International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

An Analysis of Internet of Things (IoT): Novel Architectures, Modern Applications, Security Aspects and Future Scope with Latest Case Studies

IoT in Latest Trends

Mohd Muntjir
Department of Information Technology
College of Computers and Information Technology
Taif University, Taif, Saudi Arabia

Mohd Rahul
Department of Information Technology
College of Computers and Information Technology
Taif University, Taif, Saudi Arabia

Hesham A. Alhumyani
Department of Computer Engineering
College of Computers and Information Technology
Taif University, Taif, Saudi Arabia

***Abstract*—While we might be thinking, "one of these things is not like the others," these are all examples of the Internet of Things (IoT). The Internet of Things (IoT) connects the physical and the cyber worlds. On these days, one of the main objectives of Internet is its own progression. The Internet of Things (IoT) is a pattern where everyday objects can be furnished with classifying, sensing, networking and processing potentials that will allow them to correspond over the Internet to accomplish some purpose. The future of Internet of Things are, transform the real world things into intelligent virtual things. The Internet of Things (IoT)in tends to unite everything in our world under general infrastructures. Every object will have an exclusive identifier and will be able to locate itself and connect to the Internet. Moreover, Radio Frequency Identification (RFID) techniques will be the base of Internet of Things (IoT). Eventually, IoT devices will be pervasive, context-aware and will allow ambient ability and enable knowledge growth in proficiently. This paper reports on the current state of research and the meaning of IoT is defined with its progression structure. Moreover, present study attends to IoT conception through organized review of scholarly research papers, and professional discussions with competent. We also discussed about Internet of Things (IoT) by probing the literature, recognizing current trends and relating challenges that threaten IoT transmission. Though, this paper will give good conception for the new researchers, who want to do research in this field of Internet of Things (IoT).**

***Keywords*—Internet of Things, IoT, Machine to machine, Ubiquitous, Ambient, Internet, RFID, Wi-Fi, Sensors, Actuators, cloud computing, smart city**

I. INTRODUCTION

The term *Internet of Things* (*IoT)* was invented by industry researchers but has surfaced into mainstream public view only more recently. Some maintain the Internet of Things will entirely transform how computer networks are used for the next 10 or 100 years, while others consider IoT is just hype that won't much impact the daily lives of most people. The "Internet of things" (IoT) is becoming an increasingly growing topic of conversation both in the workplace and outside of it. It's a concept that not only has the potential to impact how we live but also how we work. The Internet of things creates an opportunity to evaluate, assemble and analyze an ever-increasing selection of behavioral information.

It is expected that IoT devices will be incorporated into all forms of energy consuming devices such as switches, bulbs, power outlets, televisions, etc and be proficient to communicate with the utility supply company in order to efficiently balance power generation and energy consumption. The Internet of Things (IoT) is a term coined by Kevin Ashton, who perceived a system of ubiquitous sensors concerning the physical world to the Internet. Though things, Internet, and connectivity are the three core factors of Internet of Things (IoT), the importance is in closing the breach between the physical and digital world in self-reinforcing and self-improving techniques. [4]. Internet of Things definition is the vast network of devices connected to the Internet, including smart phones and tablets and almost anything with a sensor on it – cars, machines in production plants, jet engines, oil drills, wearable devices, and more. These "things" collect and exchange data. IoT – and the machine-to-machine (M2M) technology behind it – are bringing a kind of "super visibility" to nearly every industry. Imagine utilities and telcos that can predict and prevent service outages, airlines that can remotely monitor and optimize plane performance, and healthcare organizations that can base treatment on real-time genome

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

analysis. The business possibilities are endless. Internet of Things symbolizes a general perception for the ability of network devices to sense and collect data from the world, and then contribute that data across the Internet where it can be processed and developed for various interesting reasons. [1]. The Internet-of-Things (IoT) is steadily becoming one of the most outstanding technologies that emphasize this world, through facilitate the orchestration and coordination of a large number of physical and virtual Internet-Connected-Objects (ICO) towards human-centric services in a selection of sectors counting logistics, industry, trade, smart cities and ambient supported living. Furthermore, we will be presenting a set of internet-of-things technologies and applications in the form of a series of knowledge.

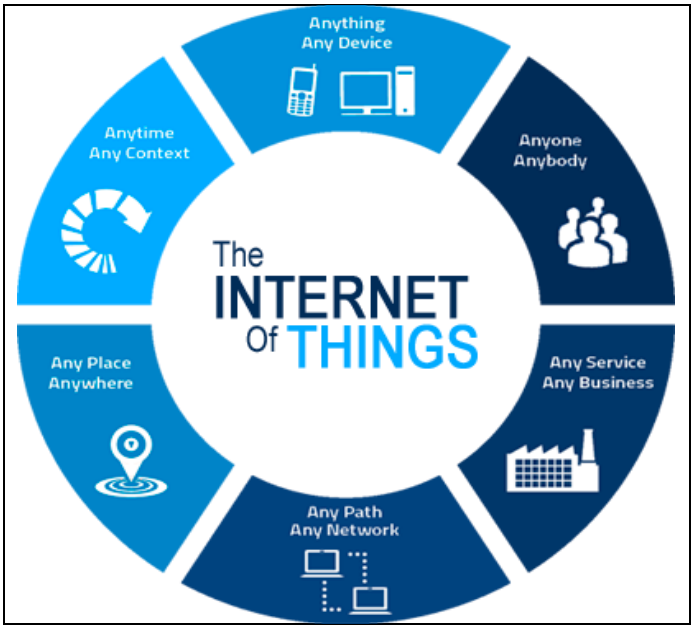

Fig. 1. IoT

The propagation of internet-connected-objects authorizes interactions both between devices and things but also between things and people, hence providing unparalleled application prospects. Definitely, people can directly connect to things such as mobile phones, electronic health records and many more things, via wearable sensors such as motion sensors and smart textiles. Similarly, things connect to each other e.g., as part wireless sensors networks, but also as part of a Wireless Sensor Network's communication with other devices such as gateways, mobile devices etc. Other example is car sensors, which are, connect to intelligent transport systems and with sensors from other medium. These communications are in most cases empowering by various networking frameworks, which offer ubiquitous high-quality connectivity, such as 4G and 5G infrastructures [2]. Cloud-based applications are the key to using leveraged data. The Internet of Things doesn't function without cloud-based applications to interpret and transmit the data coming from all these sensors. The cloud is what enables the apps to go to work for you anytime, anywhere. Here's what I mean when I say people never think big enough. This isn't just about money savings. It's not about bridges, and it's not about cities. This is a huge and fundamental shift. When we start making things intelligent, it's going to be a major engine for creating new products and new services. Of all the technology trends that are taking place right now, perhaps the biggest one is the Internet of Things; it's the one that's going to give us the most disruption as well as the most opportunity over the next five years. In my next post in this two-part series, we'll explore just how big this is going to be [107]. In order to realize the benefits of IoT, such as increasing customer intimacy, improving operational excellence and generating new revenue streams through business model innovation; there are three critical components for the ecosystem to thrive: reliable connectivity, reliable security and an agile monetization framework. Broadband Internet is become more widely available, the cost of connecting is decreasing, more devices are being created with Wi-Fi capabilities and sensors built into them, technology costs are going down, and smartphone penetration is skyrocketing.

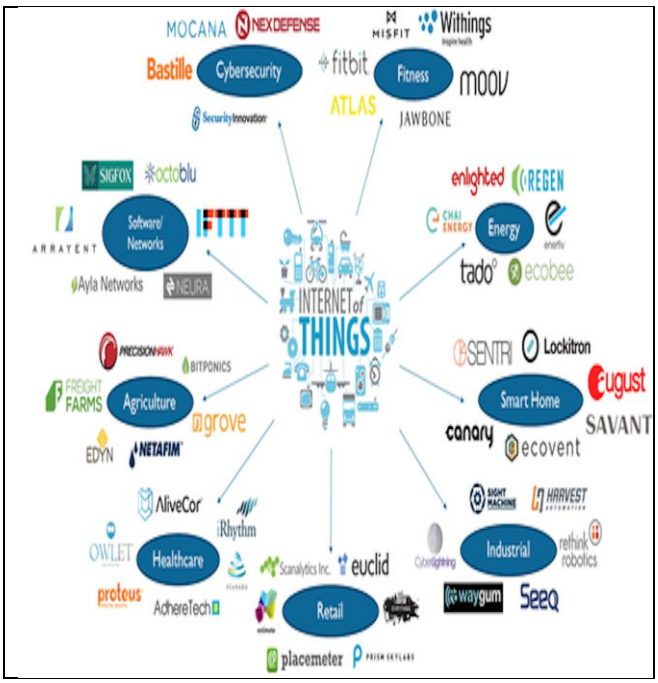

Fig. 2. IoT Map

Anyone who says that the Internet has basically improved society may be right but at the same time, the ultimate transformation essentially still lies ahead of us. Numerous innovative technologies are now joining in a way that means the Internet is on the edge of a generous development as objects large and small get connected and simulate their own web uniqueness. Succeeding on from the Internet of computers when our servers and personal computers were linked to an inclusive network system, and the Internet of mobile systems, while it was the turn of telephones and other mobile components, the next stage of development is the Internet of things (IoT), when more or less everything will be connected and accomplished in the virtual domain. [3] This revolution will be the Internet's largest expansion ever and will have sweeping conclusions on every industry, and all of our everyday lives.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

Fig. 3. IoT Structure

II. THE IOT HISTORY

A. *IoT Definition*

There is no unique definition available for Internet of Things that is acceptable by the world community of users [11]. In fact, there are many different groups including academicians, researchers, practitioners, innovators, developers and corporate people that have defined the term, although its initial use has been attributed to Kevin Ashton, an expert on digital innovation. What all of the definitions have in common is the idea that the first version of the Internet was about data created by people, while the next version is about data created by things [63]. The best definition for the Internet of Things would be: "An open and comprehensive network of intelligent objects that has the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment "Internet of Things is maturing and continues to be the latest, most hyped concept in the IT world [5]. Over the last decade the term Internet of Things (IoT) has attracted attention by projecting the vision of a global infrastructure of networked physical objects, enabling anytime, anyplace connectivity for anything and not only for anyone [6]. Internet has become more prevalent in our lives in a shorter time period than any other technology in the history. It revolutionized the communicate way of people. Currently, the Internet involves the process of connecting machines, equipment, software, and things in our surroundings [9]. This connection will be through the use of the unique Internet protocol address that permits things for communicating to each other without human intervention. This new scenario is called IoT. The term IOT is formalized by MIT Auto-ID center at [16]. "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 [64].

The Internet of Things can also be considered as a global network, which allows the communication between human-to-human, human-to-things and things-to-things, which is anything in the world by providing unique identity to each and every object [7]. IoT describes a world where just about anything can be connected and communicates in an intelligent fashion that ever before. Most of us think about "being connected" in terms of electronic devices such as servers, computers, tablets, telephones and smart phones. In what's called the Internet of Things, sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet IP that connects the Internet. These networks churn out huge volumes of data that flow to computers for analysis. When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly. What's revolutionary in all this is that these physical information systems are now beginning to be deployed, and some of them even work largely without human intervention. The "Internet of Things" refers to the coding and networking of everyday objects and things to render them individually machine-readable and traceable on the Internet [6]-[11]. Much existing content in the Internet of Things has been created through coded RFID tags and IP addresses linked into an EPC (Electronic Product Code) network [12].

B. *History*

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 [19]. 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.

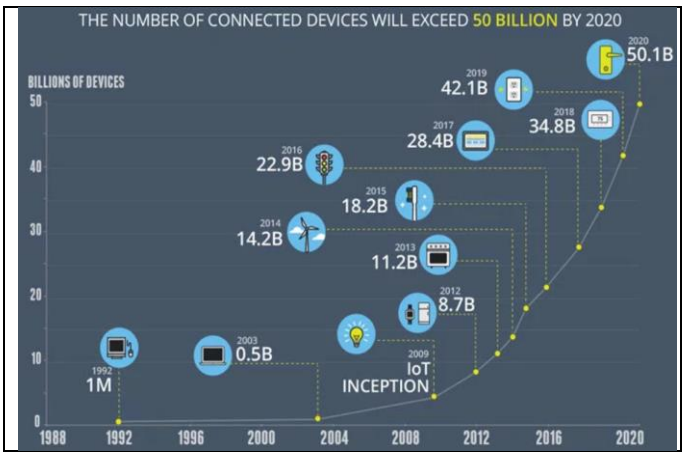

Fig. 4. IoT History

C. *Genesis*

The Internet of Things is a technological revolution that represents the future of computing and communications, and

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

its development depends on dynamic technical innovation in a number of important fields, from wireless sensors to nanotechnology. The first Internet appliance was a Coke machine at Carnegie Melon University in the early 1980s. Programmers working several floors above the vending machine wrote a server program that chased how long it had been since a storage column in the machine had been unfilled. The programmers could connect to the machine over the Internet, check the status of the machine and determine whether or not there would be a cold drink waiting them, should they decide to make the trip down to the machine. Though the buzzword "Internet of Things" evolution was set out a way back in 1980's with coffee vending machine, Kevin Auston, the Executive Director of Auto-ID Labs in MIT in 1999, coins the original term. The concept of IoT first became very popular through the Auto-ID center in 2003 and in related market analysts publications. Right from the beginning the Internet of Things evolution started, there were many things or objects connected to the internet for the different applications through diverse technologies depending on the type of object for the comfort ability of Human [5].

D. Features of IoT

The basic idea of the IoT was introduced in a technical report of the ITU in 2005. It has physical things and virtual things, which exist in the real world and cyberspace. To be more accurate, the physical things are connected to the virtual things using the Internet [8]. The ITU described the concept of IoT, and classify entities into four major categories of tagging things, feeling things, thinking things, and shrinking things. In addition, Wikipedia also defines the characteristics of the IoT, and classifies it into six categories of intelligent architecture [9], complex systems, size considerations, time considerations, and space considerations. First of all, intelligence has two different perspectives, which are ambient intelligence and autonomous control, and embedded intelligence. Ambient intelligence and autonomous control are not part of the original concept of the IoT. However, there is a shift in research to integrate the concepts of the IoT and autonomous control [10] presents an AI-oriented perspective of the IoT, which can be more clearly defined as leveraging the capacity to collect and analyze the digital traces left by people when interacting with widely-deployed smart things to discover knowledge about human life, environmental interactions, and social connections/behaviors. Second, the architecture will likely be event-driven [73]. Therefore, model-driven and functional approaches will coexist with new ones able to treat exceptions and the unusual evolution of processes. In IoT, the meaning of an event will not necessarily be based on a deterministic or syntactic model. It would, however, be based on the context of the event itself. The third characteristic is a complex system. In semi-open or closed loops. it will therefore be considered and studied as a complex system due to the huge number of different links and interactions between autonomous actors, and its capacity to integrate new actors. The fourth is time considerations. In this Internet of Things, made of billions of parallel and simultaneous events, time will no more be used as a common and linear dimension but will depend on each entity (object, process, information system, etc.). This Internet of Things will be accordingly based on massive parallel IT systems.

The last characteristics are space considerations. In an Internet of Things, the precise geographic location and dimensions of a thing will be critical information [57].

Therefore, facts about a thing, such as its location in time and space, will be less critical to track because the person processing the information can decide whether or not that information is important to the action being taken, and if so, add the missing information (or decide to not take the action). (Note that some things in the Internet of Things will be sensors, and sensor location is usually important. The Figure 2 shows a technology road map of the IoT [58].

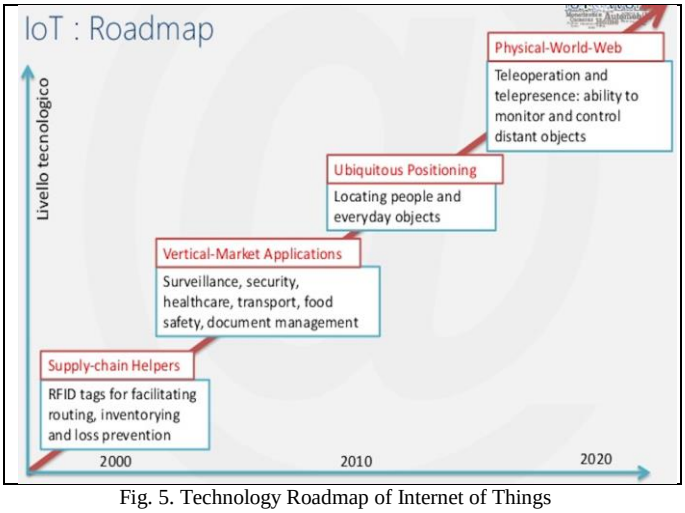

Fig. 5. Technology Roadmap of Internet of Things

E. Time Series

Accessed from the URL dated on 24/3/2013:
http://postscapes.com/internet-of-things-history [5].

