OVERVIEW OF THE IOT THAT MEETING SOCIETAL CHALLENGES

By

Prof. Mohamed M. El Hadi

Sadat Academy for Management Sciences

Abstract

The Internet of Things (IoT) is rapidly becoming a reality that surround us and intersects with many aspects of our lives. Pervasive connectivity and advances in information and communication technologies (ICTs) have made possible the connection of more devices to the Internet. This is leading to a new wave of applications that have the potential to dramatically improve the way people live, learn, work and entertain themselves. Sensors play a key role in connecting the physical world (such as temperature, Co2, light, noise, moisture) with the digital world of IoT. Availability of this data can make us more productive and less reactive in our interaction without the world around us (Evans, 2011). The IoT is considered the next evolution of the Internet. The success of IoT will be driven by applications that deliver tangible improvements to people's everyday lives. Sensors are likely to play a central role in providing the data streams upon which these applications can be built. For example, mobile and home-based environmental monitors allow people to trace ambient air quality. They can use that data to either modify their environment or alter health and wellness. As a value and impact of these applications reach widespread the need for both improved and new sensor technologies is likely to grow rapidly.

This paper is consisting of nine main sections presenting introductory section highlighting the overview of IT from the research design; the 2nd section reviews some selected literature regarding IoT evolution and characteristics; the 3rd and 4th sections present the 10T layered architecture as well as IoT elements; the 5th one pinpoints to the main technologies surrounding IoT; while the 6th section presents briefly the overall architecture developed for IoT; in the meantime, the 7th section highlights some of the IoT societal benefits and challenges and problems; the 8th section demonstrates the successful implementation of IoT as related to the middleware and communication model; The final 9th section indicates the conclusion and recommendations to be undertaking regarding IoT.

Keywords: Internet of Things (IoT), IoT Architecture, IoT Technologies, IoT Applications, IoT Challenges. IoT Implementation..

1. Introduction:

1.1 General Overview:

The next wave in the era of computing will be outside the realm of the traditional desktop. In the Internet of Things (IoT) paradigm, many of the objects that surround us will be on the network in one form or another. IoT describes a different

world of heterogeneous objects such as sensors, smart-phones, and actuators in which everything, even object has an independent identity (Mardini et al, 2017). In the meantime, many have distinct features, such as different operating systems, platforms, communication protocols, and related standards, but these differences are ignored when introducing with each other (Efremov et l, 2015). Therefore, each device needs to communicate with other things around it to the needs of its users.

IoT also describes a Radio Frequency Identification (RFID), and sensor network technologies will rise to meet this new challenge, in which information and communication systems are invisibly embedded in the environment around us. This results in the generation of enormous amounts of data which have to be stored, processed and presented in a seamless, efficient, and easily interpretable form (Buyya, 2009).

Despite the global buzz around the Internet of Things, there is no single, universally accepted definition for the term. Different definitions are used by various groups to describe or promote a particular view of what IoT means and its most important attributes.

The "Internet of Things" refers to the concept that the Internet is no longer just a global network for people to communicate with one another using computers, but it is also a platform for devices to communicate electronically with the world around them (Hernandez-Castro, et al, 2013). Though there are many definitions of IoT.

The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service (Perera et al, 2014).

This paper is consisting of nine main sections presenting introductory section highlighting the overview of IT from the research design; the 2nd section reviews some selected literature regarding IoT evolution and characteristics; the 3rd and 4th sections present the 10T layered architecture as well as IoT elements; the 5th one pinpoints to the main technologies surrounding IoT; while the 6th section presents briefly the overall architecture developed for IoT; in the meantime, the 7th section highlights some of the IoT societal benefits and challenges and problems; the 8th section demonstrates the successful implementation of IoT as related to the middleware and communication model; The final 9th section indicates the conclusion and recommendations to be undertaking regarding IoT.

1.2. Statement of the Problem:

Associated-living technologies, which is the comAccording to Atzori et al, 2010, Internet of Things cut across several different domains like Transportation and Logistics, Healthcare, Smart Environment, Personal and Social domain, Futuristic just to mention but a few. However, it is faced by some problems or challenges like, Lack of standardization, Scalability (Addressing issues, Understanding the big data), Support for mobility, Address acquisition, new network traffic patterns to handle security/privacy issues.

In response to the aforementioned problems, this paper presents the current trends in IoT research propelled by applications and the need for convergence in several interdisciplinary technologies. Specifically, we present the overall IoT vision and the technologies that will achieve it followed by some common definitions in the area along with some trends and taxonomy of IoT.

1.3 Aim and Objectives:

Aim

The aim is to unify everything in our world under a common infrastructure, giving us not only control of things around us, but also keeping us informed of the state of the things and its applications to meet the societal challenges.

Objectives

The main objective of this paper is to provide an overview of Internet of Things, architectures, elements, and vital technologies and their usages in our daily life, as well as to successfully imple-

ment these applications of IoT.

1.4 Scope of the Study:

This paper discusses the vision, the challenges, possible usage scenarios and technological building blocks of the "Internet of Things". In particular, we consider RFID, Sensor Networks, Wi-Fi and other important technological developments for smart everyday objects. The paper concludes with a discussion of social and governance issues that are likely to arise as the vision of the Internet of Things becomes a reality.

1.5 Method of Study

This study suffices that everyday object are to be addressed and controlled via the Internet, then we should ideally not be resorting to special communications protocols as is currently the case with RFID. Instead, things should behave just like normal Internet nodes. In other words, they should have an IP address and use the Internet Protocol (IP) for communicating with other smart objects and network nodes.

1.6 Definition of Terms

There are many terms as used in Internet of Things. Few terms will be defined here so as to concrete our knowledge about what Internet of Things actually is, they are: RFID, IPv6, EPC, Barcode, Wi-Fi, Bluetooth, NFC, ZigBee, Sensors, Actuators etc.

1. RFID (Radio Frequency Identification)

Radio Frequency Identification is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person. RFID is coming into increasing use in industry as an alternative to the barcode (internetofthingsagenda.techtarget.com).

2. IPV6 (Internet Protocol Version 6)

This is the most recent version of the Internet Protocol, the communication protocol that provides an identification and location system for computers on networks and routes traffic across the internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion (Wikipedia)

3. Sensors

A sensor is a device that detects and responds to some type of input from the physical environment. The specific input could be light, heat, motion, moisture, pressure or any one of a great number of other environmental phenomena. The output is generally a signal that is converted to human-readable display at the sensor location or transmitted electronically over a network for reading or further processing (whatis.techtarget.com).

4. WI-FI (Wireless Fidelity)

Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed internet and network connections. Wi-Fi is simply a trademarked phrase that means IEEE 802.11x (Wepodia.com).

2. LITERATURE REVIEW

2.1 IoT Evolution

Starts with only network and evolves into everything that can be connected with a network. The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service (Perera et al, 2014).

