IoT: Challenges in the standardization of IoT communication

Shrivastava Vandana Jaiprakash
Masters of Computer Applications
Mumbai, India

***Abstract* - The phrase Internet of Things (IoT) projects a vision of the future Internet where connecting all physical things through a network will allow them to have an active part in the Internet, exchanging information about themselves and their surroundings. This will give immediate access to information about the physical world and the objects in it leading to innovative services and increase in efficiency and productivity. This paper reviews what the Internet of Things means as a phenomenon, how standards form in this field and challenges for Internet of Things standardization. Since IoT is global phenomenon standardization plays a key role in the development of IoT. For this reason this paper focuses on the standardization activities. Standards should also serve the requirements of different application domains such as variety of industry sectors, society, environment and individual citizens.**

***Index Terms* - Internet of Things (IoT), web, internet, standards, communication, standardization, smart devices, and network**

I. INTRODUCTION

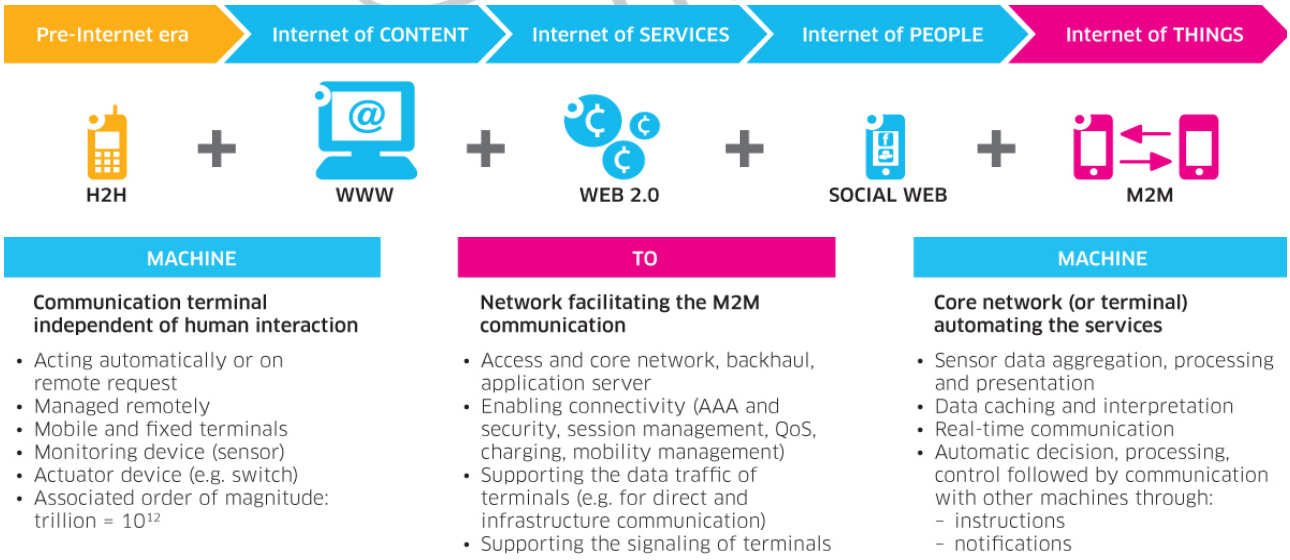
Internet of Things (IoT) refers to a recent paradigm that has been rapidly gaining ground in the area of modern wireless telecommunications. IoT is a new technological trend joining new computing and communications paradigms. Within this new trend, there are intelligent devices that have a digital entity and are interconnected on a network and to the global Internet. Everyday objects may integrate intelligence and the ability to sense, interpret and react to their environment, combining the Internet with emerging technologies.

The Internet of Things (IoT) will reach out into everyday objects and environments by connecting tiny embedded computers that can perceive their environment.