- 1999: the term Kevin Ashton, Executive Director of the Auto-ID Center in Massachute Institute of Technology (MIT), coins Internet of Things
- 1999: Neil Gershenfeld first time spoken about IoT principles in his book titled "When Things Start to Think"
- 1999: MIT Auto-ID Lab, originally founded by Kevin Ashton, David Brock and Sanjay Sarma in this year. They helped to develop the Electronic Product Code
- 2000: LG announced its first Internet of refrigerator plans
- 2002: The Ambient Orb created by David Rose and others in a spin-off from the MIT Media Lab is released into wild with NY Times Magazine naming it as one of the Ideas of Year
- (2003-2004): RFID is deployed on a massive scale by the US Department of Defense in their program and Wal-Mart in the commercial world
- 2005: The UN's International Telecommunications Union (ITU) published its first report on the Internet of Things topic
- 2008: Recognition by the EU and the First European IoT conference is held

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

- 2008: A group of companies launched the IPSO Alliance to promote the use of IP in networks of "Smart Objects" and to enable the Internet of Things
- 2008: The FCC voted 5-0 to approve opening the use of the 'white space' spectrum
- (2008-2009): The IoT was born according to Cisco's Business Solutions Group
- 2008: US National Intelligence Council listed the IoT as one of the 6 "Disruptive Civil Technologies" with potential impacts on US interests out to 2025
- 2010: Chinese Premier Wen Jiabao calls the IoT a key industry for China and has plans to make major investments in Internet of Things [59]
- 2011: IPv6 public launch-The new protocol allows for 340, 282, 366, 920, 938, 463, 463, 374, 607, 431,768,211, 456 (2128) addresses [60]

F. Aliases

Different people calling Internet of Things with different names but the objective of IoT are same in the broad sense. The aliases of Internet of Things include Web of Things, Internet of Objects, Embedded Intelligence, Connected Devices and Technology Omnipotent, Omniscient and Omnipresent. In addition to these, it has also calling as counting [5]

- Cyber Physical Systems "Integrations of computation and physical processes", in which bringing the real and virtual worlds together
- Pervasive Computing is a computer environment in which virtually every object has processing power with wireless or wired connections to a global network
- Ubiquitous Computing or Calm technology, where technology becomes virtually invisible in our lives
- Machine-to-Machine Interaction means no human intervention whilst devices are communicating end-to-end
- Human-Computer Interaction involves the study, planning, and design of interaction between people and computers
- Ambient Intelligence is a developing technology that will increasingly make our everyday environment sensitive and responsive.

G. Requirements

For successful implementation of Internet of Things (IoT), the prerequisites are (a) Dynamic resource demand (b) Real time needs (c) Exponential growth of demand (d) Availability of applications (e) Data protection and user privacy (f) Efficient power consumptions of applications (g) Execution of the applications near to end users (h) Access to an open and inter operable cloud system [5]. According to another author, there are three components, which required for seamless Internet of Things (IoT) computing [61]

1) Hardware—composed of sensors, actuators, IP cameras, CCTV and embedded communication Hardware

2) Middleware—on demand storage and computing tools for data analytics with cloud and Big Data Analytics

3) Presentation—easy to understand visualization and interpretation tools that can be designed for the different applications [62].

H. Fault tolerance for IoT

Based on the fact that IoT will face billions more devices, IoT will be more vulnerable to be attacked than the Internet, and there might be some attacker that want to control some devices directly or indirectly [20]. One way to know the level of reliability of a service is having a defined threshold for service fault tolerance. However, it should be considered that any solution for this aspect should be lightweight enough that it can be implemented on IoT. As a conclusion, we should first design all elements with secure mechanisms by improving the quality of the implementing software. Also, every element of the IoT should be able to know the real-time status of the network, to provide the feedback to other elements. Therefore, having a monitoring system would be helpful in this matter. Finally, any time that the network faces degradation in the performance or has a failure in the performance; every element should have the ability to protect them. So, various privacy protocols should also be defined for this situation to instruct the elements the way they should work in unusual situations to fix the situation and be able to recover quickly. Hence, the viability of recovery services is obvious [37].

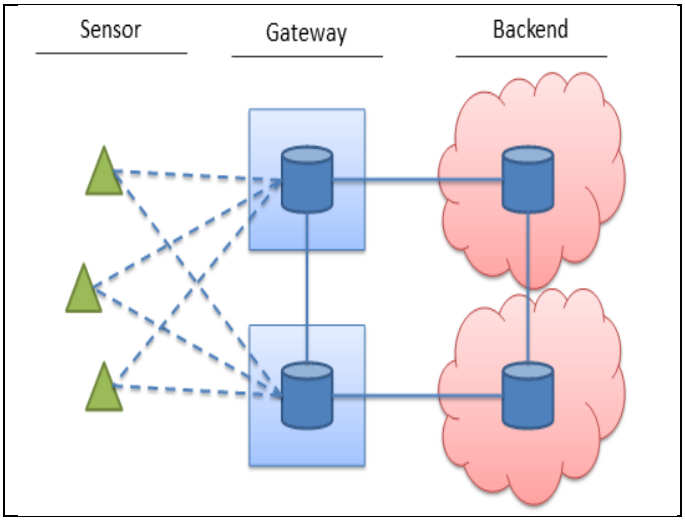

Fig. 6. Fault tolerant in IoT

Also, by providing automatic services for example in M2M (Machine to Machine) communication, the need for providing safety and security will be more crucial. Some examples are different unpredictable characters and patterns. This matter will be worse even in the distributed environment, which is the main domain for IoT. This challenge stays valid even for bounded and closed environments. There are some hot researches considering algorithms, which are able to derive value from unstructured data to increase performance. There are different factors determining main criteria of an identifier, such as: governance, security and privacy. Also, lots of existing identification schemes have been created long time ago for local usage and for specific objectives. Therefore, the need to have a global reference for identification is vital.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

I. Gartner's Hype cycle

Garter's Information Technology Hype Cycle [22] is a way to represent emergence, adoption, maturity and impact on applications of specific technologies (2) In the adjacent graph, X- axis denotes expectations and Y- axis denotes time factors (3) Internet of Things has been identified as one of the emerging technologies in Internet of Things as noted in Gartner's IT Hype Cycle (4) It has been forecasted that IoT will takes around 5-10 years for market adoption as of the 2012. See the picture for data [5].

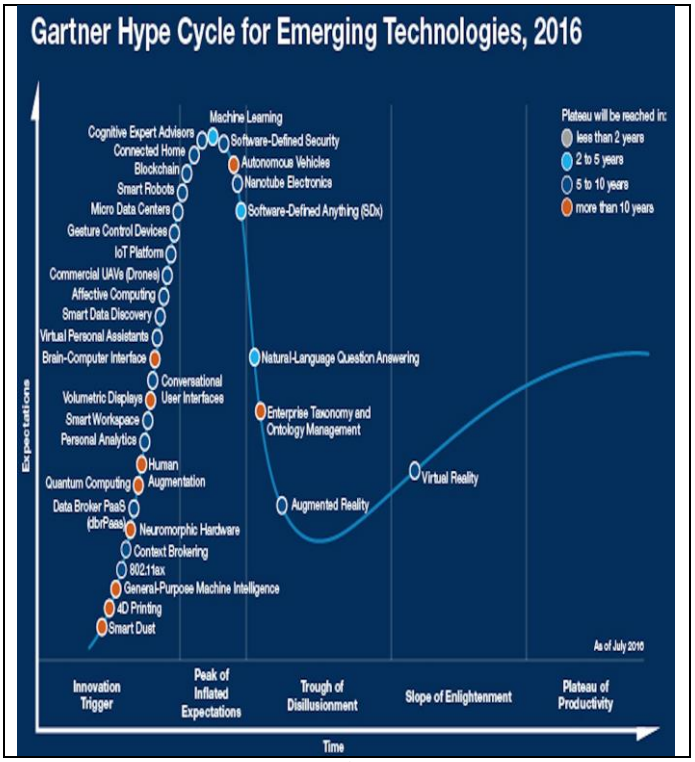

Fig. 7. Gartner's hype cycle for emerging technologies

III. ARCHITECTURE OF INTERNET OF THINGS(IOT)

Under the name "Internet of Things" (IoT) or "Industry 4.0" companies are developing a new network of intercommunicating objects of our everyday life. The Internet is continuously changing and evolving. The main communication form of present Internet is human-human. The Internet of Things (IoT) can be considered as the future evaluation of the Internet that realizes machine-to-machine learning. Reference architectures are of great help for standardization, as they define guidelines that can be used when planning the implementation of an IoT system. The Internet of Things is a technological revolution that represents the future of computing and communications. It is not the simple extension of the Internet or the Telecommunications Network. It has the features of both the Internet and the Telecommunications Network, and also has its own distinguishing feature. Through analyzing the current accepted three-layer structure of the Internet of things, we suggest that the three-layer structure can't express the whole features and connotation of the Internet of Things. After reanalyzing the technical framework of the Internet and the Logical Layered Architecture of the Telecommunication Management Network, we establish new five-layer architecture of the Internet of Things. We believe this architecture is more helpful to understand the essence of the Internet of Things, and we hope it is helpful to develop the Internet of Things [93]. The proliferation of these devices in a communicating–actuating network creates the Internet of Things (IoT), wherein sensors and actuators blend seamlessly with the environment around us, and the information is shared across platforms in order to develop a common operating picture (COP). The first architectural component of IoT is the perception layer. It collects data using sensors, which are the most important drivers of the Internet of Things.

Implementation of IoT is based on an architecture consisting of several layers: from the field data acquisition layer at the bottom to the application layer at the top [11]. The layered architecture is to be designed in a way that can meet the requirements of various industries, enterprises, societies, institutes, governments etc. Fig. 3 presents a generic layered architecture for IoT [14]. The layered architecture has two distinct divisions with an Internet layer in between to serve the purpose of a common media for communication. The two lower layers contribute to data capturing while the two layers at the top are responsible for data utilization in applications [65].

A. The 5-Layer Architecture

The Internet of Things (IoT) is defined as a paradigm in which objects equipped with sensors, actuators, and processors communicate with each other to serve a meaningful purpose.

The 3-layer architecture became not sufficient due to the expected IoT development. Therefore, 5-layer architecture is proposed. The first layer is called business. The purpose of this layer is to define the IOT applications charge and management. Also, it is responsible about the user's privacy and all research related to IOT applications [15]. The second layer is called application. The target of this layer is determining the types of applications, which will be used in the IoT [66].

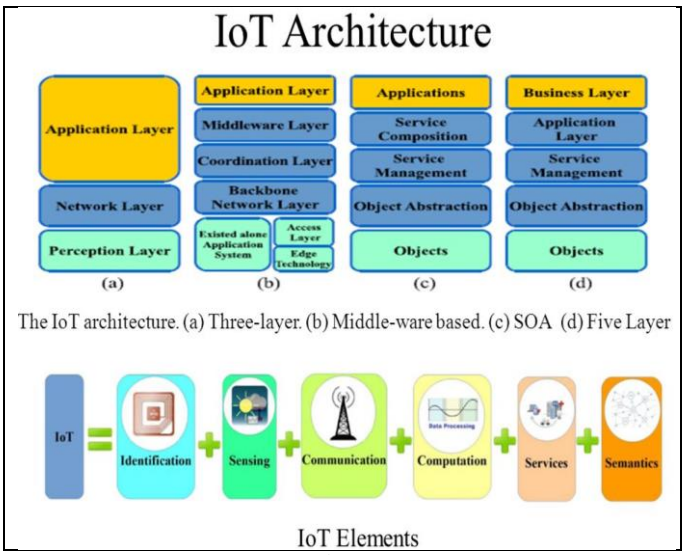

Fig. 8. Architecture of IoT with IoT Elements

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

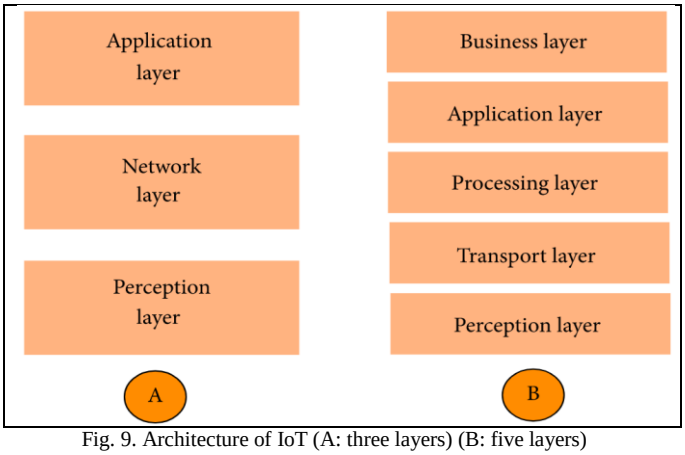

Fig. 9. Architecture of IoT (A: three layers) (B: five layers)

The third layer is called processing. Its responsibility is to handle the information gathered by perception layer. The handling process contains two main topics; storing and analyzing [9]. The target of this layer is extremely hard due to the huge gathered information about system things. So, it uses some techniques such as database software, cloud computing, ubiquitous computing, and intelligent processing in information processing and storing. The fourth layer is called transport. It seems like the network layer in the 3-layer architecture [8]. It transmits and receives the information from the perception layer to the processing layer and via versa. It contains many technologies such as infrared, Wi-Fi, and Bluetooth. Also, the target of this layer is to address each thing in the system using IPV6. The fifth layer is called perception. The target of this layer is to define the physical meaning of each thing in the IoT system such as locations and temperatures [74]. It also gathers the information about each object in the system and transforms this data to signals. In addition, it contains the technologies that are used in the IoT such as the RFID and the GPRS [9]. Following Figure presents the 5-Layer architecture.

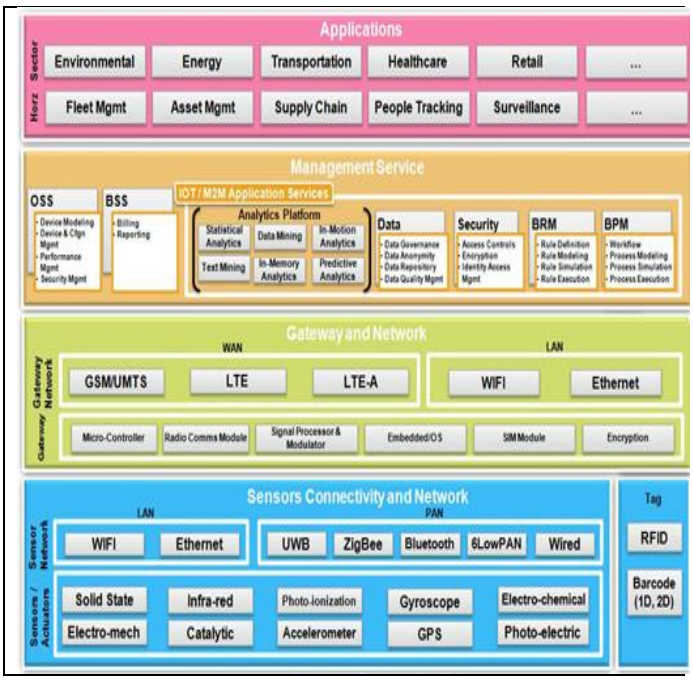

Fig. 10. Architecture of IoT

B. European FP7 Research Project

Internet of Things is a platform where every day devices become smarter. (1) This is to be used as a blueprint for IoT concrete architecture design; (2) Model: Architectural Reference Model (ARM); (3) Developed By: Project partners of the European FP7 Research Project IoT-A; (4) Derived From: Business considerations, application-based requirements and current technologies [5].

