CHAPTER ONE

1.0 INTRODUCTION

The **Internet of Things** (**IoT**) is the network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more-direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020.

British entrepreneur Kevin Ashton first coined the term in 1999 while working at Auto-ID Labs (originally called Auto-ID centers - referring to a global network of Radio-frequency identification (RFID) connected objects). Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a Smart Grid, and expanding to the areas such as smart cities.

"Things," in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring or field operation devices that assist firefighters in search and rescue operations. These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. Current market examples include smart thermostat systems and washer/dryers that use Wi-Fi for remote monitoring. Besides the plethora of new application areas for Internet connected automation to expand into, IoT is also expected to generate large amounts of data from diverse locations that is aggregated very quickly, thereby increasing the

need to better index, store and process such data. IoT is one of the platforms of today's Smart City and Smart Energy Management Systems.

The Internet of Things, an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data authentication, and access control and client privacy need to be established. An adequate legal framework must take the underlying technology into account and would best be established by an international legislator, which is supplemented by the private sector according to specific needs and thereby becomes easily adjustable. The contents of the respective legislation must encompass the right to information, provisions prohibiting or restricting the use of mechanisms of the Internet of Things, rules on IT-security-legislation, provisions supporting the use of mechanisms of the Internet of Things and the establishment of a task force doing research on the legal challenges of the IoT.

Anyone who says that the Internet has fundamentally changed society may be right, but at the same time, the greatest transformation actually still lies ahead of us. Several new technologies are now converging in a way that means the Internet is on the brink of a substantial expansion as objects large and small get connected and assume their own web identity.

Following on from the Internet of computers, when our servers and personal computers were connected to a global network, and the Internet of mobile telephones, when it was the turn of telephones and other mobile units, the next phase of development is the Internet of things, when more or less anything will be connected and managed in the virtual world. This revolution will be the Net's largest enlargement ever and will have sweeping effects on every industry — and all of our everyday lives.

CHAPTER TWO

2.0 LITERATURE REVIEW

The Internet of Things (IoT) is defined in many different ways, and it encompasses many aspects of life from connected homes and cities to connected cars and roads, roads to devices that track an individual s behavior and use the data collected for push services. Some mention one trillion Internet-connected devices by 2025 and define mobile phones as the eyes and ears of the applications connecting all of those connected things. By these internet of things billions objects can communicate over worldwide over a public, private internet protocol network in 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. Smart cities, Smart cars, Public safety, Smart Industries and Environmental Protection has been given the high intention for future protection by IoT Ecosystem. For the development the government of Europe, Asia and America has considered the Internet of Things has area innovation and growth. Many visionaries have seized on the phrase Internet of Things to refer to the general idea of things, especially everyday objects, that are readable, recognizable, locatable, addressable, and/or controllable via the Internet, irrespective of the communication means (whether via RFID, wireless LAN, wide- area networks, or other means).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. This model will consist of services that are commodities and delivered in a manner similar to traditional commodities. Due to internet of things hospitals are shifting to remote self-monitoring for patients. Due self-monitoring it gives the patient greater freedom and independence for their health and free the equipment for emergency propose for patients.

Internet of Things (IoT) is a new revolution of the Internet. Internet of Things (IoT) is can be said the expansion of internet services. It provides a platform for communication between objects where objects can organize and manage themselves. It makes objects themselves recognizable. The internet of things allows everyone to be connected anytime and anywhere. Objects can be communicated between each other by using radio frequency identification (RFID), wireless sensor network (WSN), Zigbee, etc. Radio Frequency identification assigns a unique

identification to the objects. RFID technology is used as more secure identification and for tracking/locating objects, things, and vehicle.

2.1 HISTORY

As of 2016, the vision of the Internet of things has evolved due to a convergence of multiple technologies, including ubiquitous wireless communication, real-time analytics, machine learning, commodity sensors, and embedded systems. This means that the traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things (IoT).