2.2 Characteristics of IoT

The following among others are the characteristics of IoT (Perera et al, 2014). They are:

1. Intelligence: Knowledge extraction from the generated data
2. Architecture: A hybrid architecture supporting many others
3. Complex system: A diverse set of dynamically changing objects
4. Size considerations: Scalability
5. Time considerations: Billions of parallel and simultaneous events
6. Space considerations: Localization

2.3 IPv6 and The Internet of Things

Most technology observers agree that billions of additional devices from industrial sensors to home

appliances and vehicles will be connected to the Internet between now and 2025. As the Internet of Things continues to grow the devices that require true end-to-end Internet connectivity, which will not be able to rely on IPv4 that is the protocol most Internet services use today. They will need a new enabling technology IPv6 which is a long-anticipated upgrade to the Internet's original fundamental protocol - the Internet Protocol (IP), which supports all communications on the Internet. IPv6 is necessary because the Internet is running out of original IPv4 addresses. While IPv4 can support 4.3 billion devices connected to the Internet, IPv6 with 2 to the 128th power addresses, is for all practical purposes inexhaustible. This represents about many trillions addresses, which more than satisfies the demand of the estimated 100 billion IoT devices going into service in the coming decades. Given the anticipated longevity of some of the sensors and other devices imagined for the Internet of Things, design decisions will affect the utility of solutions decades from now. Key challenges for IoT developers are that IPv6 is not natively interoperable with IPv4 and most low-cost software that is readily available for embedding in IoT devices implements only IPv4. Many experts believe, however, that IPv6 is the best connectivity option and will allow IoT to reach its potential (Internet Society).

3. IOT LAYERD ARCHITECTURE

One of the main problems with the IoT is that it is so vast and such a broad concept that there is no proposed, uniform architecture. In order for the idea of IoT to work, it must consist of an assortment of sensor, network, communications and computing technologies, amongst others. Here, some of IoT architectures or models are given by several researchers, authors and practitioners (Han et al, 2012).

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

(1) The Sensing Layer
(2) The Access Layer
(3) The Network Layer
(4) The Middleware Layer
(5) The Application Layers

These are like the Open Systems Interconnection (OSI) reference model in network and data communication (Xiaocong et al, 2012).

This means that there is no single and general agreement about the architecture of IoT that is agreed on by the whole world and researchers. Many and different architectures have been proposed by researchers. According to some researchers, IoT architecture has three layers (Application layer, Network Layer and Perception Layer), but some other researcher supports the four-layer architecture that are (Application layer, support layer, network layer, and perception layer).

Due to enhancement in IoT, the architecture of the tree layers cannot fulfill the requirements of applications, because of a challenge in IoT regarding security and privacy, the architecture of five-layers (that are Business layer, application layer, processing layer, transport layers, and perception layer) has also been proposed . It is considered that a recently proposed architecture that can fulfill the requirements of the IoT regarding security and privacy.

Although the four-layer architecture played an important role in the development of IoT, there were also some issues regarding security and storage in it. Therefore, researchers proposed the five-layer architecture to make IoT more secure (Sethi & Sarangi, 2017). This new version of IoT architecture has three layers like previous three-layer architecture, it also has proposed two more layers that are processing layer and all business layer. This five-layer architecture is considered that the newly proposed one which has the ability to fulfill requirements of IoT. It also has the ability to make the applications of IoT more secure.

These three kinds of IoT layered architectures (i.e., the three-layer, the four layered and the five-

layer) are illustrated within the following diagram:

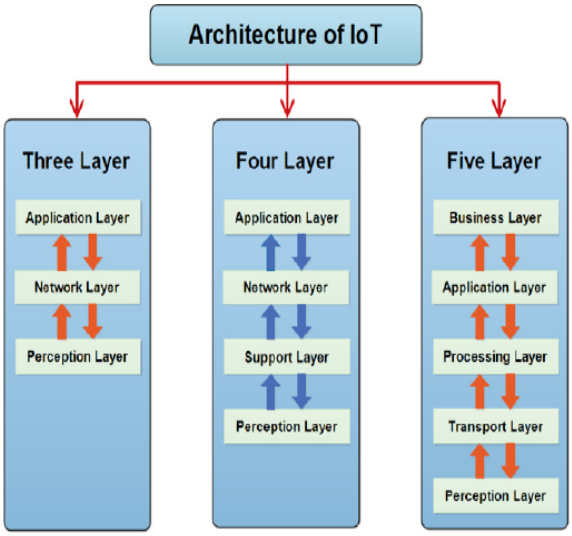

Figure (1) IoT Layered Architectures

The working of these layers and security attacks that can affect them are as presented in the following brief description of these fife layers:

3.1 Processing Layer:

The processing layer is also known as a middleware layer. It collects the information that is sent from a transport layer. It also performs processing onto the collected information, and it has the responsibility to eliminate extra information that has no meaning, and extracts the usefulness of information. In the meantime, it also removes the problem of Big Data in IoT. In Big Data, a large amount of information is received, which can affect performance of IoT. The common attacks of this layer are as follows:

- **Exhaustion**: To disturb the processing of IoT structure.
- **Malware**: An attack on the confidentiality of the information of users. It refers to the application of viruses, spyware, adware, trojans and worms to interact with the system.

3.2 Business Layer (BLA):

The business layer refers to an intended behavior of an application and acts like a manager of a whole system. It has responsibilities to manage and control applications, business and profits models of IoT. The user's privacy is also managed by this layer. It also has the ability to determine how information can be created, stored and changed. This layer permits the attackers to misuse an application by avoiding the business logic. Most problems regarding security are weaknesses in an application that result from a broken or missing security control. Common problems regarding security of business layer are:

- **Business Logic Attack (BLA):** It takes advantage of a flow in a programming, and controls as well as manages the exchange of information between a user and a supporting database of an application. Examples of this BLA are as improper coding by a programmer, password recovery validation, input validation and encryption techniques (Business Logic Attacks).
- **Zero-Day Attack**: It refers to a security hole or a problem in an application that unfamiliar to a vendor. This security hole is exploited by the attacker to take control without user's consent and without knowledge (Kaur & Singh, 2014).

3.3 Perception Layer:

This layer works like people's eyes, ears, and nose. It has the responsibility to identify things and called information from them. There are many types of sensors attached to objects to collect information such as FRID, 2-D barcode, and sensors. The sensors are chosen according to the requirement of application. The information that is collected by these sensors can be about location, changes in the air, environment, motion, vibration, etc. They are the main target of attackers who wish to utilize them to replace the sensor with these own. Therefore, the majority of threats are related to sensors (Xiaohui, 2013). Common security threats of perception layer are as follows:

- **Eavesdropping**: That is an unauthorized real-time attack where private communication, such as phone, calls, text message, fax transmission or video conferences are intercepted

by the attacker. It tries to steal information that is transmitted over a network.