The Internet of Things (IoT) is focused on connecting the human to the world. Convenience, time-management, economics, and entertainment are all significant benefits that people seek through greater connectivity. Though data analytics are always in the background, the connected human is sending and receiving small packets of data to and from their devices to realize the benefits provided by a digital lifestyle.

The Internet of Things (IoT) is a concept that describes a totally interconnected world. It's a world where devices of every shape and size are manufactured with "smart" capabilities that allow them to communicate and interact with other devices, exchange data, make autonomous decisions and perform useful tasks based on preset conditions.

Several industrial, standardization and research bodies are currently involved in the activity of development of solutions to fulfill the technological requirements of IoT.



II. VISION AND IOT SCOPE

The main form of communication on the Internet is human-human. But it is foreseeable in near future that any object will have a unique way of identification and can be addressed so that every object can be connected. The Internet will become the Internet of Things. The communication forms will expand from human-human to human-human, human-thing and thing-thing (also called M2M).This will bring a new computing and communication era and change people's life extremely. Radio Frequency Identification techniques (RFID) and related identification technologies will be the cornerstones of the upcoming Internet of Things (IOT).

Many people hold the view that cities and the world itself will be overlaid with sensing and actuation, many embedded in "things" creating what is referred to as a *smart world*. But it is important to note that one key issue is the degree of the density of sensing and actuation coverage. I believe that there will be a transition point when the degree of coverage triples or quadruples from what we have today.

For example, today many buildings already have sensors for attempting to save energy; home automation is occurring; cars, taxis, and traffic lights have devices to try and improve safety and transportation; people have smartphones with sensors for running many useful apps; industrial plants are connecting to the Internet; and healthcare services are relying on increased home sensing to support remote medicine and wellness. However, all of these are just the tip of the iceberg. They are all still at early stages of development. The steady increasing density of sensing and the sophistication of the associated processing will make for a significant change in how we work and live. We will truly have systems-of-systems that simultaneously interact to form totally new and unpredictable services.

What will be the platform or platforms that support such a vision? One possibility is a global sensing and actuation utility connected to the Internet. Electricity and water are two utilities that can be used for a myriad of purposes. Sensing and actuation in the form of an IoT platform will become a utility. IoT will not be seen as individual systems, but as a critical, integrated infrastructure upon which many applications and services can run. Some applications will be personalized such as digitizing daily life activities, others will be city-wide such as efficient, delay-free transportation, and others will be worldwide such as global delivery systems.

In cities perhaps there will be no traffic lights and even 3D transportation vehicles. Smart buildings will not only control energy or security, but integrate personal comfort, energy savings, security and health and wellness aspects into convenient and effective spaces. Individuals may have patches of bionic skin with sensing of physiological parameters being transmitted to the cloud which houses his digital health, and to the surrounding smart spaces for improved comfort, health, efficiency, and safety. In fact, smart watches, phones, body nodes, and clothes will act as personalized input to optimize city-wide services benefiting both the individual and society.