The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. Mark Weiser's seminal 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IoT. In 1994 Reza Raji described the concept in IEEE Spectrum as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1996 several companies proposed solutions like Microsoft's at Work or Novell's NEST. However, only in 1999 did the field start gathering momentum. Bill Joy envisioned Device to Device (D2D) communication as part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999. The concept of the Internet of things became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications. Radio-frequency identification (RFID) was seen by Kevin Ashton (one of the founders of the original Auto-ID Center) as a prerequisite for the Internet of things at that point. Ashton prefers the phrase "Internet for Things." If all objects and people in daily life were equipped withidentifiers, computers could manage and inventory them. Besides using RFID, the tagging of things may be achieved through such technologies as near field communication, barcodes, QR codes and digital watermarking. In its original interpretation, [when?] one of the first consequences of implementing the Internet of things by equipping all objects in the world with minuscule identifying devices or machine-readable identifiers would be to transform daily life. For instance, instant and ceaseless inventory control would become ubiquitous. [39] A

person's ability to interact with objects could be altered remotely based on immediate or present needs, in accordance with existing end-user agreements. For example, such technology could grant motion-picture publishers much more control over end-user private devices by remotely enforcing copyright restrictions and digital rights management, so the ability of a customer who bought a Blu-ray disc to watch the movie could become dependent on the copyright holder's decision, similar to Circuit City's failed DIVX.

According to Gartner, Inc. (a technology research and advisory corporation), there will be nearly 20.8 billion devices on the Internet of things by 2020. ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of things by 2020. As per a 2014 survey and study done by Pew Research Internet Project, a large majority of the technology experts and engaged Internet users who responded 83 percent agreed with the notion that the Internet/Cloud of Things, embedded and wearable computing (and the corresponding dynamic systems) will have widespread and beneficial effects by 2025. As such, it is clear that the IoT will consist of a very large number of devices being connected to the Internet. In an active move to accommodate new and emerging technological innovation, the UK Government, in their 2015 budget, allocated £40,000,000 towards research into the Internet of things. The former British Chancellor of the Exchequer George Osborne posited that the Internet of things is the next stage of the information revolution and referenced the inter-connectivity of everything from urban transport to medical devices to household appliances. The ability to network embedded devices with limited CPU, memory and power resources means that IoT finds applications in nearly every field. Such systems could be in charge of collecting information in settings ranging from natural ecosystems to buildings and factories, thereby finding applications in fields of environmental sensing and urban planning .On the other hand, IoT systems could also be responsible for performing actions, not just sensing things. Intelligent shopping systems, for example, could monitor specific users' purchasing habits in a store by tracking their specific mobile phones. These users could then be provided with special offers on their favorite products, or even location of items that they need, which their fridge has automatically conveyed to the phone. Additional examples of sensing and actuating are reflected in applications that deal with heat, water, electricity and energy management, as well as cruise-assisting transportation systems. Other applications that the Internet of things can provide is enabling extended home security features and home automation. The concept of an "Internet of living things" has been

proposed to describe networks of biological sensors that could use cloud-based analyses to allow users to study DNA or other molecules. However, the application of the IoT is not only restricted to these areas. Other specialized use cases of the IoT may also exist. An overview of some of the most prominent application areas is provided here. Based on the application domain, IoT products can be classified broadly into five different categories: smart wearable, smart home, smart city, smart environment, and smart enterprise. The IoT products and solutions in each of these markets have different characteristics.

2.2 EVOLUTION OF INTERNET:

Internet of boffins:

This was the era when ARPANET (Advanced Research Project Agency Network) carried its first data packet in 1969. It was the first network to use TCP/IP. This was followed by the Mark I Network in 1970, which was built by Davis. This network was a packet switched network to serve NPL in UK. It was soon replaced by Mark II in 1973. The other major inventions such as Telnet in 1974, Ethernet in 1980, GOSIP in 1190 and a full text web search engine in 1994 followed the trend. This era is called 'Internet of Boffins' since in this era internet was in a stage of early evolution and research.

Internet of geeks:

'Internet of Geeks' era started with the proposal of IPv6. It was the latest revision of the internet protocol. The communication protocol provides identification and location system for computers on networks and routes traffic across internet. The popular internet services started taking roots in this era. Amazon.com started its first online retail service in 1995, followed by eBay providing

customers with online auction and shopping services. Hotmail started its free web based email service in 1996, followed by Google search in 1998. PayPal started its first internet payment service in 1998. Internet penetration was low in the market until 2000.

Internet of masses:

'Internet of masses' era started with the Dot-com bubble burst in 2000. In the starting of this era Dot-com bubble burst led to high growth in stock markets due to increasing use of internet in the industrial sector. In this era many people across the globe started using internet. Social networking sites came into existence. In 2001 Wikipedia came into existence followed by Facebook in 2004, further followed by YouTube, Twitter and WikiLeaks in the consecutive years.