- **Node Capture:** It is one of the hazardous attacks faced in he perception layer of IoT. An attacker gains full control over a key node, such as a gateway node. It may leak all information including communication between sender and receiver. (Bharathi et l, 2012).
- **Timing Attack:** It is usually used in devices that have weak computing capabilities. It enables an attacker to discover vulnerabilities and extract secrets maintained in security of a system by observing how long it takes the system to respond to different queries or cryptographic algorithms (Brumley & Boneh, 2006).

3.4 Network Layer:

Network layer is also known as transmission layer. It acts like a bridge between perception layer and application layer, as well as it carries and transmits the information collected from the physical objects through sensors. The medium for the transmission can be wireless or wire based. This layer also takes the responsibility for connecting the smart things, network devices, and networks to each other. It is highly sensitive to attack from the side of attacker. It has prominent security issues regarding integrity and authentication of information that is being transport in the network. Common security threats and problems to network layer are as follows:

- **Denial of Service (DoS) Attack:** A DoS attack is an attack to prevent authentic users from accessing devices or other network resources. It is typically accomplished by flooding the targeted devices or network resources with redundant requests in an order to make it impossible or difficult for some or all authentic users to use them (Prabhakar, 2017).
- **Storage Attack:** The information of users is stored on storage devices or the cloud. Both storage devices and cloud can be attacked by the attacker and user's information may be changed to incorrect details. The application of information associated with the access of other information by different types of people provides more chance for attacks.
- **Exploit Attack:** An exploit attack is any immoral or illegal attack in a form of software, chunks of data, or a sequence of commands. It takes advantage of security vulnerabilities in an application, system or hardware. It is usually coming with the aim of gaining control of the system and steals information on a network (Exploit Attack in Network Layer)

3.5 Application Layer:

This layer defines all applications that use the IoT technology or which IoT has deployed. The applications of IoT can be smart homes, smart cities, smart health, animal tracking, etc. It has the responsibility to provide the services to the applications. The services may be very varying for each application because services depend on the information that is collected by sensors. There are many issues in the application layer in which security is the key issue. In particular, when IoT is used in order to make a smart home, it introduces many threats and vulnerabilities from the inside and outside. To implement strong security in an IoT security based smart home, one of the main issues is that the device uses in smart homes have weak computational power and a low amount of storage such as ZigBee (Ali & Awad, 2018). Common security threats and problems of application layer are as follows:

- **Cross Site Scripting**: It is an injection attack; as well s it enables an attacker to insert a client-side script, such as java script in a trusted site viewed other users. By doing so, an attacker can completely change the contents of the application according to his needs and use original information in an illegal way (Gupta & Gupta, 2017).
- **Malicious Code:** It is a code in any part of software intended to cause undesired effects and damage to the system. It also is a type of threat that may not be blocked or controlled by the use of anti-virus tools. It can either ac-

tivate itself or be like a program requiring a user's attention to perform an action.

- **The Ability of Dealing with Mass Data**: Due to a large number of devices and massive amount of data transaction between users, it has no ability to deal with data processing according to the requirements as a result., it leads to network disturbance and data loss.

Recently a new evolved IoT layers consisting of new completely six layers as the concept of a layer is that it comprises a set of capabilities that communicate with one another, but for the purpose of other components can be treated as a single entity, with a single transparent entity.

In IoT architecture, the application layer need not know what type of physical network carries the data. All the network devices comprise the network layer that transports traffic as needed by the applications.

What are these 6 layers of IoT architecture?

We define the six layers of IoT architecture as described below. Note that in some cases, layers are made up of sublayers. This a common characteristic in complex architectures, such as that of IoT.

1. **Physical/device layer**. This comprises the sensors, actuators and other smart devices and connected devices that comprise the physical layer and device layer. These smart devices either capture data (sensors), take action (actuators) or sometimes both.

2. **Network layer**. This comprises the network devices and communications types and protocols (5G, Wi-Fi, Bluetooth, etc.). Although many IoT architectures rely on general-purpose network layers, there is an increasing trend to move to dedicated IoT-specific networks.

3. **Data/database layer**. This also includes the database platform layer. There are a range of databases used for IoT architectures, and many organizations spend a fair amount of time selecting and architecting the right IoT databases.

Together, the physical layer/device layer, network layer and data/database layers comprise the infrastructure component discussed above.

4. **Analytics/visualization layer**. This layer comprises the analytics layer, visualization layer and perception layer. In essence, this layer's focus is on analyzing the data provided by IoT and providing it to users and applications to make sense of.

5. **Application/integration layer**. This is the layer of applications and platforms that integrate together to deliver the functionality from the IoT infrastructure to the business. In other words, the application layer, platform layer and integration layer are what provide the business value from the IoT infrastructure. The processing layer and business layer are all part of the larger application/integration layer.

6. **Security and management layer**. As the name implies, this layer encompasses both the security layer and the management layer. Strictly speaking, this is not a layer as it has connections with all the other layers to provide security and management. But it's an important component that's worth considering at every layer.

4. IoT MAIN ELEMENTS:

IoT provides many benefits and facilities to its users. Thus, in order to use these services and facilities properly, there is a need for some main elements of IoT as being shown in the following figure and needed to deliver the functionality of it.

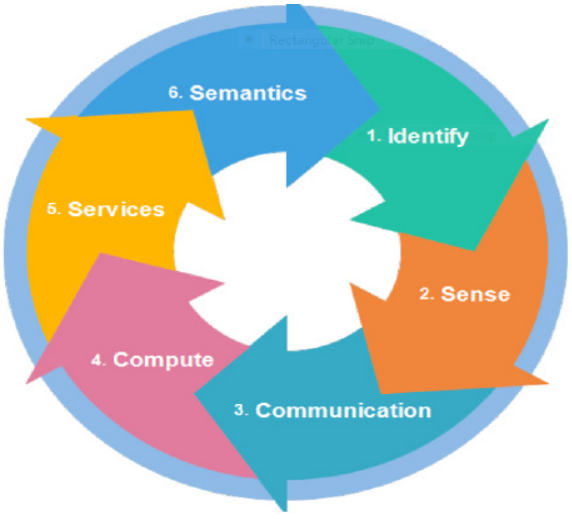

Figure (2) The IoT Main Elements

The names and description of these IoT main elements are as follows:

4.1 Identification:

IoT identification offers identity to each object within the network. There are two processes in identification: naming and addressing. Naming refers as name of the object while addressing is the unique address of specific object. These both terms are very different from each other because two or more objects that may have same name, but always different and unique address. In addition, there are many methods available that provide the naming facility to the object in the network, such as Eectron Products Codes (EPC) and ubiquitous codes (Koshizuka et al, 2010). To assign the unique address to addressing scheme.