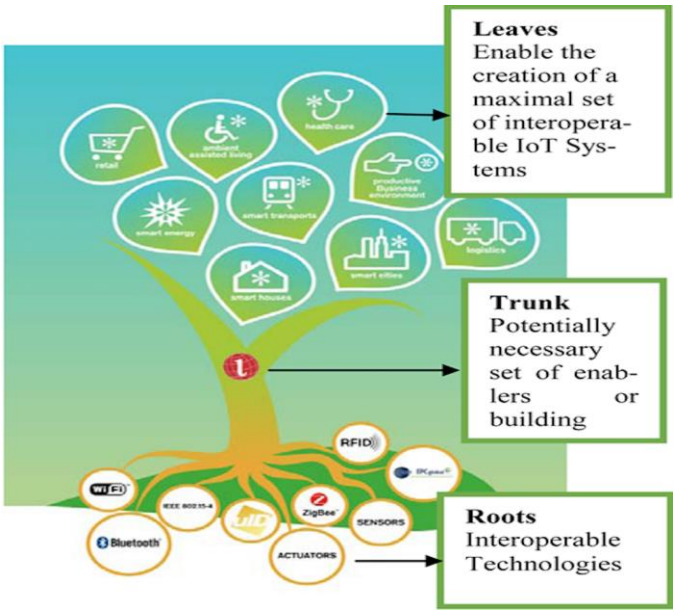

Fig. 11. FP7 Research

C. ITU Architecture

According to the recommendations of the International Telecommunication Union (ITU), the network, Architecture of Internet of Things consists of

(a) The Sensing Layer
(b) The Access Layer
(c) The Network Layer
(d) The Middleware Layer
(e) The Application Layers

These are like the Open Systems Interconnection (OSI) reference model in network and data communication [56].

D. IoT Forum Architecture

The IoT Forum says that the Internet of Things Architecture is basically categorized into 3 types including Applications, Processors and Transpiration.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

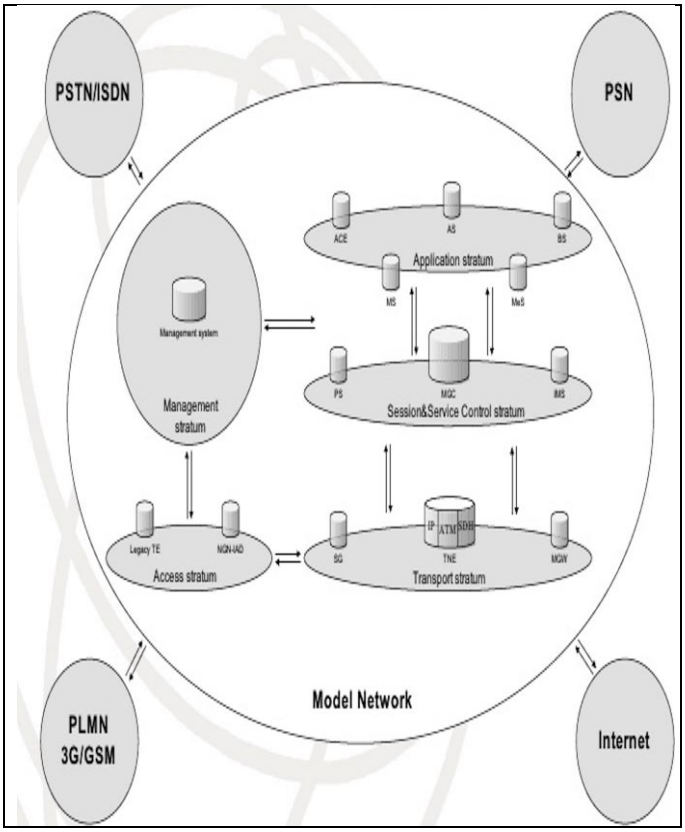

Fig. 12. International Telecommunication Union Architecture

E. Qian Xiao Cong, Zhang Jidong Architecture

According to Qian Xiao Cong and Zhang Jidong (2012), the traditional IoT is formed by three layers. The bottoms perception layer, whose function is cognizing and collecting information of objects. The middle is transportation layer, which consists of OFC, mobile phone networks, and fixed telephone networks, broadcasting networks, and closed IP data networks for each carrier. And finally the top is application layer, where abundant applications run. Typical applications include in this layer are smart traffic, precise agriculture, intelligent logistics, smart industry, environment protection, mining monitor, remote nursing, safety defense, smart government etc [56].

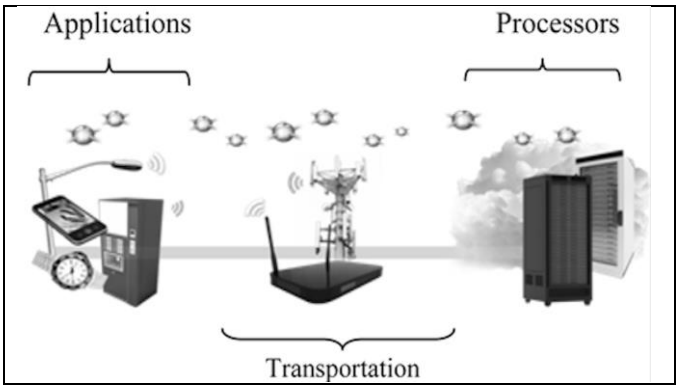

Fig. 13. Qian Xiao cong, Zhang Jidong Architecture

F. Kun Han, Shurong Liu, Dacheng Zhang and Ying Han's (2012)'s Architecture

In "Initially Researches for the Development of SSME under the Background of IoT", the model is

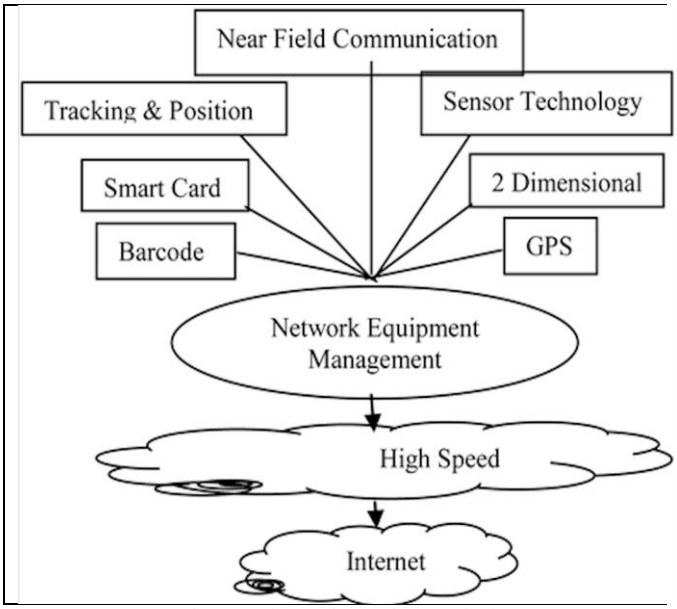

Fig. 14. Kun Han, Shurong Liu, Dacheng Zhang and Ying Han's (2012)'s Architecture [56]

G. Cloud and Fog Based Architectures

Let us now discuss two kinds of systems architectures: cloud and fog computing (see the reference architectures in [94]). Note that this classification is different from the classification in given Section, which was done on the basis of protocols [100]. In particular, we have been slightly vague about the nature of data generated by IoT devices, and the nature of data processing. In some system architectures the data processing is done in a large centralized fashion by cloud computers. Such a cloud centric architecture keeps the cloud at the center, applications above it, and the network of smart things below it [95]. Cloud computing is given primacy because it provides great flexibility and scalability. It offers services such as the core infrastructure, platform, software, and storage. Developers can provide their storage tools, software tools, data mining, and machine learning tools, and visualization tools through the cloud. Lately, there is a move towards another system architecture, namely, fog computing [[96],[97],[98]] where the sensors and network gateways do a part of the data processing and analytics. A fog architecture [99] presents a layered approach as shown in Figure below, which inserts monitoring, preprocessing, storage, and security layers between the physical and transport layers. The monitoring layer monitors power, resources, responses, and services. The preprocessing layer performs filtering, processing, and analytics of sensor data. The temporary storage layer provides storage functionalities such as data replication, distribution, and storage. Finally, the security layer performs encryption/decryption and ensures data integrity and privacy. Monitoring and preprocessing are done on the edge of the network before sending data to the cloud.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

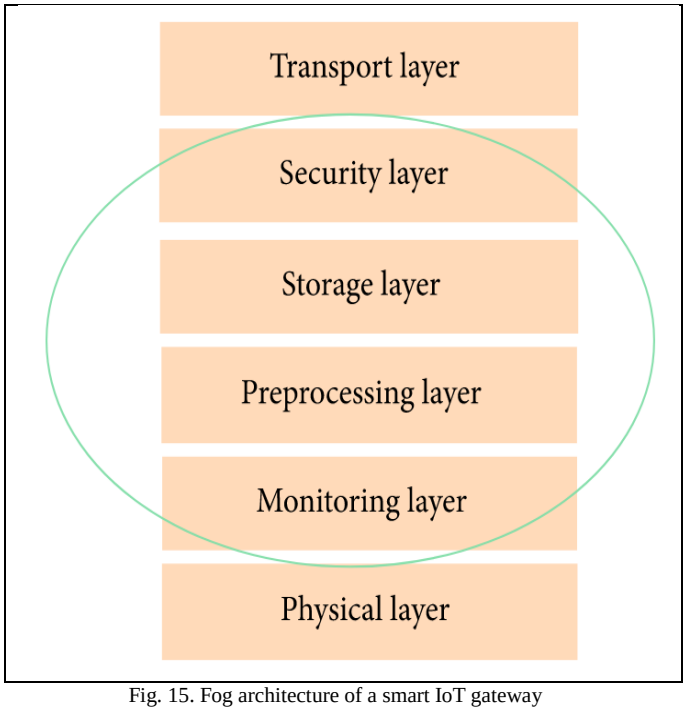

Fig. 15. Fog architecture of a smart IoT gateway

IV. TECHNOLOGIES OF IOT

A. RFID and near-field communication

In the 2000s, RFID was the dominant technology. Later, NFC became dominant (NFC). NFC has become common in smart phones during the early 2010s, with uses such as reading NFC tags or for access to public transportation. RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology. Specifically, NFC is a branch of High-Frequency (HF) RFID, and both operate at the 13.56 MHz frequency.

Radio-frequency identification (RFID) is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects [9]. The tags contain electronically stored information. Some tags are powered by electromagnetic induction from magnetic fields produced near the reader. Some types collect energy from the interrogating radio waves and act as a passive transponder. Other types have a local power source such as a battery and may operate at hundreds of meters from the reader. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader and may be embedded in the tracked object. RFID is one method for Automatic Identification and Data Capture (AIDC). RFID tags are used in many industries, for example, an RFID tag attached to an can be tracked through warehouses; and implanting RFID microchips in livestock and pets allows positive identification of animals. Since RFID tags can be attached to cash, clothing, and possessions, or implanted in animals and people, the possibility of reading personally linked information without consent has raised serious privacy concerns [11].

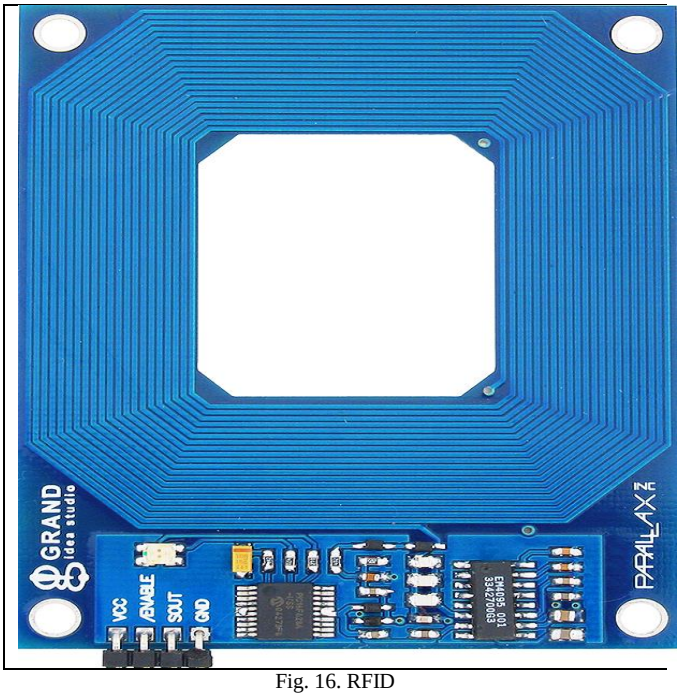

Fig. 16. RFID

Fig. 17. NFC in RFID

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

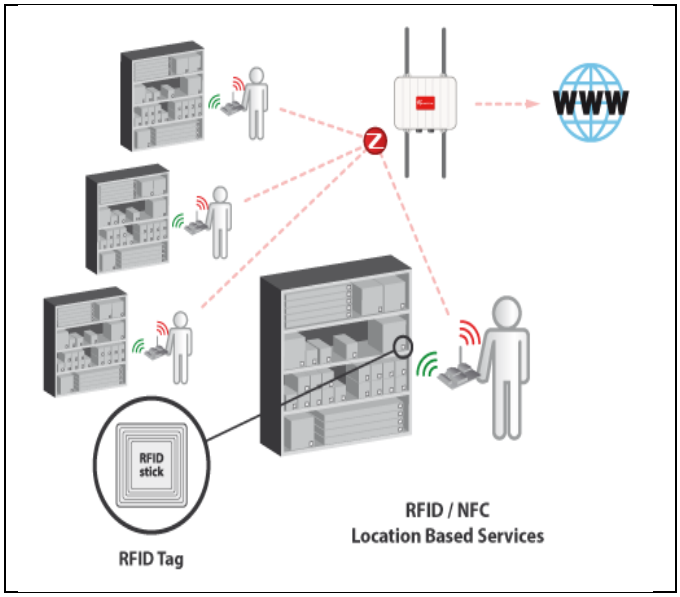

Fig. 18. NFC (Near Field Communication)

These concerns resulted in standard specifications development addressing privacy and security issues. ISO/IEC 18000 and ISO/IEC 29167 use on-chip cryptography methods for un-traceability, tag and reader authentication, and over-the-air privacy. ISO/IEC 20248 specifies a digital signature data structure for RFID and barcodes providing data, source and read method authenticity. This work is done within ISO/IEC JTC 1/SC 31 Automatic identification and data capture techniques [16].

B. Sensors

Many IoT devices have sensors that can register changes in temperature, light, pressure, sound and motion. They are your eyes and ears to what's going on the world. Before we talk about what they do, let's describe them. These sensors are part of a device category called a micro electromechanical system (MEMS) and are manufactured in much the same way microprocessors are manufactured, through a lithography process [9]. These sensors can be paired with an application-specific integrated circuit or an ASIC. This is a circuit with a limited degree of programming capability and is hardwired to do something specific. It can also be paired with microprocessor and will likely be attached to a wireless radio for communications.

For example, you are away on vacation and the house is empty. A moisture sensor detects water on the basement floor. That sensor finding is processed by an app, which has received another report from a temperature sensor that detects the flow of water in the main water pipe. When water automobile during production can be used to track its progress through the assembly line; RFID-tagged pharmaceuticals flows, it takes away heat and lowers the temperature. That both sensors are detecting anomalies is cause for concern. A high rate of flowing water may signal a burst pipe, triggering an automated valve shutoff; a slight water flow might be a running toilet, and the water on the basement floor by routine leakage from a heavy rain [13]. In either case, you get a machine-generated message describing the findings.

C. Internet Protocol (IPv6)

The original idea of the Auto-ID Center is based on RFID-tags and unique identification through the Electronic Product Code however this has evolved into objects having an IP address or URI [9]. An alternative view, from the world of the Semantic Web focuses instead on making all things (not just those electronic, smart, or RFID-enabled) addressable by the existing naming protocols, such as URI. The objects themselves do not converse, but other agents, such as powerful centralized servers acting for their human owners, may now refer them to **[11]**. The next generation of Internet applications using Internet Protocol Version 6 (IPv6) would be able to communicate with devices attached to virtually all human-made objects because of the extremely large address space of the IPv6 protocol [18]. This system would therefore be able to scale to the large numbers of objects envisaged. A combination of these ideas can be found in the current GS1/EPC global EPC Information Services (EPCIS) specifications. This system is being used to identify objects in industries ranging from aerospace to fast moving consumer products and transportation logistics [9].

D. Electronic Product Code (EPC)

An Electronic Product Code (EPC) is one common set of data stored in a tag. EPC's are coded on RFID tags because of which objects can be tracked and identified uniquely. The tag contains a 96-bit string of data. The first eight bits are a header, which identifies the version of the protocol [21]. The next 28 bits identify the organization that manages the data for this tag; the EPC Global consortium 22 assigns the organization number. The next24 bits are an object class, identifying the kind of product; the last 36 bits are a unique serial number for a particular tag. These last two fields are set by the organization that distributed the tag (WIKIPEDIA, 2013). Rather like a URL, the entire electronic product code number can be used as a key into a global database to exclusively identify a particular product [23].

E. Optical tags and quick response codes

This is used for low cost tagging. Phone camera decodes QR code using image-processing techniques [12]. In reality QR advertisement campaigns gives less turnout, as users need to have another application to read QR codes 0[11].

F. 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 [56]. Barcodes 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

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

machine-readable. Usually laser scanners read them, they can also be read using a cameras [24].