Mobile internet:

'Mobile Internet' era refers to access to the Internet via cellular phone service provider. The era got a boost with introduction of smartphones which gave a fast working internet on phones. This was the era from 2007-2011. There was steep rise in the use of internet by the people round the globe due to the mobile internet.

Internet of things:

'Internet of Things' refers to an era where things can be connected to each other using internet.

2.3 IMPACT OF INTERNET

The uses of internet include but not limited to usage of search engines which will help you to collect data from all over the world, usage of email and other instant message services which are giving flexibility of sharing information among groups within seconds, usage of internet in shopping via online shopping carts helped both clients and customers. Internet has become a platform to share knowledge between different communities. Several universities are publishing their research papers in their websites/digital libraries and helping other university students, researchers and professors scholar activities**.**

2.4 INTERNET USAGE

IDC estimates Internet of Things (IoT) market to grow to $8.9 trillion with over 212 billion connected things by 2020. The no. of connected devices surpassed total world population in year

2005 and it is estimated that no. of devices will be around 50 billion which is about 7 times of the world population at that time.

From the simplest day to day activities to the most complex human emotions, IoT will impact it.

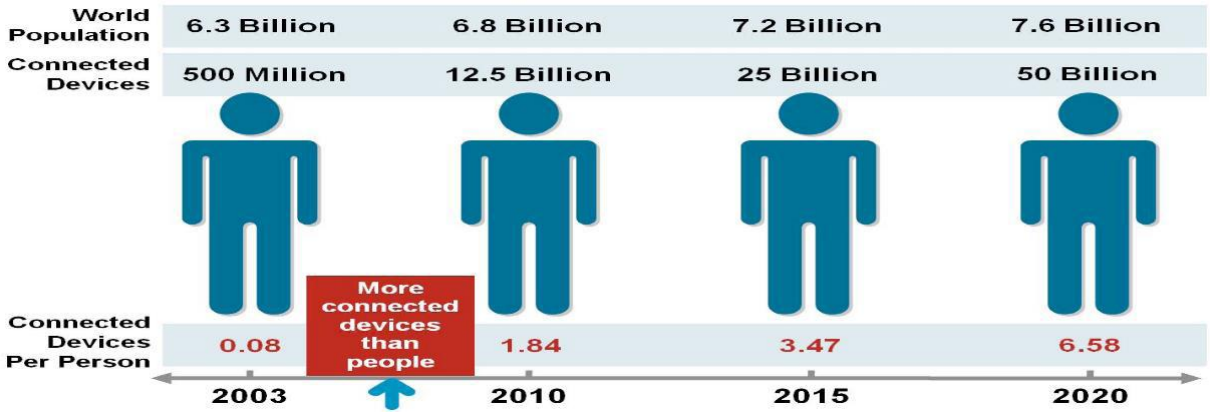


Fig1. Internet Usage and Population Statistics

CHAPTER THREE

METHODOLOGY/ARCHITECTURE

3.0 ARCHITECTURE OF INTERNET OF THINGS

Architecture of internet of Things contains basically 4 layers:

1. Application Layer
2. Gateway and the network layer
3. Management Service layer
4. Sensor layer

Application Layer

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

Gateway And The Network Layer

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

Management Layer

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

Sensor Layer

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

3.1 RFID (Radio-Frequency Identification)

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. 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 automobile during production can be used to track its progress through the assembly line; RFID-tagged pharmaceuticals 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. 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 intractability, 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.

3.2 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 microelectromechanical system (MEMS) and are manufactured in much the same way microprocessors are manufactured, through a lithography process. 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 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. In either case, you get a machine-generated message describing the findings.

3.3 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.

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 they may now be referred to by other agents, such as powerful centralized servers acting for their human owners.

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. 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.

3.4 CLOUD CENTRIC INTERNET OF THINGS

The vision of IoT can be seen from two perspectives— 'Internet' centric and 'Thing' centric. The Internet centric architecture will involve internet services being the main focus while data is contributed by the objects. In the object centric architecture, the smart objects take the center stage. In order to realize the full potential of cloud computing as well as ubiquitous sensing, a combined framework with a cloud at the center seems to be most viable. This not only gives the flexibility of dividing associated costs in the most logical manner but is also highly scalable.