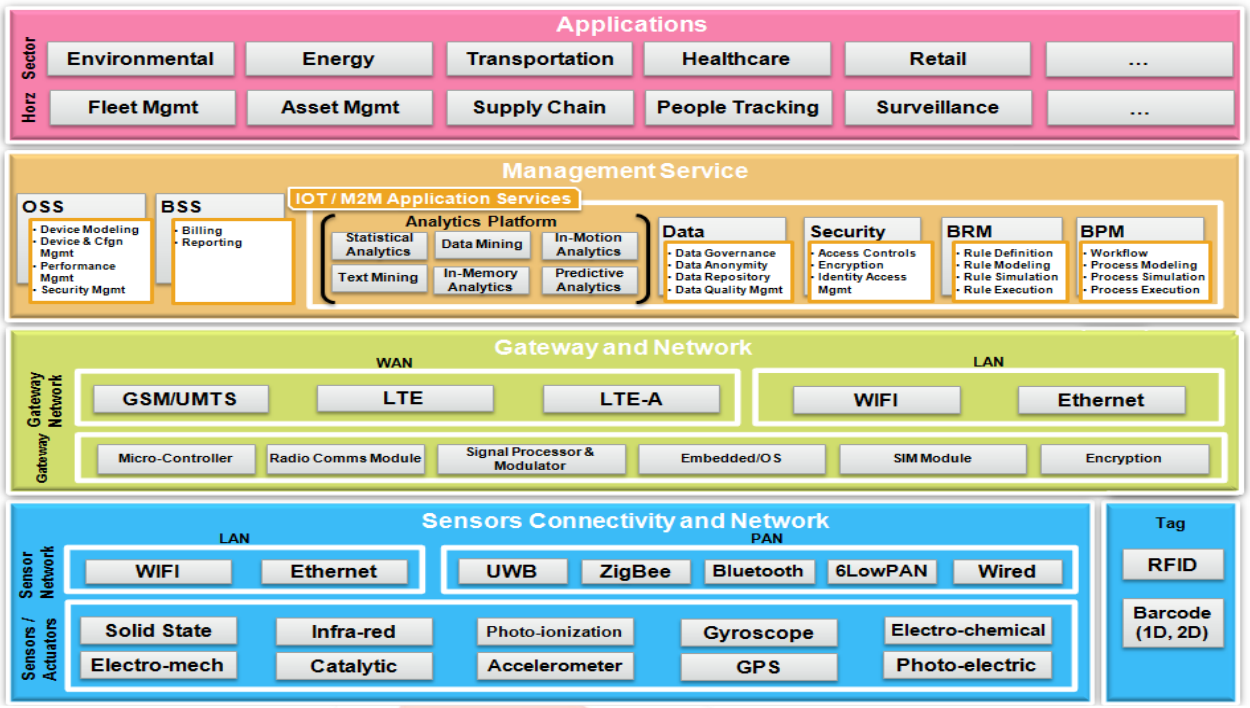
Consequently, we will often be implicitly linked into the new utility. Some examples of new services include immediate and continuous access to the right information for the task at hand, be it, traveling to work or a meeting, exercising, shopping, socializing, or visiting a doctor. Sometimes these activities will be virtual activities, or even include the use of robots. Many outputs and displays for users may be holographic. Credit cards should disappear and biometrics like voice or retinas will provide safe access to buildings, ATMs, and transportation systems.

A sensing and actuation utility will not only exist in public spaces, but also extend into the homes. Here people will be able to run health, energy, security, and entertainment apps on the infrastructure. Installing and running new apps will be as easy as plugging in a new toaster into the electric utility. One app may help monitor and control heart rate, another performs financial and investments services, another automatically ordering food and wine, or even predicting a impending medical problem that should be addressed early to avoid the problem. Humans will often be integral parts of the IoT system. The Industrial Internet is also a form of IoT where the devices (things) are objects in manufacturing plants, dispatch centers, process control industries, etc.

The Industrial Internet of Things (IIoT) is focused on connecting the entire enterprise. For large industries such as oil and gas, electric power, chemical, and pharmaceutical companies, the significant drivers are safety, efficiency, data management and productivity. Data acquisition from every connected device, seamless control connectivity to every control point, and data analytics are critical to operating large industrial enterprises. These large organizations were acquiring and transmitting much of this data prior to the internet becoming a functional business tool.

Consequently, in the future the scope of IoT is enormous and will affect every aspect of all our lives.

III. IoT Architecture



Architecture of IoT

According to the recommendations of the International Telecommunication Union, the network architecture of IoT consists of the sensing layer, the access layer, the network layer, the middleware layer and application layers.

Sensing layer: the main features of this layer are to capture the interest information in large-scale by various types of sensors, identify intelligently, and share the captured information in the related units in the network.