4.2 Sensing:

The process of collecting information from objects is known as sensing. The collected information is sent to the storage media. There are many sensing devices to collect the information from objects, such as actuators, FRID, smart senses, wearable sensing devices, etc.

4.3 Communication:

Communication is one of the main processes of IoT in which different devices are connected to each other and communicate. In communication, devices may send and receive messages, files, and other information. There are many technologies that provide facility of communication like Radio Frequency Identification (RFID) (Want, 2006), Near Field Communication (NFC) (Want, 2011), Bluetooth (McDermott, 2004), Wi-Fi (Ferro & Potorti, 2005), and Long-Term Evolution (LTE) (Crosbu & Vafa, 2013).

4.4 Computation:

Computation is performed on the collected information from the objects by using sensors. It is used to remove unnecessary information that is not needed. Many hardware and software platforms are developed to perform the process in applications of IoT. For hardware platforms Audrino, Raspberry Pi, and Intel Galileo are used, while, for software platforms, the operating system plays an important role to perform processing

There are many types of operating systems that are used like Tiny OS (Levis et al, 2005), Lite OS (Cao et al, 2008) Android, etc.

4.5 Services:

There are four types of services that are provided by IoT applications (Gigli & Koo, 2011). The first one is an identity-related services that is used get the identity of object that have sent the request. The 2nd is the information aggregation in another service whose purpose is to collect all information from object processing that is also performed by aggregation service. The other type of service is a collaborative service that makes decisions according to the collected information and sends appropriate responses to the devices. The 4th and final type of service is ubiquitous services, which is used to respond the devices immediately without rigidity about time and place.

4.6 Semantics:

It is the responsibility of IoT to facilitate users by performing their tasks. It is the most important element of IoT to fulfill its responsibilities. It acts like a brain of IoT, and gets all information to send responses to the devices

The following table shows the key technologies involved in each element of IT.

Table (1) The Elements and Key Technologies of IoT

IoT Elements	Main Technologies
Identification – Naming Addressing	-Electronic, Product Code, Ucode -IPv6
Sensing	-Smart, sensors, FRID tags -Devices and wire able sensing
Communication	RFID, Wireless Sensor Networks (WSN), Near Field Communication (NFC). Bluetooth, Wi-Fi, Long Term Evolution (LTE)
Services	-Identity-Related, Information Aggregation, Collaborative-Aware, and Ubiquitous
Semantics	Resource Description Framework (RDF), Ontology Web Language (OWL), EXI

5. IOT TECHNOLOGIES:

The Internet of Things was initially inspired by members of the RFID community, who referred to the possibility of discovering information about a tagged object by browsing an internet address or

database entry that corresponds to a particular RFID or Near Field Communication technologies. In the research paper "Research and application on the smart home based on component technologies and Internet of Things" (Baoan & Jianjun, 2011), the included key technologies of IoT are RFID, the sensor technology, nano technology and intelligence embedded technology. Among them, RFID is the foundation and networking core of the construction of Internet of Things.

The Internet of Things (IoT) enabled users to bring physical objects into the sphere of cyber world. This was made possible by different tagging technologies like NFC, RFID and 2D barcode which allowed physical objects to be identified and referred over the internet. IoT, which is integrated with Sensor Technology and Radio Frequency Technology, is the ubiquitous network based on the omnipresent hardware resources of Internet. It is also a new wave of IT industry since the application of computing fields, communication network and global roaming technology had been applied. It involves in addition to sophisticated technologies of computer and communication network outside, still including many new supporting technologies of Internet of Things, such as collecting Information Technology, Remote Communication Technology, Remote Information Transmission Technology, Measures Information Intelligence Analyzes and Controlling Technology etc. (Madakan et al, 2015). The following figure exhibits the taxonomy of IoT technologies that are explained in this section;

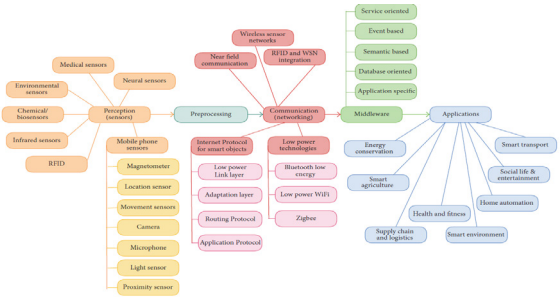

Figure (3) Taxonomy of IoT Technologies

5.1 Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is a system that transmits the identity of an object or person wirelessly using radio waves in the form of a serial number. First use of RFID device was happened in 2nd world war in Britain and it is used for Identify of Friend or Foe in 1948. Later RFID technology is founded at Auto-ID center in MIT in the year 1999. RFID technology plays an important role in IoT for solving identification issues of objects around us in a cost-effective manner. The technology is classified into three categories based on the method of power supply provision in Tags: Active RFID, Passive RFID and Semi Passive RFID. The main components of RFID are tag, reader, antenna, access controller, software and server (Madakan et al, 2015).

5.2 Internet Protocol (IP)

Internet Protocol (IP) is the primary network protocol used on the Internet, developed in 1970s. IP is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. The two versions of Internet Protocol (IP) are in use: IPv4 and IPv6. Each version defines an IP address differently. Because of its prevalence, the generic term IP address typically still refers to the addresses defined by IPv4. There are five classes of available IP ranges in IPv4: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. The actual protocol provides for 4.3 billion IPv4 addresses while the IPv6 will significantly augment the availability to 85,000 trillion addresses. IPv6 is the 21st century Internet Protocol. This supports around for 2128 addresses (Madakan et al, 2015).

5.3 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 CodeBook, Palmer (1995) acknowledges that there are alternative methods of data entry techniques. Quick Response (QR) Codes

the trademark for a type of matrix barcode first designed for the automotive industry in Japan. Bar codes are optical machine-readable labels attached to items that record information related to the item. Recently, the QR Code system has become popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard. There are 3 types of barcodes of Alpha Numeric, Numeric and 2 Dimensional. Barcodes are designed to be machine readable. Usually, they are read by laser scanners, they can also be read using a camera.

5.4 Wireless Fidelity (Wi-Fi)

Wireless Fidelity (Wi-Fi) is a networking technology that allows computers and other devices to communicate over a wireless signal. Vic Hayes has been named as father of Wireless Fidelity. The first wireless products were brought on the market under the name WaveLAN with speeds of 1 Mbps to 2 Mbps. Today, there are nearly pervasive
Wi-Fi that delivers the high-speed Wireless Local Area Network (WLAN) connectivity to millions of offices, homes, and public locations such as hotels, cafes, and airports. The integration of Wi-Fi into notebooks, handhelds and Consumer Electronics (CE) devices has accelerated the adoption of Wi-Fi to the point where it is nearly a default in these devices [24]. Technology contains any type of WLAN product support any of the IEEE
802.11 together with dual-band, 802.11a, 802.11b, 802.11g and 802.11n. Nowadays entire cities are becoming Wi-Fi corridors through wireless APs.