Sensing service providers can join the network and offer their data using a storage cloud; analytic tool developers can provide their software tools; artificial intelligence experts can provide their data mining and machine learning tools useful in converting information to knowledge and finally computer graphics designers can offer a variety of visualization tools. Cloud computing can offer these services as Infrastructures, Platforms or Software where the full potential of human creativity can be tapped using them as services.

The new IoT application specific framework should be able to provide support for:

(1) Reading data streams either from sensors directly or fetch the data from databases.

(2) Easy expression of data analysis logic as functions/operators that process data streams in a transparent and scalable manner on Cloud infrastructures

(3) If any events of interest are detected, outcomes should be passed to output streams, which are connected to a visualization program. Using such a framework, the developer of IoT applications will able to harness the power of Cloud computing without knowing low-level details of creating reliable and scale applications.

3.5 INTERNET OF THINGS IN 2016

Smartwatches

Smartwatches broke new ground last year, with the popularity of the devices like the pebble and the Galaxy Gear. More mart watches making their way in the market with better and at the feasible prices. With apple's long-anticipated announcement of the Apple Watch, as the company has been ramping up its sapphire glass production and flexible, wearable watch like patents.

Industry Innovators: Pebble, Metawatch, Samsung Galaxy Gear

The Automated home

Popular devices like Google's Nest Smart Thermostat and WeMo's electrical outlet controller gained in popularity last year. Since then, numerous home automation IoT technologies have flourished- everything from smart locks to Wi-Fi enabled light bulbs.

Industry Innovators: Nest, Lockitron, Lifx

Fitness and Health Tracking

Last year, health and fitness devices like Nike Fuel band and Jawbone Up were among the most popular IoT gadgets, making large appearance at CES.

Industry Innovators: Fitbit, Nike, Jawbone

Connected Retail

Traditional retailer store is struggling to keep up with the growing e-commerce. Thanks to the Internet of Things, innovators have started to breathe new life into the retail experience- offering connected point of sale systems, NFC payments solutions and supply chain software's.

Industry Innovators: Shopkeep, Cisco, Placemeter

Virtual Augmented Reality

Last year Oculus Rift and Google glass made headline in both the virtual and augmented Reality worlds. Oculus was acquired by Facebook for $2.3 Billion earlier this year and Google glass recently rolled out a one-day sale of its "Explorer Edition".

Industry Innovators: Oculus, Google Glass, Sony

3.6 APPLICATIONS OF INTERNET OF THINGS

According to Gartner, Inc. (a technology research and advisory corporation), there will be nearly 26 billion devices on the Internet of Things by 2020. ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of Things by 2020. As per a recent survey and study done by Pew Research Internet Project, a large majority of the technology experts and engaged Internet users who responded—83 percent—agreed with the notion that the Internet/Cloud of Things, embedded and wearable computing (and the corresponding dynamic systems) will have widespread and beneficial effects by 2025. As such, it is clear that the IoT will consist of a very large number of devices being connected to the Internet. In an active move to accommodate new and emerging technological innovation, the UK Government, in their 2015 budget, allocated £40,000,000 towards research into the Internet of Things. The British Chancellor of the Exchequer George Osborne, posited that the Internet of Things is the next stage of the information revolution and referenced the inter-connectivity of everything from urban transport to medical devices to household appliances.

Integration with the Internet implies that devices will use an IP address as a unique identifier. However, due to the limited address space of IPv4 (which allows for 4.3 billion unique addresses), objects in the IoT will have to use IPv6 to accommodate the extremely large address space required. Objects in the IoT will not only be devices with sensory capabilities, but also provide actuation capabilities (e.g., bulbs or locks controlled over the Internet). To a large extent,

the future of the Internet of Things will not be possible without the support of IPv6; and consequently the global adoption of IPv6 in the coming years will be critical for the successful development of the IoT in the future.

The ability to network embedded devices with limited CPU, memory and power resources means that IoT finds applications in nearly every field. Such systems could be in charge of collecting information in settings ranging from natural ecosystems to buildings and factories, thereby finding applications in fields of environmental sensing and urban planning.