The access layer: this layer's main function is to transfer information from the sensing layer to the network layer through existing mobile networks, wireless networks, wireless LANs, satellite networks and other infrastructure.

Network layer: this layer's main function is to integrate the information resources of the network into a large intelligence network with the Internet platform, and establish an efficient and reliable infrastructure platform for upper-class service management and large-scale industry applications.

The middleware layer: this layer's main function is management and control of network information in real-time, as well as providing a good user interface for upper layer application. It includes various business support platform, management platform, information processing platform, and intelligent computing platform.

Application layer: this layer's main function is to integrate the function of the bottom system, and build the practical application of various industries, such as smart grids, smart logistics, intelligent transportation, precision agriculture, disaster monitoring and distance medical care.

IV. Communication in IoT

Open platforms and standards will create a base for innovation from companies of all types and sizes. Open standards and interoperability are vital to building the Internet of Things. An environment where such a wide variety of devices and applications must work together simply cannot function unless it remains free from closed, proprietary standards.

The Internet of Things (IoT) describes the interconnection of objects (or Things) for various purposes including identification, communication, sensing, and data collection. "Things" in this context range from traditional computing devices like Personal Computers (PC) to general household objects embedded with capabilities for sensing and/or communication through the use of technologies such as Radio Frequency Identification (RFID).

The idea of Internet of Things that all the items were connected to Internet by sensor devices such as RFID (Radio Frequency Identification, RFID) in order to accomplish intelligent recognition and network management was first proposed by Auto-ID laboratory in MIT (Massachusetts Institute of Technology) in 1999. Its core support technology is a wireless sensor network and radio frequency identification technology.

The IoT concept is based on the idea of a universal presence of 'things' or 'objects', such as RFID tags, sensors, actuators, mobile phones, etc, with digital identification and addressing schemes that enable them to cooperate with neighbors in order to achieve some common goals. In the business sector, the most apparent consequences of IoT may arise in industrial automation and manufacturing, in logistics, in business or process management and in intelligent schemes for transporting people and goods.

Therefore, in general, the term Internet of Things refers to any type of devices that are interconnected by means of Machine-to-Machine Communications (M2M), each of which may be identified through a unique ID and defined through a virtual representation within the Internet.

Enablers of the IoT

A number of significant technology changes have come together to enable the rise of the IoT. These include the following.

- **Cheap sensors** – Sensor prices have dropped to an average 60 cents from $1.30 in the past 10 years.
- **Cheap bandwidth** – The cost of bandwidth has also declined, by a factor of nearly 40X over the past 10 years.
- **Cheap processing** – Similarly, processing costs have declined by nearly 60X over the past 10 years, enabling more devices to be not just connected, but smart enough to know what to do with all the new data they are generating or receiving.
- **Smartphones** – Smartphones are now becoming the personal gateway to the IoT, serving as a remote control or hub for the connected home, connected car, or the health and fitness devices consumers are increasingly starting to wear.
- **Wireless coverage** – With Wi-Fi coverage now ubiquitous, wireless connectivity is available for free or at a very low cost, given Wi-Fi utilizes unlicensed spectrum and thus does not require monthly access fees to a carrier.
- **Big data** – As the IoT will by definition generate voluminous amounts of unstructured data, the availability of big data analytics is a key enabler.
- **IPv6** – Most networking equipment now supports IPv6, the newest version of the Internet Protocol (IP) standard that is intended to replace IPv4. IPv4 supports 32-bit addresses, which translates to about 4.3 billion addresses – a number that has become largely exhausted by all the connected devices globally. In contrast, IPv6 can support 128-bit addresses, translating to approximately 3.4 x 1038 addresses – an almost limitless number that can amply handle all conceivable IoT devices.

Key Technology of IoT

Technologies like RFID, short-range wireless communication and sensor networks are means to achieve the network connectivity, while Internet protocol version 6 (IPv6), with its expanded address space, enables addressing, connecting and tracking things.