G. Wireless Fidelity (Wi-Fi)

Wireless Fidelity (Wi-Fi) is a networking technology that allows computers and other devices to communicate over a wireless signal [5]. 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 Wave LAN 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 [25]. Technology contains any type of WLAN product support any of the IEEE802.11 together with dual-band, 802.11a, 802.11b, 802.11g and 802.11n. Nowadays entire cities are becoming Wi-Fi corridors through wireless APs.

H. ZigBee

ZigBee is one of the protocols developed for enhancing the features of wireless sensor networks [5]. 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, and flexible protocol design. It is a low power wireless network protocol based on the IEEE 802.15.4 standard [26]. ZigBee has range of around 100meters 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.

I. Bluetooth low energy

This is one of the latest technologies. All newly releasing smart phones have BLE hardware in them. Tags based on BLE can signal their presence at a power budget that enables them to operate for up to one year on a lithium coin cell battery [11].

J. 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 [56]. Philips and Sony companies first develop it. Data exchange rate now days approximately 424 kbps. Power consumption during data reading in NFC is under 15ma [34].

K. 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 [5]. Actuators typically are used in manufacturing or industrial applications. There are three types of actuators are (1) Electrical: ac and dc motors, stepper motors, solenoids (2) Hydraulic: use hydraulic fluid to actuate motion (3) 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 [36].

L. 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 [5]. 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 [26]. Sensors mounted to a patient's body are monitoring the responses to the medication, so that doctors can measure the effects of the medicines [27].

M. 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 (1) Embedded: Many Net- worked devices are integrated in to the environment (2) Context Aware: These devices can recognize you and your situational context (3) Personalized: They can be tailored to your needs (4) Adaptive: They can change in response to you (5) Anticipatory: They can anticipate your desires without conscious mediation [5].

V. APPLICATIONS OF IOT

The potentialities offered by the IoT make it possible to develop numerous applications based on it, of which only a few applications are currently deployed [11]. Internet of Things examples extend from smart connected homes to wearables to healthcare. In fact, IoT is slowly becoming part of every aspect of our lives. In future, there will be intelligent applications for smarter homes and offices, smarter transportation systems, smarter hospitals, smarter enterprises

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

and factories [15]. Not only are Internet of Things applications enhancing our comfort, but they also give us more control to simplify routine work life and personal tasks. In the following subsections, some of the important example applications of IoT are briefly discussed.

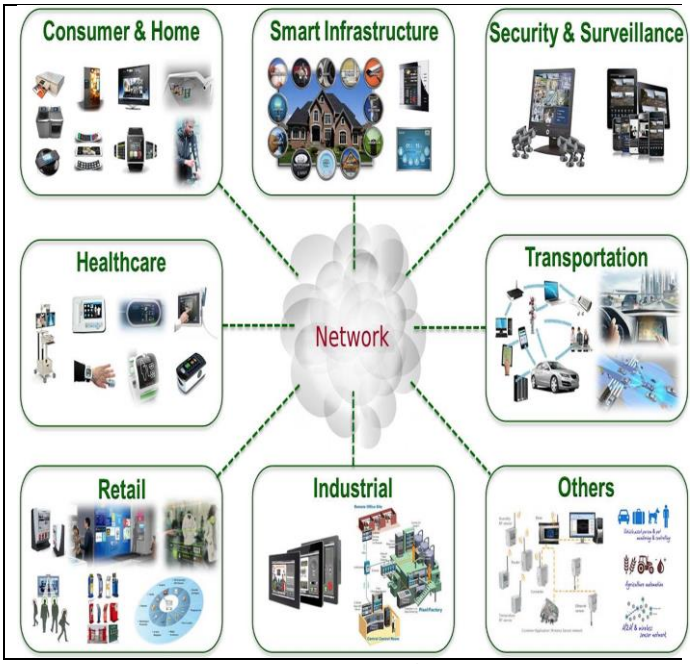

Fig. 19. Applications of IoT

A. Healthcare

The IoT is proposed to improve the quality of human life by automating some of the basic tasks that humans must perform. In that sense, monitoring and decision-making can be moved from the human side to the machine side [11]. One of the main applications of IoT in healthcare is in assisted living scenarios. Sensors can be placed on health monitoring equipment used by patients. The information collected by these sensors is made available on the Internet to doctors, family members and other interested parties in order to improve treatment and responsiveness Additionally, IoT devices can be used to monitor a patient's current medicines and evaluate the risk of new medications in terms of allergic reactions and adverse interactions [16].

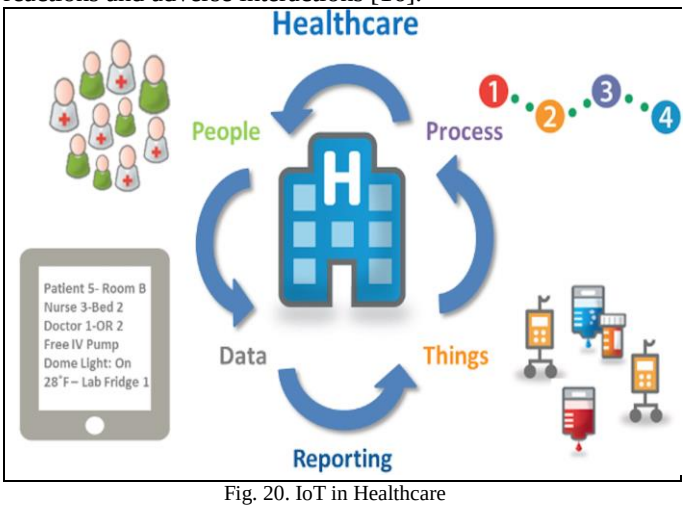

Fig. 20. IoT in Healthcare

B. Smart environments domain

1) Smart water sup ply

Smart cities must monitor water supply to ensure that there is adequate access for resident and business need. Wireless Sensor Networks provide the technology for cities to monitor their water piping systems more accurately and discover their greatest water loss risks [11]. Cities that are addressing water leakage problem with sensor technology are producing high savings from their investment. Tokyo, for example, has calculated they save $170 million each year by detecting water leakage problems early (LIBELIUM, 2013). The system can report pipe flow measurement data regularly, as well as send automatic alerts if water use is outside of an estimated normal range. This allows a smart city to determine the location of leaking pipes and prioritizes repairs based on the amount of water loss that could be prevented [41].

2) Smart homes and offices

Various electronic gadgets around us such as microwave ovens, refrigerators, heaters, air conditioners, fan and lights surround us. Actuators and sensors can be installed in these devices in order to utilize the energy sufficiently and also to add more comfort in life. These sensors can measure the outside temperature and even can determine the occupants inside the rooms and thereby control the amount of heating, cooling and flow of light etc. Doing all these can help us to minimize the cost and increase energy saving [11].

3) Improved gyms

Involving new technologies like a separate exercise profile, which can be installed on machines, can enhance the gymnasium experience and each person can be identified from his identification id alone and thereby, concerned profile will get activated [84].

4) Food sustainability

Food that we eat has to go through various stages before they arrive in the refrigerators. They are bound in a strict food cycle: production, harvesting, transportation and distribution. With the use of appropriate sensors, we can prevent the food from climatic damages by keeping a good eye on temperature, humidity, light, heat etc. [11]. Sensors can measure these variations precisely and notify the concerned person. Monitoring helps in prevention of possible plant.[85]

C. Transportation and logistics domain

1) Smart parking

The new Smart Parking sensor's to be buried in parking spaces to detect the arrival and departure of vehicles. The Smart parking provides extensive parking management solutions which helps motorists save time and fuel (LIBELIUM, 2013). A significant contribution to congestion arises from motorists searching for accessible parking spaces [11]. Providing accurate information about parking spaces helps traffic flow better, and this will also allow the deployment of application to book parking spaces directly from the vehicle [17]. This will help to reduce CO2 emissions and to minimize traffic jams.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

Fig. 21. Transportation and Logistics

2) 3D assisted driving

Vehicles like cars, buses and trains along with the roads and rails equipped with sensors may provide valuable information to the driver to provide better navigation and safety. With the use of assisted driving, we will be able to find the right track with prior information about traffic jams and incidents. In an Enterprise context, information about the vehicle transporting goods together with information about the type and status of the goods can integrate to provide valuable information about the delivery time, delivery delays and faults [86].

Fig. 22. Transportation [13]

3) Augmented maps

Tourist augmented maps with tags allow NFC-equipped phones to browse the information about the places and quickly connect it to the web services providing information about hotels, restaurants, monuments, theater and the local attractions. Hovering your mobile phone over the tag within its reading range so that the additional information about the marker can be displayed on the screen can do this.

4) Logistics

Implementing the Internet of Things in Retail chain monitoring has many advantages: RFID and NFC can be used to monitor almost every link of supply chain, ranging from commodity details, raw material purchasing, production, transportation, and storage, sale of product and after sales services. With the help of IoT, we will track the inventory in the warehouse so that stock can be refilled at the appropriate time for continuous sale and this will reduce the waiting time of customer which result in customer satisfaction, which further results in increased sales [28].

VI. ADVANTAGES OF IOT

There are many advantages of incorporating IoT into our lives, which can help individuals, businesses, and society on a daily basis. For individuals this new concept can come in many forms including health, safety, financially, and every day planning [29].

Following are the advantages of IoT (Internet of Things):

- IoT network benefits not one but all i.e. individuals, society, stake holders of businesses etc. due to the fact that IoT network saves time and money. IoT systems deliver faster and accurately with minimum utilization of energy. This improves quality of life.
- It is used for patient monitoring i.e. various types of wireless sensors are installed on the patient body, which communicate with the IoT network, and provides all the required information of the patient under treatment.
- IoT concept is used in home security devices, which are monitored and controlled either locally or remotely using easy to use applications available on mobile phones or smartphones. Typical IoT devices are security alarm; Camera, sensors, door lock etc. are used in home automation environment.
- IoT is used in asset and individual tracking, inventory control, energy conservation, shipping etc.
- It is similar to M2M but it has applications beyond M2M. M2M is used only for machine-to-machine communication. In IoT, things communicate themselves to its owner indicating its location and conditions.
- The integration of IoT into the health care system could prove to be incredibly beneficial for both an individual and a society.
- A chip could be implemented into each individual, allowing for hospitals to monitor the vital signs of the patient. By tracking their vital signs, it could help indicate whether or not serious assessment is necessary.
- With all of the information that is available on the Internet, it can also scare people into believing they need more care than what is really needed. Hospitals already struggle to assess and take care of the patients that they have. By monitoring individual's health, it will allow them to judge who

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

needs primary attention.

- The Internet of Things can also assist people with their personal safety. ADT, which is a home security system, allows individuals to monitor their security systems at home through their phones, with the ability to control it. Also, another technology that has already been released is GM OnStar. This is a system that is embedded in GM cars that can detect if a crash has occurred and it automatically calls 9-1-1. It can also track the movement of the car.
- IoT can also function as a tool that can save people money within their households. If their home appliances are able to communicate, they can operate in an energy efficient way.
- Finally, IoT can assist people with their everyday plans. A very interesting example that was given in a video was the communication between many devices that automatically adjusted to let an individual sleep in. Although this may sound unimportant, the misusage of time costs us "$135 billion a year" (Koreshoff, 2012). By allowing physical devices to communicate, it is taking the data that is individually collected, sharing it, and then translating the information into ways to make our current systems more efficient [30].
- Businesses can also reap many benefits from the Internet of Things. IoT can be useful in many different categories including asset tracking and inventory control, shipping and location, security, individual tracking, and energy conservation. As mentioned before, IoT allows for the communication between devices, commonly referred to as Machine-to-Machine (M2M) communication. With this being possible, physical devices are able to communicate to people letting them know their condition and where it is located.
- Devices such as trucks or ships allow for the maximum capacity to be filled by communication amongst devices and then relaying that information to a person to capitalize on the data supplied.
- All of these combined maximize revenue by cutting cost of inefficiencies within the business. A specific example from "A Successful 'Internet of Things' Hinges on M2M" article, is the operation of Nestles Nespresso Coffee Machine, which has "the ability to monitor factors such as temperature setting, vibration, and pressure helps ensure quality output, potentially leading to greater customer satisfaction and continued repeat business" (Frenzel, 2012). Although the idea seems quite simple, it can be very advantageous for a company to utilize the IoT to ensure quality service is given to their customers.
- Another advantage of IoT is the ability to track individual consumers and targeting these consumers based on the information supplied by the devices. In a way, it provides a more "personalized" system that could potentially increase business sales and increases their demographic. Additionally, with the increased amount of devices connected to the Internet the Smart Grid expands, conserving more energy (Frenzel, 2012).
- Devices can make decisions and adapt without human guidance to reduce their energy usage. The IoT has many advantages to businesses, individuals, consumers, the environment, and society, but as with any technology, there are always repercussions and controversies that arise.

The Major Advantages of IoT

Communication: IoT encourages the communication between devices, also famously known as Machine-to-Machine (M2M) communication. Because of this, the physical devices are able to stay connected and hence the total transparency is available with lesser inefficiencies and greater quality [31].

Automation and Control: Due to physical objects getting connected and controlled digitally and centrally with wireless infrastructure, there is a large amount of automation and control in the workings. Without human intervention, the machines are able to communicate with each other leading to faster and timely output.

Information: It is obvious that having more information helps making better decisions. Whether it is mundane decisions as needing to know what to buy at the grocery store or if your company has enough widgets and supplies, knowledge is power and more knowledge is better.

Monitor: The second most obvious advantage of IoT is monitoring. Knowing the exact quantity of supplies or the air quality in your home can further provide more information that could not have previously been collected easily. For instance, knowing that you are low on milk or printer ink could save you another trip to the store in the near future. Furthermore, monitoring the expiration of products can and will improve safety.

Time: As hinted in the previous examples, the amount of time saved because of IoT could be quite large. And in today's modern life, we all could use more time.

Money: **T**he biggest advantage of IoT is saving money. If the price of the tagging and monitoring equipment is less than the amount of money saved, then the Internet of Things will be very widely adopted. IoT fundamentally proves to be very helpful to people in their daily routines by making the appliances communicate to each other in an effective manner thereby saving and conserving energy and cost. Allowing the data to be communicated and shared between devices and then translating it into our required way, it makes our systems efficient. Automation of daily tasks leads to better monitoring of devices. The IoT allows you to automate and control the tasks that are done on a daily basis, avoiding human intervention. Machine-to-machine communication helps to maintain transparency in the processes. It also leads to uniformity in the tasks. It can also maintain the quality of

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

service. We can also take necessary action in case of emergencies.

Efficient and Saves Time: The machine-to-machine interaction provides better efficiency, hence; accurate results can be obtained fast. This results in saving valuable time. Instead of repeating the same tasks every day, it enables people to do other creative jobs.

Saves Money: Adopting this technology and keeping the devices under surveillance can achieve optimum utilization of energy and resources. We can be alerted in case of possible bottlenecks, breakdowns, and damages to the system. Hence, we can save money by using this technology.

Better Quality of Life: All the applications of this technology culminate in increased comfort, convenience, and better management, thereby improving the quality of life [31].

VII. DISADVANTAGES OF IOT

- Three of the main concerns that accompany the Internet of Things are the breach of privacy, over-reliance on technology, and the loss of jobs.
- When anything is put on the Internet it will always be there. Of course there are security measures that are taken to protect information, but there is always the possibility of hackers breaking into the system and stealing the data. For example, Anonymous is a group of individuals that hacked into federal sites and released confidential information to the public. Meanwhile the government is supposed to have the highest level of security, yet their system was easily breached. Therefore, if all of our information is stored on the Internet, people could hack into it, finding out everything about individuals lives [32].
- Also, companies could misuse the information that they are given access to. This is a common mishap that occurs within companies all the time. Just recently Google got caught using information that was supposed to be private. Information, such as the data collected and stored by IoT, can be immensely beneficial to companies.
- The privacy issues also leads to the question of who will control the Internet of Things? If there is only one company, that could potentially lead to a monopoly hurting consumers and other companies. If there are multiple companies that are given access to the information acquired, doesn't that breach consumers privacy? Also, where is the information going to be stored? Phone service suppliers such as Verizon and AT&T are no longer offering unlimited data usage for mobile phones because it is too costly, yet by 2020 it is expected that 50 billion devices will be connected, collecting and storing data (Evans, 2011).
- Another argument against IoT is the over-reliance on technology. As time has progressed, our current generation has grown up with the readily availability of the Internet and technology in general. However, relying on technology on a day-to-day basis, making decisions by the information that it gives up could lead to devastation. No system is robust and fault-free. We see glitches that occur constantly in technology, specifically involving the Internet. Depending on the amount that an individual relies on the information supplied could be detrimental if the system collapses. The more we entrust and the more dependent we are on the Internet could lead to a potentially catastrophic event if it crashes.
- Finally the connecting of more and more devices to the Internet will result in the loss of jobs. The automation of IoT will have a devastating impact on the employment prospects of less-educated workers (Schumpeter, 2010). For example, people who evaluate inventory will lose their jobs because devices can not only communicate between each other, but also transmit that information to the owner. We already are witnessing jobs being lost to automate machines, such as the checkout line in supermarkets and even ATM's. These disadvantages can be largely devastating to society as a whole, as well as individuals and consumers [31].