On the other hand, IoT systems could also be responsible for performing actions, not just sensing things. Intelligent shopping systems, for example, could monitor specific users' purchasing habits in a store by tracking their specific mobile phones. These users could then be provided with special offers on their favorite products, or even location of items that they need, which their fridge has automatically conveyed to the phone. Additional examples of sensing and actuating are reflected in applications that deal with heat, electricity and energy management, as well as cruise-assisting transportation systems. Other applications that the Internet of Things can provide is enabling extended home security features and home automation. The concept of an "internet of living things" has been proposed to describe networks of biological sensors that could use cloud-based analyses to allow users to study DNA or other molecules. All these advances add to the numerous list of IoT applications. Now with IoT, you can control the electrical devices installed in your house while you are sorting out your files in office. Your water will be warm as soon as you get up in the morning for the shower. All credit goes to smart devices which make up the smart home. Everything connected with the help of Internet. However, the application of the IoT is not only restricted to these areas. Other specialized use cases of the IoT may also exist. An overview of some of the most prominent application areas is provided here. Based on the application domain, IoT products can be classified broadly into five different categories: smart wearable, smart home, smart city, smart environment, and smart enterprise. The IoT products and solutions in each of these markets have different characteristics.

Media

In order to hone the manner in which the Internet of Things (IoT), the Media and Big Data are interconnected, it is first necessary to provide some context into the mechanism used for media process. It has been suggested by Nick Couldry and Joseph Turow that Practitioners in Media approach Big Data as many actionable points of information about millions of individuals. The

industry appears to be moving away from the traditional approach of using specific media environments such as newspapers, magazines, or television shows and instead tap into consumers with technologies that reach targeted people at optimal times in optimal locations. The ultimate aim is of course to serve, or convey, a message or content that is (statistically speaking) in line with the consumer's mindset. For example, publishing environments are increasingly tailoring messages (advertisements) and content (articles) to appeal to consumers that have been exclusively gleaned through various data-mining activities.

The media industries process Big Data in a dual, interconnected manner:

1. Targeting of consumers (for advertising by marketers)
2. Data-capture

Thus, the internet of things creates an opportunity to measure, collect and analyze an ever-increasing variety of behavioral statistics. Cross-correlation of this data could revolutionize the targeted marketing of products and services. For example, as noted by Danny Meadows-Klue, the combination of analytics for conversion tracking withbehavioural targeting has unlocked a new level of precision that enables display advertising to be focused on the devices of people with relevant interests. Big Data and the IoT work in conjunction. From a media perspective, Data is the key derivative of device inter connectivity, whilst being pivotal in allowing clearer accuracy in targeting. The Internet of Things therefore transforms the media industry, companies and even governments, opening up a new era of economic growth and competitiveness. The wealth of data generated by this industry (i.e. Big Data) will allow Practitioners in Advertising and Media to gain an elaborate layer on the present targeting mechanisms used by the industry.

Environmental monitoring

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection by monitoring air or water quality, atmospheric or soil conditions, and can even include areas like monitoring the movements of wildlife and their habitats.[61] Development of resource constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically span a large geographic area and can also be mobile.

Infrastructure management

Monitoring and controlling operations of urban and rural infrastructures like bridges, railway tracks, on- and offshore- wind-farms is a key application of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities.] IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas. Even areas such as waste management can benefit from automation and optimization that could be brought in by the IoT.

11.3 Manufacturing

Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm on industrial applications and smart manufacturing as well. The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together.

Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT. But it also extends itself to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability. Smart industrial management systems can also be integrated with the Smart Grid, thereby enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors.

Energy management

Integration of sensing and actuation systems, connected to the Internet, is likely to optimize energy consumption as a whole. It is expected that IoT devices will be integrated into all forms of energy consuming devices (switches, power outlets, bulbs, televisions, etc.) and be able to communicate with the utility supply company in order to effectively balance power generation

and energy usage. Such devices would also offer the opportunity for users to remotely control their devices, or centrally manage them via a cloud based interface, and enable advanced functions like scheduling (e.g., remotely powering on or off heating systems, controlling ovens, changing lighting conditions etc.). In fact, a few systems that allow remote control of electric outlets are already available in the market, e.g., Belkin's WeMo, Ambery Remote Power Switch, Budderfly, Telkonet's EcoGuard, WhizNets Inc., etc.

Besides home based energy management, the IoT is especially relevant to the Smart Grid since it provides systems to gather and act on energy and power-related information in an automated fashion with the goal to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. Using Advanced Metering Infrastructure (AMI) devices connected to the Internet backbone, electric utilities can not only collect data from end-user connections, but also manage other distribution automation devices like transformers and reclosers.