5.5 Bluetooth

Bluetooth wireless technology is an inexpensive, short-range radio technology that eliminates the need for proprietary cabling between devices such as notebook PCs, handheld PCs, PDAs, cameras, and printers and effective range of 10 - 100 meters. And generally, communicate at less than 1 Mbps and Bluetooth uses specification of IEEE 802.15.1 standard. At first in 1994 Ericson Mobile Communication company started project named "Bluetooth". It is used for creation of Personal Area Networks (PAN). A set of Bluetooth devices sharing a common channel for communication is called Piconet. This Piconet is capable of 2 - 8 devices at a time for data sharing, and that data may be text, picture, video and sound. The Bluetooth Special Interest Group comprises more than 1000 companies with Intel, Cisco, HP, Aruba, Intel, Ericson, IBM, Motorola and Toshiba (Madakan et al, 2015).

5.6 Near Field Communication (NFC)

Near Field Communication (NFC) is a set of short-range wireless technology at 13.56 MHz, typically requiring a distance of 4 cm. NFC technology makes life easier and more convenient for consumers around the world by making it simpler to make transactions, exchange digital content, and connect electronic devices with a touch. Allows intuitive initialization of wireless networks and NFC is complementary to Bluetooth and 802.11 with their long-distance capabilities at a distance circa up to 10 cm. It also works in dirty environment, does not require line of sight, easy and simple connection method. It is first developed by Philips and Sony companies. Data exchange rate now days approximately 424 kbps. Power consumption during data reading in NFC is under15mah.

5.7 Actuators

An actuator is something that converts energy into motion, which means actuators drive motions into mechanical systems. It takes hydraulic fluid, electric current or some other source of power. Actuators can create a linear motion, rotary motion or oscillatory motion. Cover short distances, typically up to 30 feet and generally communicate at less than 1 Mbps. Actuators typically are used in manufacturing or industrial applications. There are three types of actuators are (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.

5.8 Wireless Sensor Networks (WSN)

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

5.9 Networking and Communications

The field of networking and communication includes the analysis, design, implementation, and use of local, wide-area, and mobile networks that link computers together. The Internet itself is a network that makes it feasible for nearly all computers in the world to communicate.

A network is the combination of two or more computers and their connecting links. A physical network is the hardware (equipment such as adapters, cables, and telephone lines) that makes up the network. The software and the conceptual model make up the logical network. Different types of networks and emulators provide different functions.

The complexity of modern computer networks results several conceptual models for explaining how networks work. One of the most common of these models is the International Standards Organization's Open Systems Interconnection (OSI) Reference Model, also referred to as the OSI seven-layer model.

The OI Refence Model consists of seven layers as in the following figure:

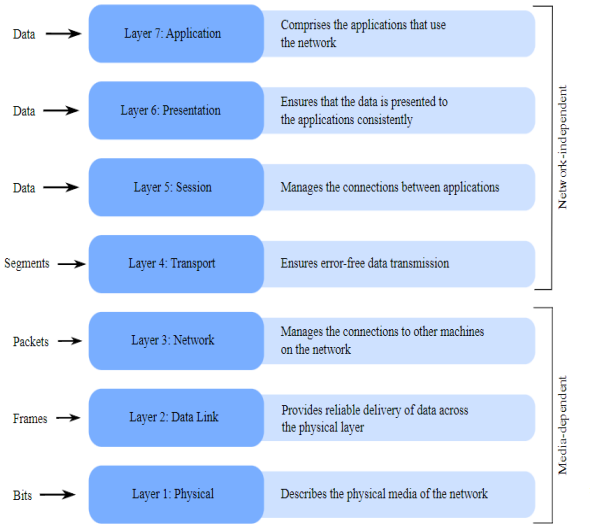

Figure (4) OSI Reference Model Seven Layers

5.10 Sensor Networks (SNs)

Consist of a certain number (which can be very high) of sensing nodes (generally wireless) communicating in a wireless multi□hop fashion (Perera et al, 2014). Sensor Networks generally exist without IoT but IoT cannot exist without Sensor Networks.

- Sensor Networks have been designed, developed, and used for specific application purposes like Environmental monitoring, agriculture, medical care, event detection etc.
- For IoT purposes, Sensor Networks need to have a middleware addressing issues like Abstraction support, data fusion, resource constraints, dynamic topology, application knowledge, programming paradigm, adaptability, scalability, security and QoS support.

6.APPLICATIONS OF IOT:

There are a diverse set of areas in which intelligent applications have been developed.

There are a lot of applications in which IoT has been deployed. These applications have become smart, and perform their work robotically by tacking help from the Internet (Al-Fugaha, 2015 & Mishra, et al, 2016). Among the main application

is the healthcare where sensors are used to check human's body temperature, blood pressure and heartbeat rate (Islam, 2015). Another application is smart home because humans use many electronic things like refrigerators, microwave ovens, fans, heaters, and air conditioners at homes, the sensors are installed to detect the problem about the problem to manufacturing In addition there is application of IoT about animal tracking. The GPS sensors are installed in an animal's body to trace them easily, it is also used to monitor the animal's feed (Memon et al, 2016). Another IoT application is smart robotics grippers that contact an object directly to collect sensing information. There are a lot of sensors and instruments installed in a smart gripper such as touch, motion, vision, optical and force sensors, The smartness level of smart gripper depends on the equipped sensors because they collect information in a real-time mode and collected information is used to make decisions. Therefore, they must be confined by design criteria such as cost, weight, and compactness (Bi et al 2018).

In addition, there are numerous applications of IoT such as smart transportation, infrastructure management (highways, bridges and railways tracks), manufacturing, smart building, smart agriculture and smart retail, etc.

This indicates clearly that IoT has been applied to several different domains (Atzori et al, 2010) which are categorized in the following:

- Transportation and Logistics (Logistics, Supply Chain, Assisted Driving, Mobile Ticketing, Environmental monitoring, Augmented Maps).
- Healthcare (Tracking, Identification, Authentication, Data collection, Sensing).
- Smart Environment (Comfortable Homes/ offices, Industrial Plants, Smart Museums/ gyms)
- Personal and Social Domain (Social networking, Historical queries, Losses, Thefts).
- Futuristic (Robot taxi, city information model, enhanced game room).
- Smart Environmental and Agriculture that concerns with production using greenhouse, air pollution
- Industrial Internet of Things (IIoT) applications as related to asset tracking, preventive maintenance, inventory management, remote monitoring and control, employee and environmental safety.

The makers of IoT devices are increasing each and every day. The reason for increasing the number of IoT devices is that they provide comfort in human life and perform work with better outcomes than humans.