Compatibility: Currently, there is no international standard of compatibility for the tagging and monitoring equipment. I believe this disadvantage is the most easy to overcome. The manufacturing companies of this equipment just need to agree to a standard, such as Bluetooth, USB, etc. This is nothing new or innovative needed [11].

Complexity: As with all complex systems, there are more opportunities of failure. With the Internet of Things, failures could sky rocket. For instance, let's say that both you and your spouse each get a message saying that your milk has expired, and both of you stop at a store on your way home, and you both purchase milk. As a result, you and your spouse have purchased twice the amount that you both need. Or maybe a bug in the software ends up automatically ordering a new ink cartridge for your printer each and every hour for a few days, or at least after each power failure, when you only need a single replacement.

Privacy/Security**:** With all of this IoT data being transmitted, the risk of losing privacy increases. For instance, how well encrypted will the data be kept and transmitted with? Do you want your neighbors or employers to know what medications that you are taking or your financial situation?

Safety**:** Imagine if a notorious hacker changes your prescription, or if a store automatically ships you an equivalent product that you are allergic to, or a flavor that you do not like, or a product that is already expired. As a result, safety is ultimately in the hands of the consumer to verify any and all automation. As all the household appliances, industrial machinery, public sector services like water supply and transport, and many other devices all are

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

connected to the Internet, a lot of information is available on it. This information is prone to attack by hackers. It would be very disastrous if unauthorized intruder's access private and confidential information.

Compatibility: As devices from different manufacturers will be interconnected, the issue of compatibility in tagging and monitoring crops up. Although this disadvantage may drop off if all the manufacturers agree to a common standard, even after that, technical issues will persist. Today, we have Bluetooth-enabled devices and compatibility problems exist even in this technology! Compatibility issues may result in people buying appliances from a certain manufacturer, leading to its monopoly in the market.

Complexity: The IoT is a diverse and complex network. Any failure or bugs in the software or hardware will have serious consequences. Even power failure can cause a lot of inconvenience.

Lesser Employment of Menial Staff: The unskilled workers and helpers may end up losing their jobs in the effect of automation of daily activities. This can lead to unemployment issues in the society. This is a problem with the advent of any technology and can be overcome with education. With daily activities getting automated, naturally, there will be fewer requirements of human resources, primarily, workers and less educated staff. This may create Unemployment issue in the society.

Technology Takes Control of Life: Our lives will be increasingly controlled by technology, and will be dependent on it. The younger generation is already addicted to technology for every little thing. We have to decide how much of our daily lives are we willing to mechanize and be controlled by technology.

Scenarios**:** Imagine a scenario when: Your fridge can identify that you have run out of milk; it contacts the supermarket and orders the quantity you usually need, and also informs you by sending a message on your phone! Your alarm rings at 6:30 am; you wake up and switch it off. As soon as you switch off your alarm, it conveys to the geyser to heat water at a temperature you prefer and also the coffee maker starts brewing coffee! You are on your way while returning home from work and you use an app on your mobile to switch on the lights, the AC in your home, and tune the TV to your favorite channel so that your house is ready to welcome you before you even open your door! What would really make a refrigerator "smart" would be if it could read tags and alert owners when their food is about to reach their expiry date, for example. Or perhaps it could refer to an online calendar and make orders on a regular basis for certain items to be delivered. This technology has a lot of applications in various fields. Following are some possible areas where we can leverage the power of the Internet of Things (IoT) to solve day-to-day problems. However, it can be put to many more uses.

Smart Cities: The IoT can be used to monitor the vibrations of buildings, bridges, and monuments in case the building material is threatened or overloaded. Noise pollution can be controlled around hospitals and schools. It can be used to manage traffic especially during traffic jams, peak hours, accidents, and rains. It can be used to manage street lights—automatically switch them off in the presence of sunlight and switch them on at the onset of darkness. Another good application is alerting the officials to empty the trash bins when filled with waste.

Home Automation: The IoT can be used to remotely control and program the appliances in your home. It can be useful in detecting and avoiding thefts.

Industrial Automation: By using this technology, we can automate manufacturing processes remotely. It can also prove useful in optimizing the production processes. We can manage the inventory and the supply chain. We can also diagnose if the machines require repair and maintenance. We can monitor the emission of toxic gases to avoid damage to workers' health and the environment.

Health Monitoring: We can use this technology to identify health problems. The patterns of heart rate, pulse, digestive system, and blood pressure can be monitored and diagnosed for anomalies. The information can be sent to the doctor for analysis. The hospital can also be contacted in times of emergencies. This system will be very useful to senior citizens and disabled people who live independently.

Smart Environment: A very important application of IoT is detecting pollution and natural calamities. We can monitor the emissions from factories and vehicles to minimize air pollution. We can track the release of harmful chemicals and waste in rivers and the sea, thereby arresting water pollution. We can also keep tabs on the quality of water being supplied for drinking. We can send warnings of earthquakes and tsunamis by detecting tremors. We can keep the water level of rivers and dams under surveillance to be alert in case of floods. The detection of forest fire is also possible with this technology [87].

VIII. CHALLENGES OF IOT

Providing security for this giant technology is really challenging, mainly because there is not any boundary or limitation on the way that it can go. In this section we provide the possible challenges that the IoT will face. Connectivity Variety of wired and wireless connectivity standards is required to enable different application needs [11].

Power is critical: Many IOT applications need to run for year's over2batteries and reduce the overall energy consumption.

IOT is complex: IOT application development needs to be easy for all developers, not just to experts.

Government interest: If Government allows then only set up of I.O.T in a particular country is possible. Government allow only when they get profit from this new technology. Also depend very much upon the economy and revenue of the country.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

Compatibility: As devices from different manufacturers will be interconnected; the issue of compatibility in tagging and monitoring crops up. Although this disadvantage may drop off if all the manufacturers agree to a common standard, even after that, technical issues will persist [33]. Today, we have Bluetooth-enabled devices and compatibility problems exist even in this technology! Compatibility issues may result in people buying appliances from a certain manufacturer, leading to its monopoly in the market.

For IoT to achieve its vision, a number of challenges need to be overcome. Recently, many researchers have proposed IoT technology [8]. However, there are still a lot of challenges. In this section, we introduce the challenges of IoT and discuss them in detail. [75] To do this, we classify the challenges of IoT into three major categories of security, data capacity, and application. The first challenge to IoT is security. A number of things in IoT send data to each other using the Internet. That is a security weakness. In particular, many studies about the IoT have proposed the REST protocol. REST has a weakness of security because it does not maintain sessions when data is sent. [76] Therefore, it should resolve the weakness of security to provide IoT services. The second is data capacity. In IoT, many things send data to a web server or another thing. The backbone network for the IoT must support a huge amount of data. To do this, existing web servers must be expanded. In addition, the backbone network for the IoT must be accommodated. Therefore, the Content Centric Network (CCN) technology and big data technology should be used for the IoT. The last is the application of IoT. Recently a number of applications developed for smartphones and tablets. However, they are not related to the Internet of Things. Therefore, we need a variety of applications to realize the IoT. To do this, we should invigorate an ecosystem for the IoT and support a number of application developers [77].

A. Context awareness for privacy

For the security methods that are based on the context awareness, it is needed that any essential part in the context would be addressed effectively [20]. For example if the sensor because of the bad quality cannot recognize an image, the security enforcements cannot be applied to that image. Some access features should be provided to supply the required information from context. Also, sometimes, automatic security management may work incorrectly in some context, mainly because it could not recognize the context. Providing context awareness is an essential challenge in IoT [78].

B. Digital device in a physical ambient

In recent years, in order to measure different information, coupling between physical environment and processor has been growing significantly. For instance, a car that can be driven by a computer in a center or a medicine for a patient will be used as the sensors employed on her body providing body situation [21]. However, if there would not be any guaranteed security, all these systems can be manipulated and attacked by different hacker, and cause harmful results [79].

For example in the above two cases, an attacker may bring up a lethal accident by driving the car in a wrong direction, or may kill the patient by ordering wrong medicine. Moreover, sometimes IoT devices are considered as intellectual property that they might be highly valuable; so, they need to be protected, and also, for the right of owner. However, it is an unavoidable that when a property is accessible through the physical environment, it can easily been misused by an attacker [56].

C. Identification in the IoT environment

Object and service identification is recognized as one of the main challenges on the way to developing global Internet of Things (IoT). Many identification services accessible these days with various means of generating and verifying identification for the enhanced personal information protection. However, it has not been clearly defined yet regarding what identification methods are purposely acceptable or how to use them in IoT environment.

In all layers of IoT, it is essential to provide identification. It is one of the biggest challenges based on the fact that IoT will face a tremendous number of applications and structures with different unpredictable characters and patterns. This matter will be worse even in the distributed environment, which is the main domain for IoT. This challenge stays valid even for bounded and closed environments. There are some hot researches considering algorithms, which are able to derive value from unstructured data to increase performance. There are different factors determining main criteria of an identifier, such as: governance, security and privacy. Also, lots of existing identification schemes have been created long time ago for local usage and for specific objectives. Therefore, the need to have a global reference for identification is vital [82].

D. Authenticating devices

Lots of devices that use the sensors and actuators should follow specific policy and proxy rules for authentication to authorize the sensors to public their information. Meanwhile, low cost solutions in this field have not been provided as much as needed [34]. Currently, if we want to provide the security for the sensors we have to use high-cost solutions, which is a conflict with the main goal of IoT to provide lightweight protocols [35].

E. Data Combination

We will have lots of different data produced by IoT. Combining these data to provide more comprehensible only providing a large group of new general security can do information policies, which leads us to a more complex user profile. However, these mechanisms even may put the security of users more in danger by sharing their information that may cause even harder challenges in this matter [80].

F. Scalability in IoT

As the technology grows the number of users and devices with different type of communication and technologies grow widely. IoT needs to provide interaction for unbounded number of entities with significant differences in the interaction patterns. Therefore, IoT has to provide capabilities based access control mechanisms, to ensure the security for this tremendous number of elements [36].

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

G. Secure Setup and Configuration

Solving the challenge of scalability of IoT has to implement in such a way of having a secure Setup and structure too. The basic design of the system can be implemented based on privacy. For example, a service can be designed in such a way that each user can manage a specific group of people being able of having access to the information, and the list of people can be managed dynamically [37]. Therefore, it is essential to provide security architecture with the appropriate mechanisms. In another point of view, having symmetric or asymmetric cryptographic credentials regarding the situations provides a more secure infrastructure. The process to build this structure is challenging, especially for the large number of devices that IoT will be faced with [81].

H. CI and IoT

The impact of development of IoT on the CI (Critical Infrastructure), such as: energy, telecom and utilities, need tobe cleared because IoT technology is going to be implied on the devices in CI, a clear example is the M2M (Machine to Machine) standardization activity. The new risks and new privacy issues that IoT may bring to CI are an avoidable challenge that should be considered. Moreover, providing security for IoT gets more important in this matter, because IoT in CI has to do with crucial CI's aspects, such as: providing safety to prevent industrial accidents, or supplying required services to have a constant electrical power for hospitals [21].

I. Conflicting market interest

IoT will make a very competitive market by providing correlated data from different sources. Therefore, it will help to satisfy costumers 'needs more efficiently. As a result, providing different techniques to protect the personal data of people will be the main issue at combing and correlating information. This goal should be satisfied by deployment low weight privacy solutions, which is considered as a challenge [21].

J. Considering IoT in an evolving Internet

The effect of Internet evolution is undeniable on IoT. The way that the Internet is used and the infrastructure of implementing Internet's elements are the two main aspects of effecting IoT.

However, data security and privacy have determining roles in evolving Internet. Preparing security and privacy protection for the Internet through standardization will create challenges in this field [83]. Hence, as the paper asserts, this evolution will raise different questions such as: If such an Internet environment becomes the "trusted" Internet would it be socially acceptable for IoT to remain outside? Can such an evolution indeed benefit IoT security and privacy? What are the implications for IoT governance? In another point of view any vendor should investigate any effect that can have on the Internet by designing its services if the product would be successful. Hence, it should be studied carefully to ensure that the new design would not harm the Internet in all different aspects such as bandwidth usage or latency in the communication environments [38].

K. Human IoT Trust relationship

There should be a specific level of trust that human can have on different part of IoT. Trust on the machines along with that human beings still can have the privacy has been considered widely by researchers. Trust can be defined as the level of confidence that is possible to have on specific service or entity. However, trust is not defined only for human beings, it can even be defined for systems or machines, for example for webpages, which shows the level of trust in the digital society. In another point of view, trust can be defined as how much we can be sure that system is doing its job in the required way and providing true information. Moreover, in the M2M communications in an IoT domain, each device should have the knowledge about that how much it can trust on the machine to transfer important and sensitive information. This statement is true even for a machine that is sending crucial information to a person; in such a way that important information should not be in access of any wrong person. As a result, trust can be defined in three ways; first, how much a user can trust ona machine; second, how much a device can trust on another device; third, how much a device can trust a user [21].

L Data management

Other perspective can be defined as how to manage the data. Cryptographic mechanisms and protocols usually are the best choices to protect data, but sometimes we may not be able to implement these techniques on small elements. Therefore, we should have policies regarding how to manage any type of data with various policy mechanisms. However, if this idea wants to be implemented, we should change many more current mechanisms [37].

M. Lifespan of every IoT's entities

The fact that any product in IoT should have a specific short lifespan, and would not survive for long years is undeniable. As an example, UDP (User Datagram Protocol) services provide a degree of amplification; which means that they respond with more data than they started to communicate with over UDP. [71] This amplification is the result of the fact the source address can be spoofed because UDP is connectionless. Hence this amplification will result in a powerful denial of service. Thus, any device, which implements such, a service will face to the instability of the Internet. Also the same scenarios with GSM (Global System for Mobile Communications), WEP (Wired Equivalent Privacy) and a number of other wireless protocols have shown that this assumption is incorrect [38].

In the above section, we got familiar with the current challenges that are on the long way of flourishing IoT. It is said that IoT will come into stage at 2020 and researchers are trying to find solutions for the weakness points of IoT. In the next section, we will talk about the solutions that have been proposed and implemented to provide a safer environment for this new promising technology.

IX. SECURITIES AND PRIVACY ISSUES OF IOT

Despite the immense potential of IoT in the various spheres, the whole communication infrastructure of the IoTis flawed from the security standpoint and is susceptible to loss of

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

privacy for the end users. Some of the most prominent security issues plaguing the entire developing IoT system arise out of the security issues present in the technologies used in IoT for information relay from one device to another. As such some of the prominent security issues stemming out from the communication technology are the following [39]:

A. Security issues

In the wireless sensor networks (WSNs):
The hierarchical relationship of the various security issues plaguing the wireless sensor network is shown in Figure 1.The oppressive operations that can be performed in a wireless sensor network can be categorized under three categories [40]
i. Attacks on secrecy and authentication
ii. Silent attacks on service integrity
iii. Attacks on network availability: The denial of service (DoS) ([41, 42] attack falls under this category. This prevention of accessibility of information to legitimate users by unknown third party intruders can take place on different layers of a network [43,44,45]

B. DoS attack on the physical layer:

The physical layer of a wireless sensor network carries out the function of selection and generation of carrier frequency, modulation and demodulation, encryption and decryption, transmission and reception of data [46]. This layer of the wireless sensor network is attacked mainly through
i. Jamming: In this type of DoS attack occupies the communication channel between the nodes thus preventing them from communicating with each other.
ii. Node tampering: Physical tampering of the node to extract sensitive information is known as node tampering.

C. DoS attack on the link layer:

The link layer of WSN multiplexes the various data streams, provides detection of data frame, MAC and error control. Moreover the link layer ensures point-point or point multipoint reliability [47].
The DoS attacks taking place in this layer are:
i. Collision: This type of DoS attack can be initiated when two nodes simultaneously transmit packets of data on the same frequency channel. The collision of data packets results in small changes in the packet results in identification of the packet as a mismatch at the receiving end. This leads to discard of the affected data packet for re-transmission [48]
ii. Unfairness: As described in, unfairness is is pleated collision based attack. It can also be referred to as exhaustion based attacks.
iii. Battery Exhaustion: This type of DoS attack causes unusually high traffic in a channel making its accessibility very limited to the nodes. Such a disruption in the channel is caused by a large number of requests (Request To Send) and transmissions over the channel [72].