Medical and healthcare systems

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

Building and home automation

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential).

Home automation systems, like other building automation systems, are typically used to control lighting, heating, ventilation, air conditioning, appliances, communication systems, entertainment and home security devices to improve convenience, comfort, energy efficiency, and security.

Transportation

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

3.7 SECURITY AND SECURITY CHALLENGES

Concerns have been raised that the Internet of things is being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary. According to the Business Insider Intelligence Survey conducted in the last quarter of 2014, 39% of the respondents said that security is the biggest concern in adopting Internet of things technology. In particular, as the Internet of things spreads widely, cyber-attacks are likely to become an increasingly physical (rather than simply virtual) threat. In a January 2014 article in Forbes, cybersecurity columnist Joseph Steinberg listed many Internet-connected appliances that can already "spy on people in their own homes" including televisions, kitchen appliances, cameras, and thermostats. Computer-controlled devices in automobiles such as brakes, engine, locks, hood and truck releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the onboard network. In some cases, vehicle computer systems are Internet- connected, allowing them to be exploited remotely. By 2008 security researchers had shown the ability to remotely control pacemakers without authority. Later hackers demonstrated remote control of insulin pumps and implantable cardioverter defibrillators. David Pogue wrote that some recently published reports about hackers remotely controlling certain functions of automobiles were not as serious as one might otherwise guess because of various mitigating circumstances; such as the bug that allowed the hack having

been fixed before the report was published, or that the hack required security researchers having physical access to the car prior to the hack to prepare for it.

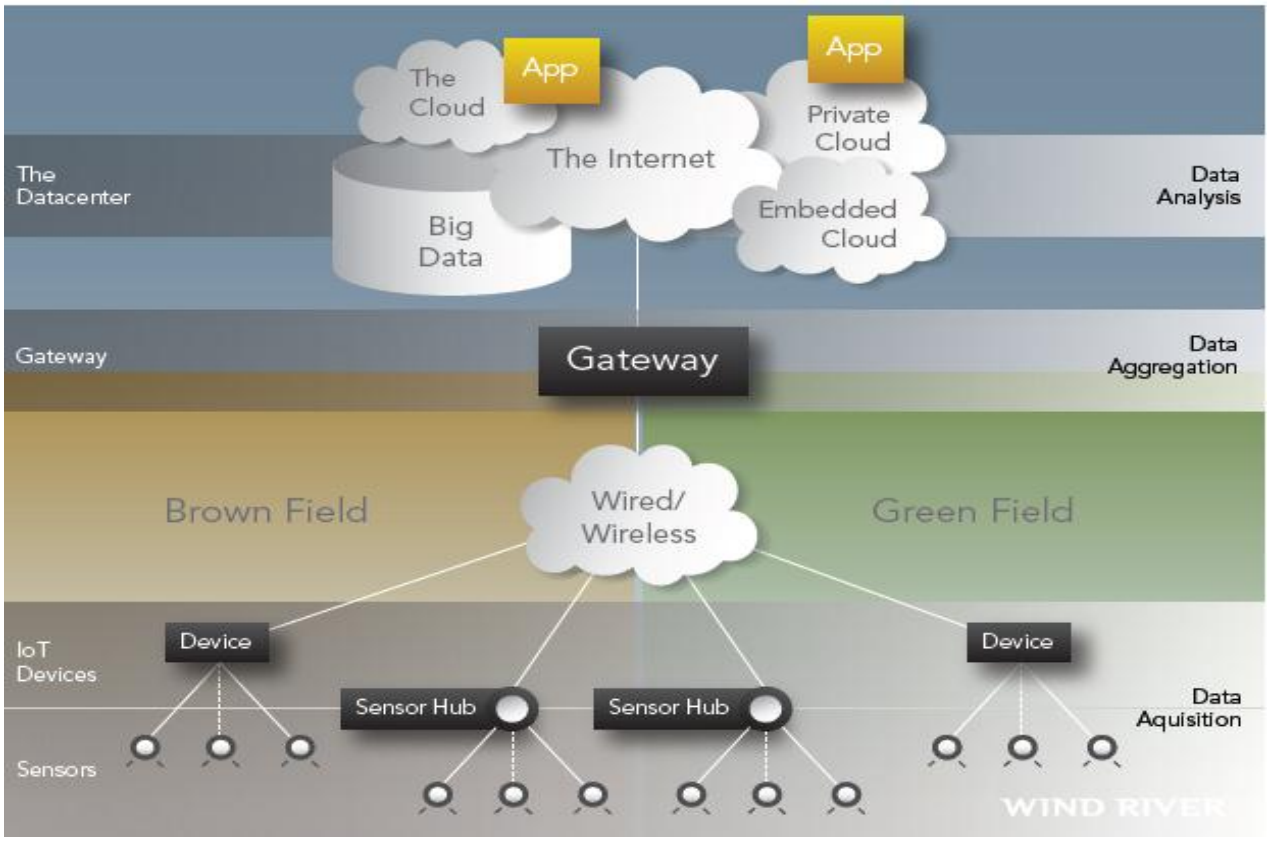
3.8 NEW THREATS, CONSTRAINTS, AND CHALLENGES