7.IOT SOCIETAL BENEFITS AND CHALLENGES:

The positive impact of the Internet of Things on citizens, businesses, and government will be significant, ranging from helping government reduce healthcare costs and improving quality of life, to reduce carbon footprints, increasing accress to education in remote underserved communities, and improving transportation safety.

7.1 IoT Benefits:

The IoT is merging the physical and digital world together, bringing intelligence to devices, without people, to collect and share data over the Internet. The premise behind IoT is that it improve the way we make decisions, saving our time and money but also improving our quality of life.

IoT can include devices such as smart microwaves which cook food according to the weight guaged and then deliver recipe suggestions; smart cars which detect maintenance issues, take corectivetion and alert the automaker; cloud-connected minibars which add to the hote bill at the guest removal of an item, ten order a replacement; and fitness devices which measure heart rate,tepcount, quality of sleep,and more; and then use the information to sugget customized exercise plans.

On alargecale, someloctions around the world have become smart cities, where data relating to environment, trffic, water management, power

security, and even crowd control can be collected and analyzed to create a more efficient city. Smart city technologies and programs have so far been implemented in ingapore, Dubai, Amsterdam, Stockholm, and many other smart cities.

7.2 Iot Challenges:

There are many open challenges that have been described by variouss researchers including those related to power supply; enabling a complex sensing environment; evolving architecture; multiple connectivity options; complexity of IoT; security of information exchnge within IoT; and privacy (Atzori, et al, 2010; Gluhk et al, 2011). Due to the widey accepted bussine model that on engage investments to encourage the deployment of these technologies,there is difficulty in the doption of IoT paradigm (Zanella et al, 2014).

The common major challenges of IoT and its future directions are availability, performance, reliability, security and privacy, scalability, percision, interoperability, compatibility, Big IoT Data, mobility, and investment. IoT is used to facilitate information and data anywhere at any time for many persons based on his request (Marshal et al (2015). So, to realize IoT availability is a highly critical issue, the IoT network requires the high availability to achieve it, and the feasible solution is redundent hardware components (Macedo et al (2014). Since IoT depends on components and performance of involving technologies, its performance cannot be evaluated using a simple mechanism. Therefore, the other factors that influence the performance of IoT are network traffic, huge amount of data, and heavy reliance on cloud computing.

In addition, security and privacy are an essential requirement of most of the applications, thus in IoT, memory cards of a device have a limited capacity, so only small amounts of data can be stored in them, and some of the data will be stored in other sites remotely, that needs high security and privacy.

To a certain extent, the bove-mentioned challenges can be met, with the aid of a variety of wirelessand wired connectivity options, such as Radio requency Identification (RFID), Ner-Field Communication (NFC), Bluetooth and Wi-Fi technolgies. Thee connectivity options are categorized into three broad types consiering their geographical are average that is personll rea network (PEN), local area network (LAN), and widdde area network (WAN). The existing Wi-Fi networks shoulld be modefied to attain a wider coverage and to support mesh networks (Kasznik, 2015). In addition, the confirmation on communication prthway of IoTis very important to understand the informaation exchange within IoT. It uses variouss sstanddrds, techniques and protocols to disseminate information.

In the meantime, it is esential to support devicetodevice (D2D),device-to-server (D2S), and server-to-server (S2S) to facilitate information sharing within IoT. There are multiple standards and protocols tke a higher priority, such IPv4 and IPv6 that is being usse over low-power wireless personal area network (LoWPAN); user datagram protocol (UDP); constrained applicaation protocol (CoAP); and transmission control protoco (TCP). However, UDP is considered adventageous aand cost-effective, due to its smaller size and performaance according to constraained device developers (Internet of Thing Protocols & Standards).

Inspite of all what is presented above there are still existed open problems and challenged faced in the deployment of IoT which are (Atzori et al, 2010),

- Lack of Standardization: Several standardization efforts but not integrated in a comprehensive framework.
- Scalability: Addressing issues, Understanding the big data, Number of devices increasing exponentially, how can they uniquely be tagged/named? How can the data generated by these dev ices be managed?
- Support for mobility
- Address acquisition: IPv4 protocol may already reached its limit. However, IPv6 ad-

dressing has been proposed for low power wireless communication nodes within the WPAN context

- • New network traffic patterns to handle
- Security/Privacy Issues

Anyway, the main advantages and disadvantages are presented within the following figures:

Figure (5) IoT Advantages and Disadvantages

8.SUCCESSFUL IMPLEMENTATION OF IOT

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.

According to another author, there are three components, which required for seamless Internet of Things (IoT) computing:

(a) Hardware - composed of sensors, actuators, IP cameras, CCTV and embedded communication hardware

(b) Middleware - on demand storage and computing tools for data analytics with cloud and Big Data Analytics

(c) Presentation - easy to understand visualization and interpretation tools that can be designed for the different applications (Madakan et al, 2015).

8.1 Middleware

Middleware is a software layer that stands between the networked operating system and the application and provides well known reusable solutions to frequently encountered problems like heterogeneity, interoperability, security, dependability (Issarny, 2008).

IoT requires stable and scalable middleware solutions to process the data coming from the networking layers.

8.2 Internet of Things Communication Model

From an operational perspective, it is useful to think about how IoT devices connect and communicate in terms of their technical communication models. The Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects which outlines a framework of four common communication models used by IoT devices. The discussion below presents this framework and explains key characteristics of each model in the framework (Tschofenig et al, 2015).

8.2.1 Device-to-Device Communications

The device-to-device communication model represents two or more devices that directly connect and communicate between one another, rather than through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet. Often, however these devices use protocols like Bluetooth, Z-Wave or ZigBee to establish direct device-to-device communications. These device-to-device networks allow devices that adhere to a particular communication protocol to communicate and exchange messages to achieve their function. This communication model is commonly used in applications like home automation systems, which typically use small data packets of

information to communicate between devices with relatively low data rate requirements. Residential IoT devices like light bulbs, light switches, thermostats, and door locks normally send small amounts of information to each other (e.g., a door lock status message or turn on light command) in a home automation scenario.

8.2.2 Device-to-Cloud Communications

In a device-to-cloud communication model, the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service. This communication model is employed by some popular consumer IoT devices like the Nest Labs Learning Thermostat44 and the Samsung SmartTV.45 In the case of the Nest Learning Thermostat, the device transmits data to a cloud database where the data can be used to analyze home energy consumption. Further, this cloud connection enables the user to obtain remote access to their thermostat via a smartphone or Web interface, and it also supports software updates to the thermostat. Similarly with the Samsung SmartTV technology, the television uses an Internet connection to transmit user viewing information to Samsung for analysis and to enable the interactive voice recognition features of the TV.