D. DoS attack on the network layer:

The main function of the network layer of WSN is routing.
The specific DoS attacks taking place in this layer are:
i. Spoofing, replaying and misdirection of traffic.
ii. Hello flood attack: This attack causes high traffic in channels by congesting the channel with an unusually high number of useless messages. Here a single malicious node sends a useless message, which is then replayed by the attacker to create a high traffic [70].
iii. Homing: In case of homing attack, a search is made in the traffic for cluster heads and key managers which have the capability to shut down the entire network.
iv. Selective forwarding: As the name suggests, in selective forwarding, a compromised node only sends a selected few nodes instead of all the nodes. This selection of the nodes is done on the basis of the requirement of the attacker to achieve his malicious objective and thus such nodes doe's not forward packets of data.
v. Sybil: In a Sybil attack, the attacker replicates a single node and presents it with multiple identities to the other nodes.
vi. Wormhole: This DoS attack causes relocation of bits of data from its original position in the network. This relocation of data packet is carried out through tunneling of bits of data over a link of low latency.
vii. Acknowledgement flooding: Acknowledgements are required at times in sensor networks when routing algorithms are used. In this DoS attack, a malicious nodes poofs the Acknowledgements providing false information to the destined neighboring nodes

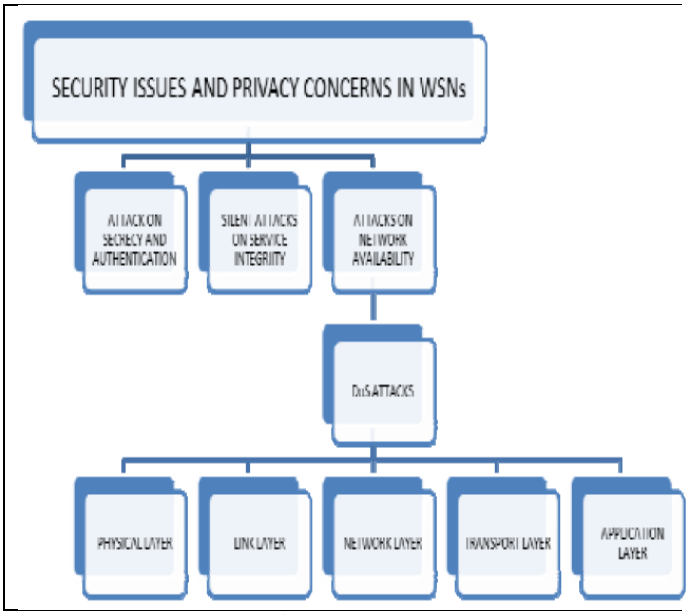

Fig. 23. Hierarchical diagram of security issues in Wireless Sensor Network

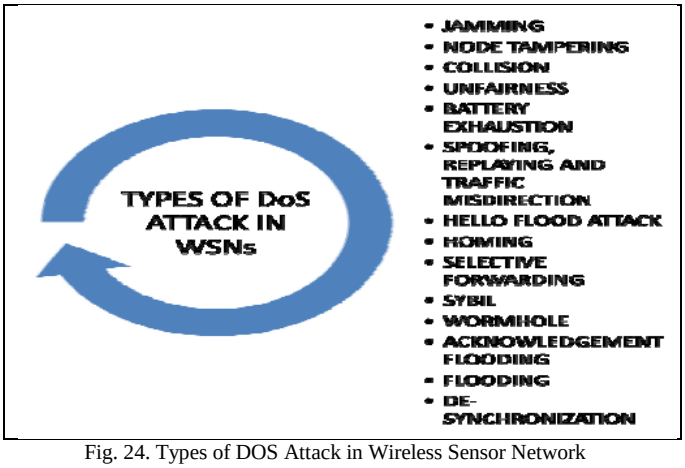

Fig. 24. Types of DOS Attack in Wireless Sensor Network

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

X. SOMECASE STUDIES OF IOT

A. Smart Gateway for Smart Meter

Guinard [9] provided a Smart Gateway for Smart Meters. In this paper, the author designed and implemented the prototype of smart gateways for a smart meter. With the prototype, the author is started by illustrating the application of the IoT architecture for monitoring and controlling the energy consumption of households [49]. Figure 2 shows the architecture of smart gateways for a smart meter. The smart gateway for a smart meter is divided into three layers. The first layer is devices and sensors, so-called ploggs. Each plogg communicates over Bluetooth or Zigbee. The second layer is a gateway. It is constructed of a miniature web server. Therefore, the data of ploggs is sent to the web via this gateway. Finally, the third layer is the mobile interface. Throughout this layer, a smart meter provides variety household services to users. The smart gateway supports service as follows: [69]

1. Local aggregates of device-level services
2.Various formats
3.Supports GET & POST method

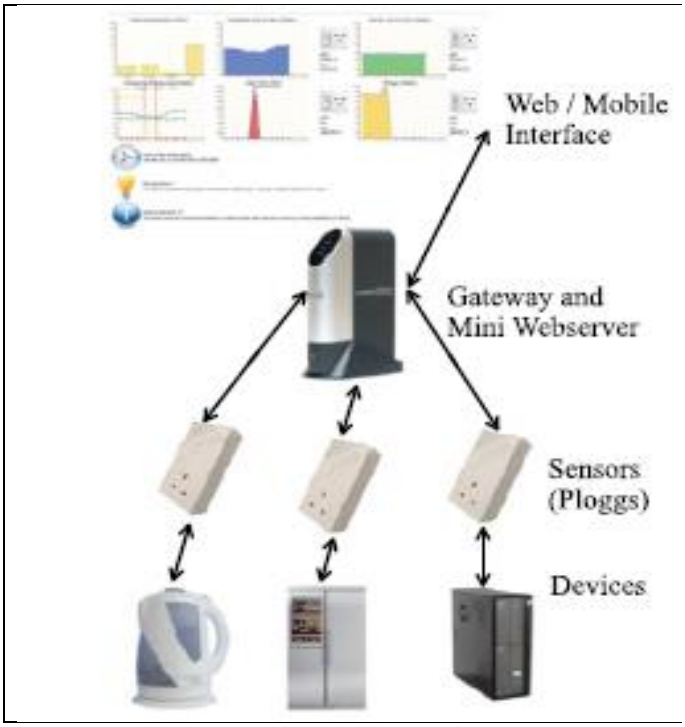

Fig. 25. Architecture of the smart gateway for smart meter

The smart gateway is a C++ embedded component with the role to automatically find all the Ploggs in the environment and make them available as web resources. In addition, a small footprint web server is used to enable access to each Plogg's functionality over the web. To implement this, the authors provide RESTful Ploggs and Sun SPOTs. Therefore, it uses the HTTP methods GET,
PUT, UPDATA, and DELET. In addition, to support the HTTP method, the authors implement Sun SPOTs, which run a small footprint Java Virtual Machine. Sun SPOTs are composed of two main parts: a software stack embedded on each node, and a proxy server to forward the HTTP requests from the Web to the SPOTs. This paper has contributed to a step toward the realization of the IoT by integrating things in the real world such as wireless sensor networks, embedded devices and household appliances with any other Internet content. In addition, this paper describes two ways to integrate devices to the Internet using REST, which directs integration based on advances in embedded computing, and a Smart Gateway-based approach for resource-limited devices [55].

B. Pachube

Pachube [50] is a well-known web site related to the IoT. Pachube, which pronounced patch-bay, connects people to devices, applications, and the IoT. It uses a web-based service, and manages the world's real-time data. Pachube gives people the power to share, collaborate, and make use of information generated in the world around them. Figure 4 shows the architecture of Pachube. In Figure 4, things are sent to the Pachube server to its own data using REST. And the Pachube server collects data and stores it in the database from things. Finally, the data provides a mash-up service with a Pachube Google Gadget. To do this, Pachube provides a native Application Programming Interface (API). Therefore, all devices use this API via an HTTP method to send data. In addition, Pachube provides a variety of web data formats such as JSON, XML, and CSV. Through this, users apply their service and can use web and mobile applications.

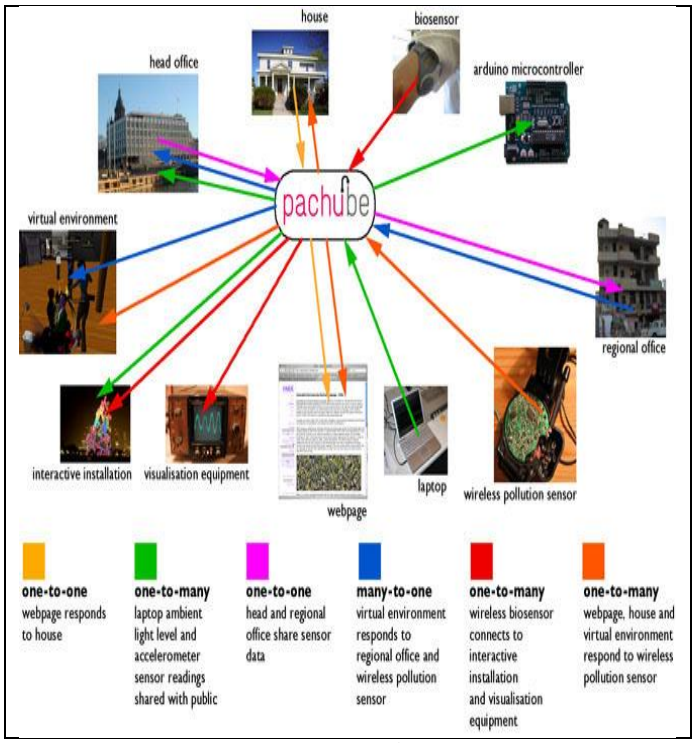

Fig. 26. Architecture of Pachube

C. Mobile Internet of Things (M-IoT)

The growing usage of connected devices, machines and vehicles is making organizations more effective and enriching the lives of individuals. To support the development of this Internet of Things (the IoT), the mobile industry is developing and standardizing a new class of

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

technologies that will help network operators to tailor the cost, coverage and power consumption of connectivity for specific IoT applications. Aimed at business leaders, this paper discusses low power, wide area (LPWA) technologies that will enable connected devices to have a battery life measured in years, rather than days or months [101].

Fig. 27. Mobile Internet of Things

Zhiyoung Shi [51] proposed the design and implementation of a mobile Internet of Things (M-IoT) based on a TDS CDMA network. The TD-SCMA is a well-known 3G service in China. The 3G TD-SCDMA networks are used as the basic network of transmitting information for the IoT. At the same time, the TD-SCDMA mobile terminal is integrated with an RFID reader. TD-SCDMA networks can provide high-bandwidth and high-speed information transmission channels for the IoT. In order to realize the information exchange between the TD-SCDMA network and the Internet of Things, the communication protocols of the Internet of Things are designed and implemented. The Figure 5 shows the network architecture. In addition, the author provides a communication protocol for the M-IoT. To do this, the author proposed two communication protocols, RFID tags-to-M-IoT and M-IoT-to-RFID tags. Figure 6 (a) shows a RFID tags-to-M-IoT communication protocol, and (b) shows M-IoT-to-RFID tags communication protocol. The communication protocols are modeled and simulated by OPNET. The results show that M-IoT can realize mobile information interactivity for both fixed and mobile objects. M-IoT based on a TDSCDMA network can not only expand the application of IoT, but also benefit from the promotion of TD-SCDMA network applications.

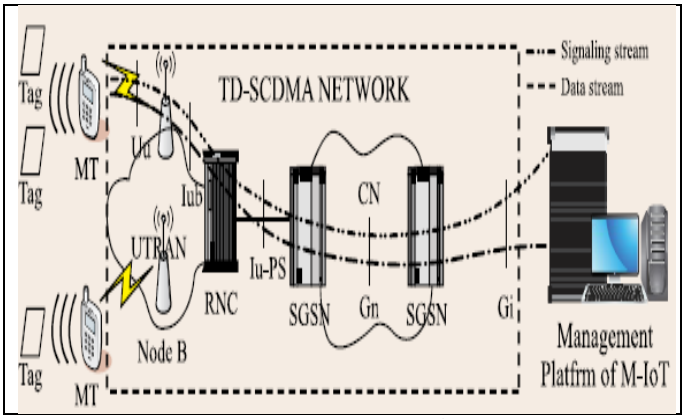

Fig. 28. Network Architecture of M-IoT

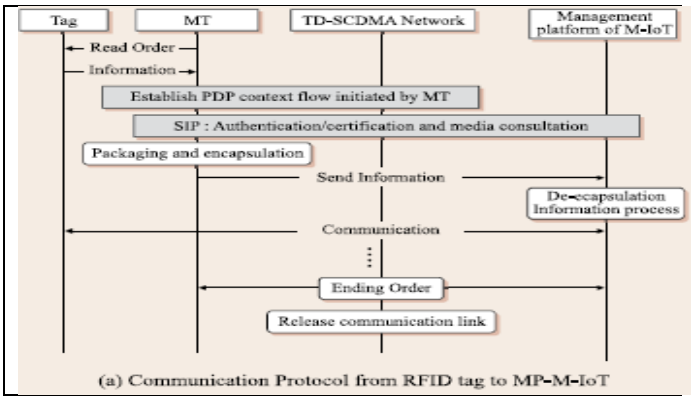

Fig. 29. (a) RFID tags-to-M-IoT communication Protocol

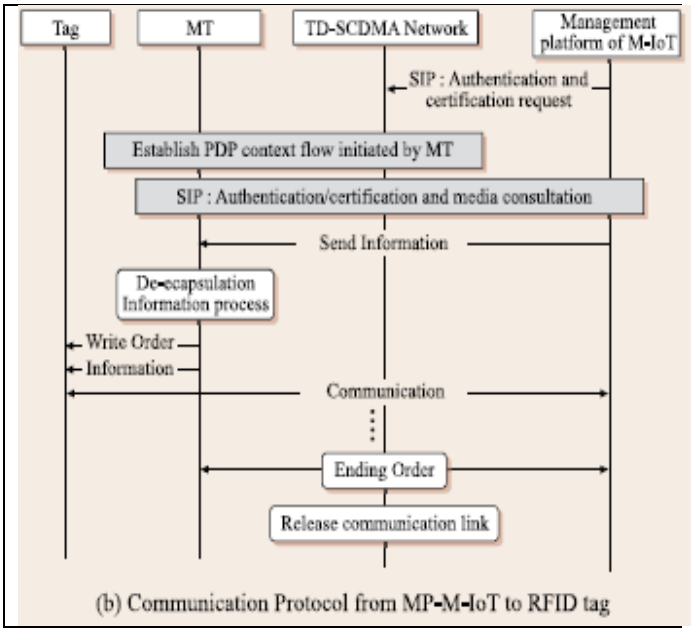

Fig. 29. (b) M-IoT-to-RFID tags communication protocol

D. Energy management system based On Energy collection

The IoT is a new communication and network paradigm, and various studies of the IoT have been conducted. Fortino proposed a multilayered agent-based architecture for the development of proactive, cooperating, and context-aware smart objects through a JADE-based middleware [102]. The multilayered agent-based architecture considered a wide

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

range of smart objects from reactive to proactive, from small to very large, and from stand-alone to social. Gubbi present a new vision for Internet of Things based on cloud [103]. Atzori analyzed the major opportunities arising from the integration of social networking concepts into the Internet of Things [104]. Cirani proposed a scalable and self-configuring architecture for large-scale IoT [105]. This architecture can provide autonomous services and resource discovery mechanisms with no human intervention to smart objects [106]. Qingbin Meng [52] proposed a design of an energy self-sufficient Internet of Things. In addition, this study initially achieves a system, which can provide energy permanently to the Internet of Things using solar energy and lithium batteries.

To do this, this paper proposed network model of the IoT, which is made up of a sensor network, transmission network, and application network [67]. First of all, the sensor network is like the skin and features of the IoT, and it can identify things and collect data. The sensor networks are constructed of RFID tags, RFID readers, cameras, GPS sensors, and terminal and sensor networks. Second, the transmission network is the nerve and the brain of the IoT and it can transmit and process data. The transmission network is constructed of an integrated network of communication and the Internet, a network management center, information center, and intelligent processing centers. Finally, the application network combines the division of labor of the IoT with industry needs to achieve a wide range of intelligence. The Figure 7 shows the structure of the IoT [68].