Applying these same practices or variants of them in the IoT world requires substantial reengineering to address device constraints. Blacklisting, for example, requires too much disk space to be practical for IoT applications. Embedded devices are designed for low power consumption, with a small silicon form factor, and often have limited connectivity. They typically have only as much processing capacity and memory as needed for their tasks. And they are often "headless" that is, there isn't a human being operating them who can input authentication credentials or decide whether an application should be trusted; they must make their own judgments and decisions about whether to accept a command or execute a task.

The endless variety of IoT applications poses an equally wide variety of security challenges. For example In factory floor automation, deeply embedded programmable logic controllers (PLCs) that operate robotic systems are typically integrated with the enterprise IT infrastructure. How can those PLCs be shielded from human interference while at the same time protecting the investment in the IT infrastructure and leveraging the security controls available?

Similarly, control systems for nuclear reactors are attached to infrastructure. How can they receive software updates or security patches in a timely manner without impairing functional safety or incurring significant recertification costs every time a patch is rolled out?

A smart meter one which is able to send energy usage data to the utility operator for dynamic billing or real-time power grid optimization must be able to protect that information from unauthorized usage or disclosure. Information that power usage has dropped could indicate that a home is empty, making it an ideal target for a burglary or worse.



A generic Internet of Things topology: A typical IoT deployment will consist of sensor-equipped edge devices on a wired or wireless network sending data via a gateway to a public or private cloud. Aspects of the topology will vary broadly from application to application; for example, in some cases the gateway may be on the device. Devices based on such topologies may be built from the ground up to leverage IoT (Greenfield) or may be legacy devices that will have IoT capabilities added post-deployment (brownfield).

3.9 BUILDING SECURITY IN FROM THE BOTTOM UP

Knowing no one single control is going to adequately protect a device, how do we apply what we have learned over the past 25 years to implement security in a variety of scenarios? We do so through a multi-layered approach to security that starts at the beginning when power is applied,

establishes a trusted computing baseline, and anchors that trust in something immutable that cannot be tampered with.

Security must be addressed throughout the device lifecycle, from the initial design to the operational environment:

1. **Secure booting:** When power is first introduced to the device, the authenticity and integrity of the software on the device is verified using cryptographically generated digital signatures. In much the same way that a person signs a check or a legal document, a digital signature attached to the software image and verified by the device ensures that only the software that has been authorized to run on that device, and signed by the entity that authorized it, will be loaded. The foundation of trust has been established, but the device still needs protection from various run-time threats and malicious intentions.
2. **Access control:** Next, different forms of resource and access control are applied. Mandatory or role-based access controls built into the operating system limit the privileges of device components and applications so they access only the resources they need to do their jobs. If any component is compromised, access control ensures that the intruder has as minimal access to other parts of the system as possible. Device-based access control mechanisms are analogous to network-based access control systems such as Microsoft® Active Directory®: even if someone managed to steal corporate credentials to gain access to a network, compromised information would be limited to only those areas of the network authorized by those particular credentials. The principle of least privilege dictates that only the minimal access required to perform a function should be authorized in order to minimize the effectiveness of any breach of security.
3. **Device authentication:** When the device is plugged into the network, it should authenticate itself prior to receiving or transmitting data. Deeply embedded devices often do not have users sitting behind keyboards, waiting to input the credentials required to access the network. How, then, can we ensure that those devices are identified correctly prior to authorization? Just as user authentication allows a user to access a corporate network based on user name and password, machine authentication allows a device to access a network based on a similar set of credentials stored in a secure storage area.

