish setting in these areas.

CHAPTER 6

APPLICATION

1.)MEDIA

In order to hone the manner in which the Internet of Things (IoT), the Media and Big Data are interconnected, it is first necessary to provide some context into the mechanism used for media process. It has been suggested by Nick Couldry and Joseph Turow that Practitioners in Media approach Big Data as many actionable points of information about millions of individuals. The industry appears to be moving away from the traditional approach of using specific media environments such as newspapers, magazines, or television shows and instead tap into consumers with technologies that reach targeted people at optimal times in optimal locations. The ultimate aim is of course to serve, or convey, a message or content that is (statistically speaking) in line with the consumer's mindset. For example, publishing environments are increasingly tailoring messages (advertisements) and content (articles) to appeal to consumers that have been exclusively gleaned through various data-mining activities.

2.) Environmental monitoring

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection by monitoring air or water quality, atmospheric or soil conditions, and can even include areas like monitoring the movements of wildlife and their habitats.[61] Development of resource constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically span a large geographic area and can also be mobile. Infrastructure management Monitoring and controlling operations of urban and rural infrastructures like bridges, railway tracks, on- and offshore- wind-farms is a key application of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users

of these facilities.] IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas. Even areas such as waste management can benefit from automation and optimization that could be brought in by the IoT.

3.) Manufacturing

Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm on industrial applications and smart manufacturing as well. The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together. Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT. But it also extends itself to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability. Smart industrial management systems can also be integrated with the Smart Grid, thereby enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors.

4.) Energy management

Integration of sensing and actuation systems, connected to the Internet, is likely to optimize energy consumption as a whole. It is expected that IoT devices will be integrated into all forms of energy consuming devices (switches, power outlets, bulbs, televisions, etc.) and be able to communicate with the utility supply company in order to effectively balance power generation and energy usage. Such devices would also offer the opportunity for users to remotely control their devices, or centrally manage them via a cloud based interface, and enable advanced functions like scheduling (e.g., remotely powering on or off heating systems, controlling ovens, changing lighting conditions etc.). In fact, a few systems that allow remote control of electric outlets are

already available in the market, e.g., Belkin's WeMo, Ambery Remote Power Switch, Budderfly, Telkonet's EcoGuard, WhizNets Inc., etc. Besides home based energy management, the IoT is especially relevant to the Smart Grid since it provides systems to gather and act on energy and power-related information in an automated fashion with the goal to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. Using Advanced Metering Infrastructure (AMI) devices connected to the Internet backbone, electric utilities can not only collect data from end-user connections, but also manage other distribution automation devices like transformers and reclosers.

5.) Medical and healthcare systems

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers or advanced hearing aids. Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. Other consumer devices to encourage healthy living, such as, connected scales or wearable heart monitors, are also a possibility with the IoT. More and more end-to-end health monitoring IoT platform are coming up for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements. Distinct advantages over similar products from the US and Europe are cost-effectiveness and personalization for chronic patients. Doctors can monitor the health of their patients on their smart phones after the patient gets discharged from the hospital.

6.) Building and home automation

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential). Home automation systems, like other building automation systems, are typically used to control lighting, heating, ventilation, air conditioning, appliances, communication systems, entertainment and home security devices to improve convenience, comfort, energy efficiency, and security.

7.) Transportation

The IoT can assist in integration of communications, control, and information processing across various transportation systems. Application of the IoT extends to all aspects of transportation systems, i.e. the vehicle, the infrastructure, and the driver or user. Dynamic interaction between these components of a transport system enables inter and intra vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistic and fleet management, vehicle control, and safety and road assistance .

CHAPTER 7

CONCLUSION

.

The thought of always being tracked and your data being recorded does bring a fear to a consumer's mind, but we have to move away from it to see the benefits that this great technology is going to bring to us. The above examples were about a 'connected you', making your life seamless, but it brings with it higher benefits like connected cities, better commerce and an improved ecosystem. As often happens, history is repeating itself. Just as in the early days when Cisco's tagline was "The Science of Networking Networks," IoT is at a stage where disparate networks and a multitude of sensors must come together and interoperate under a common set of standards. This effort will require businesses, governments, standards organizations, and academia to work together toward a common goal. Next, for IoT to gain acceptance among the general populace, service providers and others must deliver applications that bring tangible value to peoples' lives. IoT must not represent the advancement of technology for technology's sake; the industry needs to demonstrate value in human terms. In conclusion, IoT represents the next evolution of the Internet. Given that humans advance and evolve by turning data into information, knowledge, and wisdom, IoT has the potential to change the world as we know it today—for the better. How quickly we get there is up to us.

BIBLIOGRAPHY

[1] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer and Shahid Khan, ”Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges,” in Proceedings of Frontiers of Information Technology (FIT), 2012, pp. 257-260

[2] Guicheng Shen and Bingwu Liu, ”The visions, technologies, applications and security issues of Internet of Things,” in E -Business and E -Government (ICEE), 2011, pp. 1-4

[3] Ling-yuan Zeng, ”A Security Framework for Internet of Things Based on 4G Communication,” in Computer Science and Network Technology (ICCSNT), 2012, pp. 1715-1718

[4] ”The”Only”CokeMachineontheInternet,”CarnegieMellon University, School of Computer Science.

[5] M. Weiser, ”The computer for the 21st century”, Sci. Amer., 1991, pp.66 -75

[6] Jason Pontin, ”Bill Joy’s Six Webs,” MIT Technology Review, 29 September 2005

[7]KevinAshton,”That’InternetofThings’Thing”,RFIDJourna l, 22 June 2009

[8] Ferguson, T. (2002) Have Your Objects Call My Object. Harvard Business Review, June, 1-7.

[9] Nunberg, G. (2012) The Advent of the Internet: 12th April, Courses.