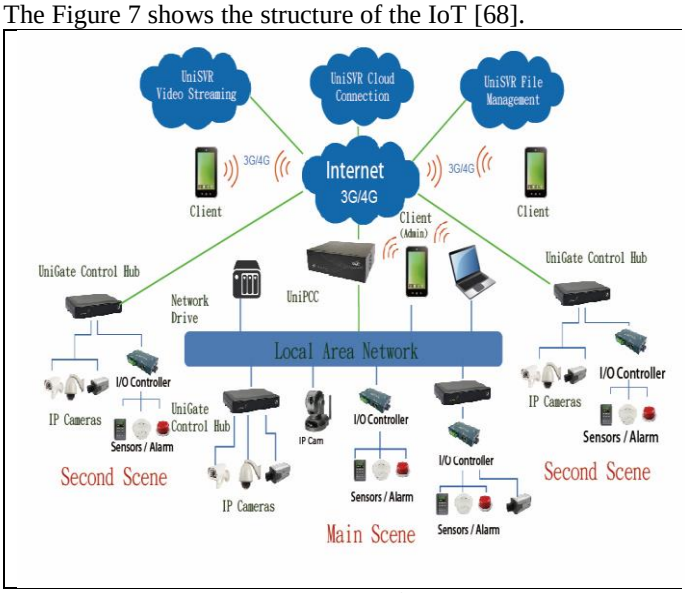

Fig. 30. Structure of IoT

In order to implement this, the author classifies three categories of central processing modules, external perception interfaces, and external communication interfaces. In the central processing module, they implement a terminal using a low-power embedded control system. The core processor of the embedded control system is S3C6410 ARM11, which is a low-cost, low power, and high performance microprocessor solution based on 16/32-bit RISC core. In an external perception interface, it mainly includes RFID readers, infrared sensors, environmental sensors, multi-channel analog sensor interfaces, and a multi-channel sensor interface. In an external communication interface, it is mainly divided into a cable communication interface and a wireless communication interface. The cable communication interface mainly includes RS485, RS232, USB and Ethernet cables. The wireless communication interface mainly includes the GSM, GPRS, Zigbee, WiFi, and Bluetooth modules. This paper adopts a modular design for the universal terminal structure of the IoT. In addition, the author initially achieves a system, which can provide energy permanently to the IoT using solar energy and lithium batteries. The system makes use of solar panels to enable nodes to add energy.

E. Design Food Quality Supervision Platform Based on the IoT

Bing Jia [53] proposed a method for constructing a quality supervision platform for the whole process of food production with the use of the IoT. In addition, the authors presented the crucial technology of constructing the platform and relevant implementation, including the associated matching algorithms between the RFID tags and on dimensional code, building methods of food quality modeled by the theory of ontology-based context modeling, and the combination and presentation methods of service functions for the different users. In order to use this system, the architecture of IoT was described as four layers, which included the object sense layer, data transmission layer, information integration layer, and application layer. Figure 8 shows the architecture design of PFQC-IoT. In the object sense layer, it used a two-dimensional barcode, RFID tags, and sensors to collect data. In the intelligent diagnosis layer, it integrated knowledge through a lot of business models. In the application service layer, it provided different functions according to different user roles.

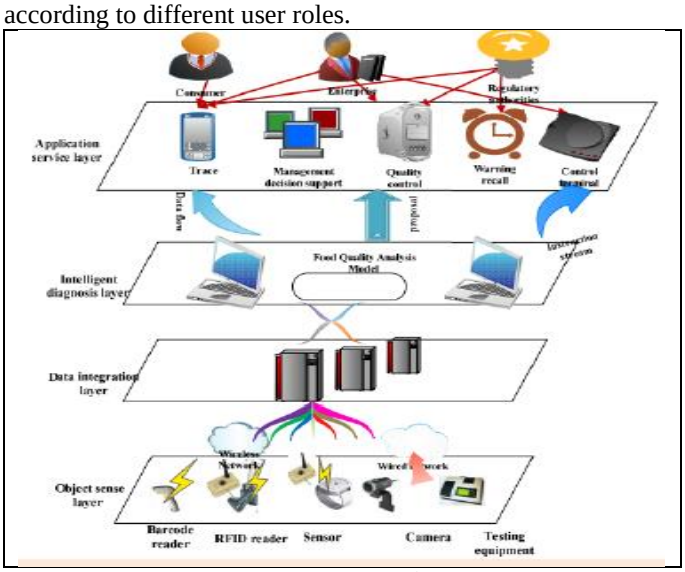

Fig. 31. Architecture design of PFQC-IoT

XI. SPECIFICATION OF WEB SERVICES IN IOT

A. SOAP

SOAP was originally part of the specification that included the Web Services Description Language (WSDL) and Universal Description, Discovery, and Integration (UDDI). It is used now without WSDL and UDDI. Instead of the discovery process described in the History of the Web Services Specification section below, SOAP messages are

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

hard-coded or generated without the use of a repository. SOAP commonly uses HTTP, but other protocols such as Simple Mail Transfer Protocol (SMTP) may by used. SOAP can be used to exchange complete documents or to call a remote procedure [88].

B. REST

REST (Representational state transfer) is an architectural style consisting of a coordinated set of architectural constraints applied to components, connectors, and data elements, within a distributed hypermedia system. REST appeals to developers because it has a simpler style that makes it easier to use than SOAP. It is also less verbose so that less volume is sent when communicating. REST ignores the details of component implementation and protocol syntax in order to focus on the roles of components, the constraints upon their interaction with other components, and their interpretation of significant data elements. [89].

C. UDDI

UDDI is defined as "a set of services supporting the description and discovery of businesses, organizations, and other Web services providers, the web services they make available, and the technical interfaces which may be used to access those services" by OASIS (The Organization for the Advancement of Structured Information Standards) . UDDI is an industry initiative that enables businesses to publish their services and allows potential users to discover these services [90].

D. WSDL

The Web Services Description Language (WSDL) forms the basis for the original Web Services specification. The following figure illustrates the use of WSDL. At the left is a service provider. At the right is a service consumer.

E. Technical Aspects of Web services in IoT

1) Cluster Discovery

Mobility plays an essential role in future networks, hence end users should be be able to benefit from the services offered by the premises/infrastructure where they are moving around. Cluster discovery is the first step to make end users aware of the services offered by a cluster of IoT devices. Energy consumption is a major parameter for cluster discovery, as the discovery mechanism should be frequently executed. Bluetooth, Bluetooth low energy and Wi-Fi technologies are typically used for device discovery in a mobile ad-hoc environment. In all these types are analyzed and the Bluetooth technology is chosen for device discovery. The eDiscovery algorithm based on Bluetooth technology is proposed in the research to discover the device. The simulation results show the efficiency of the eDiscovery algorithm over existing ones. Beacon stuffing methods for device discovery based on Wi-Fi technology. The score-based scanning approach is proposed in this work to make energy efficient device discovery.

Most of the device discovery mechanisms discussed in the literature are working on the MAC layer, however, for middleware services, these approaches are not suitable to apply. To overcome this limitation three algorithms i.e. connectivity based dynamic algorithm, a policy based scalable algorithm and a window-based broadcasting algorithm. After discovering the device, the user must provide his/her preferences and requirements through an interface to benefit from services offered by the cluster of devices. Hence, there is a need of energy efficient device discovery and a user guide to provide the users requirements and to discover and access the services. The research work will focus on, to design an energy efficient device discovery Algorithm [91].

2) Service Discovery

In the IoPTS scenario, there may be a large number of services will be available at specific location, however the user should only get relevant services as per his/her requirements. Service discovery is the process by which a user can identify services of his interest. It involves three roles: service provider, service requester and matchmaker. The service provider uses a published protocol to advertise the services that it can provide, the user /service requester uses a query protocol to request the service of his interest, and the matchmaker finds the service among all available services, which closely match with the user's preference [92].

TABLE. 1. DIFFERENCES BETWEEN THE IoT AND TRADITIONAL INTERNET

Topic	Traditional Internet	Internet of Things
Who creates content?	Human	Machine
How is the content consumed?	By request	By pushing information and triggering actions
How is the content combined?	Using explicit defined links	Through explicitly defined operators
What is the value?	Answer Questions	Action and timely information
What is done so far?	Both Content creation (HTML) and content consumption (search engines)	Mainly content creation

XII. THE FUTURE OF IOT

The recent hype about our IoT future has forced companies to consider the basic building blocks for the Internet of Things—i.e., hardware, software and support—to enable developers to deploy applications that can connect anything within IoT's scope. In this paper, we introduced the IoT and summarized case studies about the IoT. Through numerous Internet technology advances, the world is moving towards any time, any place, anyone connected paradigm. In the present context, "Things" are simply those computerized and networked devices that become part of the IoT. Some of those Things will be directly accessible over the Internet, whereas others would be supposedly hidden in local networks behind firewalls and address-translating routers. New applications and businesses are created continuously, and Internet content is always evolving. In this climate many researchers have proposed IoT technology. However, there are still a lot of challenges. In order to resolve these problems, we should overcome the challenges of the IoT. Therefore, future work requires resolution of these challenges. Grouping the web services required by user as well as their discovery is an important issue in IoT scenario. In the future, home automation, smart cities, intelligent

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

transport and e-health in such domain IoT applications can be developed. There are large numbers of devices that can sense the activity that are happening in the surrounding to provide services to the end users. Most of the IoT devices are capable of sensing environmental parameters but do not have the intelligence to give proper response depending on the sensed information. Hence, it is necessary that the IoT devices should be grouped in clusters. Users must be made aware of the presence of cluster to benefit from the services offered by it, and hence there is need of a cluster discovery mechanism [54]. Our message is intended as a wake-up call for computer professionals, but is also relevant to everyone involved as a user. We know the potential of IoT markets is huge, but some domains will mature more quickly than the rest. Here is Internet of Things application areas that have the potential for exponential growth.

XIII. CONCLUSIONS

IoT has been gradually bringing a sea of technological changes in our daily lives, which in turn helps to making our life simpler and more comfortable, though various technologies and applications. There is innumerable usefulness of IoT applications into all the domains including medical, manufacturing, industrial, transportation, education, governance, mining, habitat etc. Though IoT has abundant benefits, there are some flaws in the IoT governance and implementation level. The key observations in the literature are that (1) there is no standard definition in worldwide
(2) Universal standardizations are required in architectural level (3) Technologies are varying from vendor-vendor, so needs to be interoperable (4) for better global governance, we need to build standard protocols. Let us hope future better IoT [5]. The Internet has drastically changed the way we lived, as in scenario all the interaction is done over the Internet. The IoT has the potential to add a new dimension to this process by enabling communication between smart objects. IoT should be considered as a part of future internet as everything is going to be connected in a network so that objects can interact with each other, but still there are lots of issues which are to be solved to make this a reality. Lot of research is required in this field, once implemented successfully; the quality of life is improved because of the reduction of the effort made by humans on unimportant things. In this paper, we also presented the technologies and applications that can be used to make Internet of Things a reality. After that, we state some good examples where Internet of Things is of great use, and at last we discuss some open issues, which are still to be solved before the wide acceptance of this technology. Thus, from all the above, the contribution of our research could be useful in the literature especially in the field of IoT area, because provide a fulfill scheme concerning the application of IoT. The forces behind the development of Internet of Things, technology push forces and technology pull forces, see in the IoT a vast new market for the deployment of current and future information and communication technologies (ICT) that will help both the communication of devices. In this paper we also discussed a survey of the current technologies used in the IoT domain as of 2016. Currently, this field is in a very nascent stage. The technologies in the core infrastructure layers are showing signs of maturity. However, a lot more needs to happen in the areas of IoT applications and communication technologies. These fields will definitely mature and impact human life in inconceivable ways over the next decade.

ACKNOWLEDGEMENT

We would like to gratefully and sincerely thank to The Dean and Vice Dean of our College and Chairman of our Department for his guidance, understanding, patience, and most importantly, his friendly nature during this research paper. We would also like to thank my friends and colleagues, and the university who provided me an efficient support to work on this atmosphere and good infrastructure. We would also like to thank to all the previous researchers who worked very hard and helped others to comprehend the subject of Internet of Things (IoT).

REFERENCES

[1] Bradley Mitchell," Introduction to the Internet of Things (IoT)", https://www.lifewire.com/introduction-to-the-internet-of-things-817766
[2] John Soldatos," Internet of Things Tutorial: Introduction", http://www.kdnuggets.com/2016/12/internet-of-things-tutorial-chapter-1-introduction.html
[3] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010. ISBN: 978-1-4419-1673-0
[4] Internet of Things," https://aws.amazon.com/iot/"
[5] Somayya Madakam, R. Ramaswamy, SiddharthTripathi,"Internet of Things (IoT): A Literature Review", Journal of Computer and Communications, May 2015, Volume 3, 164-173, http://www.scirp.org/journal/jcc
[6] Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. (2011) Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. Advances in Internet of Things: Scientific Research, 1, 5-12.
[7] Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of "Internet of Things". First International Conference on Security of Internet of Things, Kerala, 17-19 August 2012, 51-56
[8] Min-Woo Ryu, Jaeho Kim, Sang-Shin Lee, and Min-Hwan Song, "Survey on Internet of Things: Toward Case Study", Smart Computing Review, vol. 2, no. 3, June 2012,pp 195-202
[9] Biddlecombe, E. (2009) UN Predicts "Internet of Things". Retrieved July 6.
[10] Butler, D. (2020) Computing: Everything, Everywhere. Nature, 440, 402-405.
[11] Ruchi Parashar1, Abid Khan2, Neha3,"A SURVEY: THE INTERNET OF THINGS",International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 4, Issue 3 (May-June, 2016), PP. 251-257
[12] Yinghui H., Guanyu L., 2010. Descriptive Models for Internet of Things. IEEE International Conference on Intelligent Control and Information Processing, Dalian, China, Pages: 483- 486.
[13] Bo Y., Guangwen H., 2008. Application of RFID and Internet of Things in Monitoring and Anticounterfeiting for Products. International Seminar on Business and Information, Wuhan, Hubei, China, Pages: 392- 395.
[14] [ongzhu Z., Xueping W., Jiangwei C., Xianghai L., Pengfei C., 2010 .Automotive recycling information management based on the internet of things and RFID technology. IEEE International Conference on Advanced Management Science (ICAMS), Changchun, China, page(s): 620 – 622
[15] Muriel D., Juan F., 2010. Expanding the learning environment: combining physicality and virtuality The Internet of Things for eLearning. IEEE International Conference on Advanced Learning Technologies (ICALT), Sousse, Tunisia, Pages: 730- 731.
[16] Mealling M, 2003 Auto-ID Object Name Service (ONS) v1.0, Auto-ID Center Working Draft
[17] https://en.wikipedia.org/wiki/Internet_of_Things
[18] Miao W., Ting L., Fei L., ling S., Hui D., 2010.Research on the architecture of Internet of things. IEEE International Conference on