4. **Firewalling and IPS:** The device also needs a firewall or deep packet inspection capability to control traffic that is destined to terminate at the device. Why is a host-based firewall or IPS required if network-based appliances are in place? Deeply embedded devices have unique protocols, distinct from enterprise IT protocols. For instance, the smart energy grid has its own set of protocols governing how devices talk to each other. That is why industry-specific protocol filtering and deep packet inspection capabilities are needed to identify malicious payloads hiding in non-IT protocols. The device needn't concern itself with filtering higher-level, common Internet traffic the network appliances should take care of that but it does need to filter the specific data destined to terminate on that device in a way that makes optimal use of the limited computational resources available.
5. **Updates and patches:** Once the device is in operation, it will start receiving hot patches and software updates. Operators need to roll out patches, and devices need to authenticate them, in a way that does not consume bandwidth or impair the functional safety of the device. It's one thing when Microsoft sends updates to Windows® users and ties up their laptops for 15 minutes. It's quite another when thousands of devices in the field are performing critical functions or services and are dependent on security patches to protect against the inevitable vulnerability that escapes into the wild. Software updates and security patches must be delivered in a way that conserves the limited bandwidth and intermittent connectivity of an embedded device and absolutely eliminates the possibility of compromising functional safety.

CHAPTER FOUR

4.0 SUMMARY AND CONCLUSION

4.1 SUMMARY

The Internet of Things (IoT) is defined in many different ways, and it encompasses many aspects of life from connected homes and cities to connected cars and roads, roads to devices that track an individual s behavior and use the data collected for push services. The Internet of Things is an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data authentication, access control and client privacy need to be established.

4.2 CONCLUSION

As often happens, history is repeating itself. Just as in the early days when Cisco's tagline was "The Science of Networking Networks," IoT is at a stage where disparate networks and a multitude of sensors must come together and interoperate under a common set of standards. This effort will require businesses, governments, standards organizations, and academia to work together toward a common goal. Next, for IoT to gain acceptance among the general populace, service providers and others must deliver applications that bring tangible value to peoples' lives. IoT must not represent the advancement of technology for technology's sake; the industry needs to demonstrate value in human terms.

In conclusion, IoT represents the next evolution of the Internet. Given that humans advance and evolve by turning data into information, knowledge, and wisdom, IoT has the potential to change the world as we know it today for the better. How quickly we get there is up to us.

REFERENCES

Caruso, M. J. (2007a). "Applications of Magnetoresistive Sensors in Navigation Systems." Honeywell PositionSensing Solutions Retrieved December, 29, 2009, from http://www.ssec.honeywell.com/magnetic/.

Caruso, M. J. (2007c). "Applications of Magnetic Sensors for Low Cost Compass Systems." Honeywell Magnetic Sensors Retrieved December, 29, 2009, from http://www.ssec.honeywell.com/magnetic/datasheets/lowcost.pdf.

Caruso, M. J., & Withanawasam, L.S. (2007b). "Vehicle Detection and Compass Applications using AMR Magnetic Sensors." Honeywell Magnetic Sensors Retrieved December, 29, 2009, from http://www.ssec.honeywell.com/magnetic/.

Caruso, M. J., Bratland, T., Smith, C.H., & Schneider, R. (2007d). "A New Perspective on Magnetic Field Sensing." Honeywell Magnetic Sensors Retrieved December, 30, 2009, from http://www.ssec.honeywell.com/magnetic/datasheets/new_pers.pdf.

Cavallo, F., Sabatini, A.M. , & Genovese, V. (2005). A step toward GPS/INS personal navigation systems: realtime assessment of gait by foot inertial sensing Intelligent Robots and Systems, 2005. (IROS 2005). 2005 IEEE/RSJ International Conference on Edmond, Alberta, Canada.

Cea, A., Dobre, D., Bajic, E. (2006). Ambient Services Interactions for Smart Objects in the Supply Chain. Service Systems and Service Management, 2006 International Conference on Troyes.

https://en.wikipedia.org/wiki/Internet_of_Things

www.wired.com/insights/2014/11/the-**internet-of-things**-bigger/

http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

http://www.theinternetofthings.eu/