However, interoperability challenges can arise when attempting to integrate devices made by different manufacturers. Frequently, the device and cloud service are from the same vendor.46 If proprietary data protocols are used between the device and the cloud service, the device owner or user may be tied to a specific cloud service, limiting or preventing the use of alternative service providers. This is commonly referred to as "vendor lock-in", a term that encompasses other facets of the relationship with the provider such as ownership of and access to the data. At the same time, users can generally have confidence that devices designed for the specific platform can be integrated (Marsan et al, 2015).

8.2.3 Device-to-Gateway Model

In the device-to-gateway model, or more typically, the device-to-application-layer gateway (ALG) model, the IoT device connects through an ALG service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation

Several forms of this model are found in consumer devices. In many cases, the local gateway device is a smartphone running an app to communicate with a device and relay data to a cloud service. This is often the model employed with popular consumer items like personal fitness trackers. These devices do not have the native ability to connect directly to a cloud service, so they frequently rely on smartphone app software to serve as an intermediary gateway to connect the fitness device to the cloud. The other form of this device-to-gateway model is the emergence of "hub" devices in home automation applications. These are devices that serve as a local gateway between individual IoT devices and a cloud service, but they can also bridge the interoperability gap between devices themselves. For example, the SmartThings hub is a standalone gateway device that has Z-Wave and Zigbee transceivers installed to communicate with both families of devices. It then connects to the SmartThings cloud service, allowing the user to gain access to the devices using a smartphone app and an Internet connection.

8.2.4 Back-End Data-Sharing Model

The back-end data-sharing model refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. This architecture supports "the [user's]

desire for granting access to the uploaded sensor data to third parties". This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where "IoT devices upload data only to a single application service provider". A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed. For example, a corporate user in charge of an office complex would be interested in consolidating and analyzing the energy consumption and utilities data produced by all the IoT sensors and Internet-enabled utility systems on the premises. Often in the single device-to-cloud model, the data each IoT sensor or system produces sits in a stand-alone data silo. An effective back-end data sharing architecture would allow the company to easily access and analyze the data in the cloud produced by the whole spectrum of devices in the building. Also, this kind of architecture facilitates data portability needs. Effective back-end data sharing architectures allow users to move their data when they switch between IoT services, breaking down traditional data silo barriers. The back-end data-sharing model suggests a federated cloud services approach or cloud applications programmer interfaces (APIs) are needed to achieve interoperability of smart device data hosted in the cloud (Tschofenig, 2015).

9. SUMMARY, CONCLUSION AND RECOM MENDATION

9.1 Summary:

The Internet of Things promises to deliver a step change in individuals' quality of life and enterprises' productivity. Through a widely distributed, locally intelligent network of smart devices, the IoT has the potential to enable extensions and enhancements to fundamental services in transportation, logistics, security, utilities, education, healthcare and other areas, while providing a new ecosystem for application development. A concerted effort is required to move the industry beyond the early stages of market development towards maturity, driven by common understanding of the distinct nature of the opportunity. This market has distinct characteristics in the areas of service distribution, business and charging models, capabilities required to deliver IoT services, and the differing demands these services will place on mobile networks. While the concept of combining computers, sensors, and networks to monitor and control devices has been around for decades, the recent confluence of key technologies and market trends is ushering in a new reality for the "Internet of Things". IoT promises to usher in a revolutionary, fully interconnected "smart" world, with relationships between objects and their environment and objects and people becoming more tightly intertwined. The prospect of the Internet of Things as a ubiquitous array of devices bound to the Internet might fundamentally change how people think about what it means to be "online". While the potential ramifications are significant, a number of potential challenges may stand in the way of this vision - particularly in the areas of security; privacy; interoperability and standards; legal, regulatory, and rights issues; and the inclusion of emerging economies. The Internet of Things involves a complex and evolving set of technological, social, and policy considerations across a diverse set of stakeholders.

9.2 Conclusion:

The proliferation of devices with communicating-actuating capabilities is bringing closer the vision of an Internet of Things, where the sensing and actuation functions seamlessly blend into the background and new capabilities are made possible through access of rich new information sources. IoT is an ideal emerging technology to influence this domain by providing new evolving data and the required computational resources for creating revolutionary applications. The Internet of Things is happening now, and there is a need to address its challenges and maximize its benefits while reducing its risks. In this manner, the needs of the end-

user are brought to the fore. Allowing for the necessary flexibility, availability, higher performance and many other factors to meet the diverse and sometimes competing needs of different sectors. Due to the integration of novel concepts as well as the adoption of existing technologies, IoT is still evolving. Thereby, it supports the development of more competitive, realistic, and advanced IoT-based applications.

9.3 Recommendations:

A framework is to be proposed enabled by a scalable cloud to provide the capacity to utilize the IoT. The framework allows networking, computation, storage and visualization themes separate thereby allowing independent growth in every sector but complementing each other in a shared environment. The standardization which is underway in each of these themes will not be adversely affected with Cloud at its center. Accommodate IoT with existing practices: Policies, Procedures, & Standards, Awareness Training, Risk Management, Vulnerability Management, Forensics, Increased network traffic: will your firewall / IDS / IPS be compatible and keep up? Increased demand for IP addresses both IPv4 and IPv6, Increased network complexity - should these devices be isolated or segmented? Strengthen partnerships with researchers, vendors, and procurement department.

The following research fields need to be researched to develop optimal and efficient solutions for IoT with low cost and high efficiency:

- There is a need for unmanned vehicle (UAV) to replace a massive number of IoT devices, especially in agriculture, traffic and monitoring which will help to reduce power consumption and pollution.
- Transmission data from sensor to the mobile cloud is integrating the wireless sensor network and mobile cloud.
- M2M communication plays a critical role to reduce energy use and hazardous emissions. Smart machines must be more smarter to enable automated systems.
- To achieve energy balancing for supporting efficient communication between IoT devices, the radio frequency energy harvest should be considered.
- More research is needed to develop te design of IoT devices which helps to reduce CO2 emission and energy usage.

References:

- Al-Fugaha, A. et al (2015). "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys and Tutorials, vol 17, pp. 2347-2376.

- Ali, B. & Awad, A. I. (2018). "Cyber and Physical Security Vulnerability Assessment of IoT-Based Smart Homes," Sensors, vol. 18.

- Atzori, L., Iera, A. & Morabito, G. (2010). "The Internet of Things". A survey, Computer Networks, vol., 54, pp. 2787-2805

- Baoan, L. & Jianjun, Yu (2011). "Research and Application on the Smart Home on the component Technologies and Internet of Things," Procedia Engineering, vol., 15, pp. 2o87-2092.

- Bharathi et al (2012). "Node Capture in Wireless Sensor Network: A Survey," In: Proceedings of the 2012 IEEE International Conference on Computational Intelligence & Computing Research (ICCIC), Coimbatore, India, pp. 18-20 December 2012, pp. 1-3.