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

Advanced Computer Theory and Engineering (ICACTE), Sichuan province, China, Pages: 484-487.
[19] Guangwen H., 2008. Application of RFID and Internet of Things in Monitoring and Anticounterfeiting for Products. International Seminar on Business and Information, Wuhan, Hubei, China, Pages: 392- 395
[20] Maede Zolanvari,Prof. Raj Jain,"IoT Security:ASurvey",http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_sec/index.html,pp 1-15
[21] TuhinBorgohain,UdayKumar,SugataSanyal,"Survey of Security and Privacy Issues of Internet of Things",Int. J. Advanced Networking and Applications Volume: 6 Issue: 4 Pages: 2372-2378 (2015) ISSN: 0975-0290,pp 2372-2378
[22] Jason Pontin: "ETC: Bill Joy's Technology Review, 29 Septemb November 2013
[23] Z.G. Prodanoff, Optimal frame si slotted ALOHA based RFID Communications (2009), 1016/j.comcom.2009.11.007
[24] Grieco A., Occhipinti, E. and Colombini, D. (1989) Work Postures and Musculo-Skeletal Disorder in VDT Operators. Bollettino de Oculistica, Suppl. 7, 99-111
[25] Pahlavan, K., Krishnamurthy, P., Hatami, A., Ylianttila, M., Makela, J.P., Pichna, R. and Vallstron, J. (2007) Handoff in Hybrid Mobile Data Networks. Mobile and Wireless Communication Summit, 7, 43-47
[26] Chen, X.-Y. and Jin, Z.-G. (2012) Research on Key Technology and Applications for the Internet of Things. Physics Procedia, 33,561-566
[27] Chorost, M. (2008) The Networked Pill, MIT Technology Review, March
[28] International Journal of Computer Science Engineering (IJCSE)Big Data on Internet of Things: Applications, Architecture, Technologies,Techniques and Future Directions
[29] Advantages of IoT,"Advantages of IoT | Disadvantages of IoT | Internet of Things",http ://www.rfwirelessworld.com/Terminology/Advantages-and-Disadvantages-of-IoT-Internet-Of-Things.html
[30] Advantages,"The Internet of Things",https://sites.google.com/a/cortland.edu/the-internet-of-things/advantages
[31] Bhaskara Reddy Sannapureddy,"Pros & Cons of Internet Of Things (IOT)",https://www.linkedin.com/pulse/pros-cons-internet-things-iot-bhaskara-reddy-sannapureddy
[32] Disdvantages , " The Internet of Things",https://sites.google.com/a/cortland.edu/the-internet-of-things/advantages
[33] Towards Internet of Things: Survey and Future Vision Omar Said o.saeed@tu.edu.sa IT/ College of Computers and Information Technology Taif University Taif, Saudi Arabia. Mehedi Masud mmasud@tu.edu.sa CS/ College of Computers and Information Technology Taif University Taif, Saudi Arabia
[34] Whitehouse, "Security of Things: An Implementers Guide to Cyber-Security for Internet of NCC Group Publications, Apr. 2014
[35] Raza Shahid, "Lightweight Security Solutions for the Internet of Things", Doctoral thesis, Mlard
[36] Malisa Vucinic, Bernard Tourancheau, Franck Rousseau, Andrzej Duda, Laurent Damon, Robert
[37] Rodrigo Roman, Pablo Najera, Javier Lopez, "Securing the Internet of Things", Computer Societ 58, Sep. 2011
[38] Whitehouse, "Security of Things: An Implementers Guide to Cyber-Security for Internet of NCC Group Publications, Apr. 2014
[39] TuhinBorgohain, UdayKumar,SugataSanyal,"Survey of Security and Privacy Issues of Internet of Things",Int. J. Advanced Networking and ApplicationsVolume: 6 Issue: 4 Pages: 2372-2378 (2015) ISSN: 0975-0290,pp 2372-2378
[40] [AashimaSingla, RatikaSachdeva, "Review on Security Issues and Attacks in Wireless Sensor Networks" International Journal of Advanced Research in Computer Science and Software Engineering <www.ijarcsse.com>. Volume 3, Issue 4, April 2013 ISSN: 2277 128X
[41] M. Sharifnejad, M. Shari, M. Ghiasabadi and S. Beheshti, "A Survey on Wireless Sensor Networks Security", SETIT, (2007)
[42] B. T. Wang and H. Schulzrinne, "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, vol. 2, (2004)May 2-5, pp. 901-904
[43] Sen, Jaydip. "Security and privacy challenges in cognitive wireless sensor networks." arXiv preprint arXiv: 1302.2253 (2013)
[44] M. Saxena,"Security in Wireless Sensor Networks-A Layer based classification", Technical Report, Center for Education and Research in Information Assurance &Security-CERIAS, Purdue University. pages.cs.wisc.edu/~msaxena/papers/2007-04-cerias.pdf, (2007)
[45] J. Sen, "A Survey on Wireless Sensor network Security", International Journal of Communications Network and Information Security, vol. 1, no. 2, (2009) August, pp. 59-82
[46] http://sensors-and-networks.blogspot.in/2011/08 physical-layer-for-wireless-sensor.html
[47] Ahmad Abed AlhameedAlkhatib, and Gurvinder Singh Baicher. "Wireless sensor network architecture." International conference on computer networks and communication systems (CNCS 2012) IPCSIT.Vol. 35. 2012, pp. 11-15
[48] transmission [48] [Sunil Ghildiyal, Amit Kumar Mishra, Ashish Gupta, Neha Garg, "Analysis of Denial of Service (DoS) Attacks in Wireless Sensor Networks" IJRET: International Journal of Research in Engineering and Technology;eISSN: 2319-1163 | pISSN: 2321-7308
[49] Woo Ryu, Jaeho Kim, Sang-Shin Lee, and Min-Hwan Song, "Survey on Internet of Things: Toward Case Study", Smart Computing Review, vol. 2, no. 3, June 2012,pp 195-202]
[50] Web site, https://cosm.com/?Pachube_redirect=true
[51] Zhiyong Shi, Kui Liao, Shiping Yin, Qingbo Ou, "Design and Implementation of the Mobile Internet of Things based on TD-SCDMA network," *Information Theory and Information Security (ICITIS)*, 2010
[52] Qingbin Meng, Jie Jin, "The Terminal Design of the Energy Self-Sufficiency Internet of Things," *Control, Automation and Systems Engineering (CASE), 2011 International Conference on*, 2011
[53] Qingbin, Yongjian Yang, "The design of food quality supervision platform based on the Internet of Things," *Transportation, Mechanical, and Electrical Engineering (TMEE), 2011 International Conference on*, 2011
[54] Jyoti L. Khachane1, Latika R. Desai2,"Survey Paper on Web Services in IOT",International Journal of Science and Research (IJSR)ISSN (Online): 2319-7064,Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611,pp 635-637]
[55] StylianiChatziefthymiou and Sotirios K. Goudos,"A survey of IoT: Architecture, Applications and Future Vision",4th International conference on Modern Circuits and System Technologies, pp 1-3
[56] Madakam, R. Ramaswamy, SiddharthTripathi,"Internet of Things (IoT): A LiteratureReview",Journal of Computer and Communications, 2015, 3, 164-173 Published Online May 2015 in SciRes. http://www.scirp.org/journal/jcchttp://dx.doi.org/10.4236/jcc.2015.350 21,pp 164-173
[57] Lianos, M. and Douglas, M. (2000) Dangerization and the End of Deviance: The Institutional Environment. British Journal of Criminology, 40, 261-278
[58] Ferguson, T. (2002) Have Your Objects Call My Object. Harvard Business Review, June, 1-7
[59] Dodson, S. (2008) The Net Shapes up to Get Physical. Guardian
[60] Graham, M. and Haarstad, H. (2011) Transparency and Development: Ethical Consumption through Web 2.0 and the Internet of Things. Research Article, 7
[61] Jayavardhana, G., Rajkumar, B., Marusic, S. and Palaniswami, M. (2013) Internet of Things: A Vision, Architectural Elements, and Future Directions. Future Generation
[62] Shao, W. and Li, L. (2009) Analysis of the Development Route of IoT in China. Perking: China Science and Technology Information, 24, 330-331
[63] Luigi A., Antonio I., Giacomo M. 2010.The Internet of Things: A survey. Science Direct journal of Computer Networks, Volume 54, Pages: 2787–2805
[64] Zouganeli E., Einar Svinnset I., 2009. Connected Objects and the Internet of Things – a Paradigm Shift. International Conference on Photonics in Switching, Pisa, Italy, Pages: 1-4
[65] Tongzhu Z., Xueping W., Jiangwei C., Xianghai L., Pengfei C., 2010 .Automotive recycling information management based on the internet of things and RFID technology. IEEE International Conference on Advanced Management Science (ICAMS), Changchun, China, page(s): 620 – 622
[66] Gustavo G, Mario O., Carlos K., 2008. Early infrastructure of an Internet of Things in Spaces
[67] Gubbi, Buyya, Marusic, Palaniswami,Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems 29 (2013) 1645-1660
[68] Zanella ,Bui, Castellani, Vangelista, Zorzi, Internet of Things for Smart Cities, IEEE Internet of Things journal, VOL. 1, NO. 1, February 2014
[69] Palatella ,Accettura, Vilajosana, Watteyne, Grieco, Boggia, Dohler, Standarized Protocol Stack for the Internet of (Important) Things, IEEE

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

Communications Surveys & Tutorials, VOL. 15, NO. 3, THIRD QUARTER 2013
[70] Huang, Li, A Semantic Analysis for Internet of Things, 2010 International Conference on Intelligent Computation Technology and Automation
[71] Singh, Tripathi, Jara, A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services, 2014 IEEE World Forum on Internet of Things (WF-IoT)
[72] Shin, A socio-technical framework for Internet-of-Things design: A human-centred design for the Internet of Things, Telematics and Informatics 31 (2014) 519–531
[73] Louis COETZEE, Johan EKSTEEN, "The Internet of Things – Promise for the Future? An Introduction," in Proc. of IST-Africa 2011 Conference, 2011
[74] A. Gavras, A. Karila, S. Fdida, M. May, and M. Potts, "Future Internet research and experimentation," ACM SIGCOMM Computer Communication Review, vol. 37, 2007
[75] IEEE SA 21451-7-2011, "IEEE Information technology--Smart transducer interface for sensors and actuators--Part 7: Transducers to radio frequency identification (RFID) systems communication protocols and transducer electronic data sheet (TEDS) formats," Sensor and RFID Integration Working Group (SRFID), 2011
[76] Uckelmann. Dieter, Isenberg. Marc-André, Teucke. Michael, Halfar. Harry, Scholz-Reiter. Bernd, An integrative approach on Autonomous Control and the Internet of Things," Unique Radio Innovation for the 21st Century: Building Scalable and Global RFID Networks, pp. 163-181, April 2011.
[77] Qingbin Meng, Jie Jin, "The Terminal Design of the Energy Self-Sufficiency Internet of Things," Control, Automation and Systems Engineering (CASE), 2011 International Conference on, 2011
[78] Bin Guo, Daqing Zhang, Zhu Wang, "Living with Internet of Things, The Emergence of Embedded Intelligence," ITHINGSCPSCOM '11 Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Sep 2011
[79] Bhattasali, Tapalina, Rituparna Chaki, and SugataSanyal. "Sleep Deprivation Attack Detection inWireless Sensor Network." arXiv preprint arXiv:1203.0231(2012)
[80] G. Bianchi, "A comparative study of the varioussecurity approaches used in wireless sensor networks,"International Journal of Advanced Science andTechnology, vol. 17, (2010)April, pp. 31-44
[81] Roy, Bibhash, Suman Banik, Parthi Dey, Sugata Sanyaland Nabendu Chaki, "Ant colony based routing formobile ad-hoc networks towards improved quality ofservices." Journal of Emerging Trends in Computingand Information Sciences 3.1 (2012): 10-14
[82] Vipul Goyal, Ajith Abraham, Sugata Sanyal and SangYong Han, "The N/R One Time Password System."Information Assurance and Security Track (IAS'05),IEEE International Conference on InformationTechnology: Coding and Computing (ITCC'05), USA,April, 2005. pp 733-738, IEEE Computer Society
[83] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures",Elsevier'sAdHoc Networks Journal, Special Issue onSensor Network (SNPA), (2003)September, pp. 293-315
[84] D. Guinard, T. Vlad, Towards the web of things: web mashups for embedded devices, in: Proceedings of the International World WideWeb Conference 2009 (WWW 2009), Madrid, Spain, April 2009.
[85] A.M. Vilamovska, E. Hattziandreu, R. Schindler, C. Van Oranje, H. DeVries, J. Krapelse, RFID Application in Healthcare – Scoping andIdentifying Areas for RFID Deployment in Healthcare Delivery, RANDEurope, February 2009.
[86] J. Sung, T. Sanchez Lopez, D. Kim, The EPC sensor network for RFIDand WSN integration infrastructure, in: Proceedings of IEEEPerComW'07, White Plains, NY, USA, March 2007.
[87] G. Broll, E. Rukzio, M. Paolucci, M. Wagner, A. Schmidt, H. Hussmann,PERCI: pervasive service interaction with the internet of things, IEEEInternet Computing 13 (6) (2009) 74–81
[88] Zhang, Lili, et al. "Research on IOT RESTful Web Service Asynchronous Composition Based on." Intelligent Human-Machine Systems andCybernetics (IHMSC), 2014 Sixth InternationalConference on. Vol. 1. IEEE, 2014
[89] Gao, Ruiling, et al. "Web-based motion detectionsystem for health care."Computer and InformationScience (ICIS), 2015 IEEE/ACIS 14th InternationalConference on. IEEE, 2015
[90] Chakraborty, Dipanjan, et al. "Toward distributedservice discovery in pervasive computingenvironments." Mobile Computing, IEEE Transactionson 5.2 (2006): 97-112
[91] Rambold, Michael, et al. "Towards autonomic servicediscovery a survey and comparison." ServicesComputing, 2009. SCC'09. IEEE InternationalConference on. IEEE, 2009
[92] Rong, Wenge, and Kecheng Liu. "A survey of context aware web service discovery: from user'sperspective." Service Oriented System Engineering(SOSE), 2010 Fifth IEEE International Symposium on.IEEE, 2010.
[93] Miao Wu, Ting-Jie Lu, Fei-Yang Ling, Jing Sun and Hui-Ying Du, "Research on the architecture of Internet of Things," 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), Chengdu, 2010, pp. V5-484-V5-487.doi: 10.1109/ICACTE.2010.5579493
[94] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," IEEE Software, vol. 33, no. 1, pp. 112–116, 2016.
[95] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): a vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
[96] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: a platform for internet of things and analytics," in Big Data and Internet of Things: A Road Map for Smart Environments, pp. 169–186, Springer, Berlin, Germany, 2014.
[97] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proceedings of the 1st ACM MCC Workshop on Mobile Cloud Computing, pp. 13–16, 2012.
[98] I. Stojmenovic and S. Wen, "The fog computing paradigm: scenarios and security issues," in Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS '14), pp. 1–8, IEEE, Warsaw, Poland, September 2014.
[99] M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," in Proceedings of the 2nd IEEE International Conference on Future Internet of Things and Cloud (FiCloud '14), pp. 464–470, Barcelona, Spain, August 2014.
[100] Pallavi Sethi ,Smruti R. Sarangi," Internet of Things: Architectures, Protocols, and Applications",Journal of Electrical and Computer Engineering Volume 2017 (2017), Article ID 9324035, 25 pages, https://doi.org/10.1155/2017/9324035
[101] https://www.gsma.com/iot/mobile-internet-of-things-industry-paper/
[102] Fortino G., Guerrieri A., Russo W.Agent-oriented smart objects developmentProceedings of the 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD '12)May 2012Wuhan, ChinaIEEE90791210.1109/cscwd.2012.62219292-s2.0-84864195643
[103] Gubbi J., Buyya R., Marusic S., Palaniswami M.Internet of Things (IoT): a vision, architectural elements, and future directionsFuture Generation Computer Systems20132971645166010.1016/j.future.2013.01.0102-s2.0-84876943063
[104] Atzori L., Iera A., Morabito G.From 'smart objects' to 'social objects': the next evolutionary step of the internet of thingsIEEE Communications Magazine20145219710510.1109/mcom.2014.67100702-s2.0-84893373985
[105] Cirani S., Davoli L., Ferrari G., Leone R., Medagliani P., Picone M., Veltri L.A scalable and self-configuring architecture for service discovery in the internet of thingsIEEE Internet of Things Journal20141550852110.1109/JIOT.2014.23582962-s2.0-84908447810
[106] Jongbae Kim, Jinsung Byun, Daebeom Jeong, Myeong-in Choi, Byeongkwan Kang, Sehyun Park,"An IoT-Based Home Energy Management System over Dynamic Home Area Networks",International Journal of Distributed Sensor Networks,January 1, 2015
[107] Daniel Burrus, Burrus Research,"The Internet of Things Is Far Bigger Than Anyone Realizes", https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

Author's Info

Mohd Muntjir is working in Department of Information Technology, College of Computers and Information Technology Taif University at Taif Saudi Arabia. He received his M.C.A. degree from H.N.B. Garhwal University Uttarakhand India and Ph.D. degree in Computer Science from OPJS University, Rajasthan India. He is a member of professional societies like ACM, IEEE, VAS, IJETAE, and CSTA. His interested are mainly in Database Management Systems, E-Learning, Data Mining and IoT (Internet of Things). The author has published many research papers in distinctive journals, conferences and books/book Chapters.

Mohd Rahul is working in Department of Information Technology, College of Computers and Information Technology Taif University at Taif Saudi Arabia. He has obtained his Ph.D. Degree form OPJS University Rajasthan India. Mohd Rahul received M.C.A. degree from Punjab Technical University Jalandhar, India and M.Tech (IT) degree from KSO University Karnataka, India. His research interests are Cloud Computing, Computer Networks, routing protocols, and IoT (Internet of Things). Mohd Rahul has published many research papers in distinctive journals, conferences and books and book Chapters.

Dr. Hesham Alhumyani is working in Department of Computer Engineering in College of Computers and Information Technology Taif University at Taif Saudi Arabia. He has obtained his Ph.D. Degree from University of Connecticut Storrs, USA. His research interests are Wireless Sensor Networks, Underwater Sensing, IoT (Internet of Things), and Cloud Computing. Dr. Hesham Alhumyani has published many research papers in distinctive journals and conferences.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)