- Bi, Z. et al (2018). "Real-Time Force Monitoring of Smart Gripper for Internet of Things (IoT) Applications," Journal of Industrial Information,

- Brumley, D. & Boneh, D. (2005). "Remote Timing Attacks Use Practical," Computer Network, vol., 48, pp. 701-716.

- Business Logic Attack. http://whatis.tectarget.com/drinition/business-logic-attack.

- Buyya, R. et al (2009). "Cloud computing and

emerging IT platforms": Vision, hype, and reality for 27 delivering computing as the 5th utility, Future Generation Computer Systems 25 (2009) 599-616

- Cao, Q et al (2008). "The LiteOS Operating System: Towards Unix-Like Abstractions for Wireless Sensor Networks," In: Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN'08), St. Louis, MO: USA, 22 - 24 April 2008, pp. 233-244.

- Duffy Marsan, Carolyn. (2015). "IAB Releases Guidelines for Internet-of-Things Developers." IETF Journal 11.1 (2015): 6-8. Internet Engineering Task Force, July 2015. Web. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

- Efremov, S. et al (2015). "An Integrated Approach to Common Problems in the Internet of Things," Procedia Engineering, vol. 100, pp. 1215-1223.

- Evans, Dave (2011). "The Internet of Things - How the Next Evolution of the Internet is Changing Everything," CISCO

- Exploit Attack in Network Layer. http://searchsecurity.techtarget.com/definition/exploit.

- Gigli. M. & Koo, S. (2011). "Internet of Things: Services and Applications Categorized," Advanced Internet of Things, vol., 1,

- Gluhak, A. et al (2011). "A Survey on acilities for Experimental Internet of Things Research," IEEE Communications Magazine, vol. 49, no. 11, pp. 58-67.

- Gupta, S. & Gupta, B. B. (2017). "Cross-Site Scripting (XSS) Attacks and Defense mechanisms Classification and State-of-the-Art," International Journal of System Assurance Engineering Management, vol. 8, pp.512-530.

- Han, D. et al (2012)." Convergence of sensor networks/Internet of Things and power grid information network at aggregation layer". Proceedings of the International Conference on Power System Technology (POWERCON).

- Hernandez-Castro, J. C., et al (2013). "Cryptanalysis of the SASI ultra-light weight RFID authentication protocol". [cited 2013 May 20]; available from http://arxiv.org/abs/0811.4257 .

- https://internetofthingsagenda.techtarget.com

- https://www.wepodia.com

- Internet of Things Protocols & Standards. Postscapes. http://postscapes.com/internet-of-things-protocols

- Islam, S. R. et al (2015). "The Internet of things for Health Care: A Comprehensive

Survey," IEEE Access, vol 3, pp. 678-708.

- Kaur, R. & Singh, M. A. (2014). "A Survey on Zero-Day Polymorphic Worm Detection

Techniques," IEEE Communications Survey and Tutorials, vol. 16, pp. 1520-1549.

- Kasznik, E. (2015). "Internet of Things. http://www.worldipreview.com/contributed-article/semiconductor-focus-the-third-wave-of-revolution

- Khan, I.U. et al (2017). "Internet of Things: Applications in Home Applications,"

vol. 5, pp. 79-84.

- Levis, P. et al (2005) "TinyOS: Operating System for Sensor Networks," Ambient

Intelligence, vol., 35, pp. 115-148.

- Macedo, D. et al (2014). "A Dependability Evaluation for Internet of Things Incorporating Redundancy Aspects," In: ICNSC, Miami FL.

- Madakam, S., Ramaswamy, R. and Tripathi, S. (2015). "Internet of Things (IoT)". A Literature Review. Journal of Computer and Communications, 3, 164-173.

- Mardini, W. et al (2017). "Genetic Algorithm for Friendship Selection in Social IoT," In: International Conference on Engineering &MIS (ICEMIS).
- Marshal, I. et al (2015). "Choices for Interaction with Things on Internet and Underlying Issues," Ad Hoc Network, vol., 28, pp. 68-90.
- Menon, M. H. et al (2016). "Internet of Things (IoT) Enabled Smart Animal Farm," In: Proceedings of the 3rd International Conference on Computing for Sustainable Gopal Development (INDIACom), New Delhi, India, 16-18 March 2016, pp. 2067-2072.
- Mishra, D. et al (2016). "Vision, Applications, and Further Challenges of Internet of Things: A Bibliometric Study of the Recent Literature," Indian Management Data Systems, vol. 116,pp. 1331-1355.
- Perera, C., et al. (2014). "Sensing as a Service Model for Smart Cities Supported by Internet of Things", Trans. Emerging Telecommunications Technologies, vol. 25, no. 1, pp. 81-93, 2014.
- Prabhakar, S. (2017). "Network Security in Digitalization: Attacks and Defense," International Journal of Research Computer Application Robotics, vol. 5, pp. 46-52.
- "Radio-Frequency Identification." Wikipedia, the Free Encyclopedia https://en.wikipedia.org/wiki/Radiofrequency_Identification
- Sethi, P. & Sarangi, S. R. (2017). "Internet of Things: Architecture, Protocols, and Applications," Journal of Electrical and Computer Engineering,
- Sicari, S. et al (2019). "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146-164.
- Thomson, G., et al (2008) Amigo Interoperability Framework: Dynamically Integrating Heterogeneous Devices and Services. In: Mühlhäuser M., Ferscha A., Aitenbichler E. (eds) Constructing Ambient Intelligence. Aml 2007. Communications in Computer and Information Science, vol 11. Springer, Berlin, Heidelberg
- Tschofenig, H., et. al (2015), "Architectural Considerations in Smart Object Networking". Tech. no. RFC 7452. Internet Architecture Board, Mar. 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt
- Tschofenig, H., et. al.(2015). "Architectural Considerations in Smart Object Networking". Tech. no. RFC 7452. Internet Architecture Board, Mar. 2015. Web. https://tools.ietf.org/html/rfc7452
- "Values and Principles." Principles. Internet Society, 2015.
http://www.internetsociety.org/who-we-are/mission/values-and-principles-
Whatis.techtarget.com
- Xiaohui, X. (2013). "Study on Security Problems and Key Technologies of the Internet of Things," In: Proceedingsof the 5th International Conference on Computational and Information Sciences (ICCIS), Shiyan, China, 21-23 June 2013, pp. 407-410.
- Xiaocong, Q., & Jidong, Z. (2012). Study on the structure of "Internet of Things (IOT)" business operation support platform. Proceedings of the 12th IEEE International Conference on Communication Technology (ICCT).
- Yoqoop, I. et al (2017). "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements and Open Challenges," IEEE Wired Communications, vol. 24, pp 10-10.
- Zanella, A. et al (2014). "Internet of Things for Smart Cities," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32.