RFID system uses radio frequency tags to bear information. To identify automatically, RFID tag and reader communicate by non-contact sensors, radio waves or microwaves. The most prominent feature of RFID technology is: non-contact reading and writing, distance from a few cm to dozens of meters, to recognize high speed moving objects, strong security, and can identify multiple targets simultaneously.

The key technologies of RFID includes high-adaptive wireless communication technology, high confidentiality; low power consumption, high reliability of RFID devices; small volume, high efficiency antenna technology; low-cost chip and reader.

V. STANDARDS IN IoT

Standards issues pose a challenge, but these will be resolved as the standards process continues to evolve.

The Internet of Things will eventually include billions of interconnected devices. It will involve manufacturers from around the world and countless product categories. All of these devices must communicate, exchange data and perform closely coordinated tasks—and they must do so without sacrificing security or performance.

It is required to provide a common communications technology that supports all applications/services as well as heterogeneous networking interfaces.

This sounds like a recipe for mass confusion. Fortunately, the building blocks to accomplish many of these tasks are already in place. These include:

• **Existing standards** such as Bluetooth®, Wi-Fi®, RFID, ZigBee®, Bluetooth Low Energy, Z-wave and IPv6 that provide a ready foundation for robust, highly scalable networking and communications;

• **Open hardware platforms** such as the ARM® architecture that provide a set of shared, baseline technologies for creating intelligent, networking-capable devices;

• **Emerging standards** such as 6LoWPAN, Weightless, 802.11ah, etc., that will support the wide range of communication and networking technologies required for a truly comprehensive Internet of Things;

• **Data standards** such as eXtensible Markup Language (XML) and Resource Description Framework (RDF) that support interoperable applications and devices;

• **Global standards bodies** such as IEEE, International Society of Automation (ISA), the World Wide Web Consortium (W3C), OMA, IETF and IPSO alliance (to name a few) bring together manufacturers, technology vendors, policymakers and other interested stakeholders.

Everybody involved in the standards-making process knows that one size will not fit all— multiple (and sometimes overlapping) standards are a fact of life when dealing with evolving technology. At the same time, a natural pruning process will encourage stakeholders to standardize and focus on a smaller number of key standards.

VI. CURRENT WORK ON STANDARDS

In development of standards, focus should be on designs that can support a wide range of applications. Standards should also serve the requirements of different application domains such as variety of industry sectors, society, environment and individual citizens.

Many competing standards can paralyze markets as users will wait for a dominant technology to emerge. To avoid such a situation, co-ordination between standardizing bodies is necessary and various formal contracts about these matters do exist.

Machine-to-Machine (M2M) standardization efforts in Europe are conducted by The European Telecommunications Standards Institute (ETSI). ETSI has formed a M2M Technical Committee specially to conduct standardization activities relevant to M2M systems and sensor networks. The committee works on development and maintenance of an end-to-end architecture as well as, standardization efforts on sensor network integration, naming addressing, location, Quality of Service, security, charging, management, application and hardware interfaces.

Technical interoperability is another issue that benefits from early adoption of standards. Promotion of interoperability has been recognized as an important factor for the development of IoT. They all deal with how systems can communicate, exchange data and use information.

A contrary approach to early adoption of standards is to let the community decide the mechanisms that work best, through trial and error. The view suggests that rigid standards development and regulation, does not give enough time for the dominant standard to emerge and artificial standards can be adopted prematurely.

A proposal for main application domains of IoT is: industry, environment and society. Industry consists of manufacturing, logistics, banking etc. Environment comprises among others of agriculture, recycling and energy management. And finally society deals with governmental issues such as services, society structures and e-inclusion.

While these applications domains have different goals their requirements are not significantly different.

In IoT standard design there are some special areas that need to be considered ensuring global interoperability. Some areas also have constraints concerning existing regulations. Example of such restriction is permitted frequency bands and power levels for radio frequency communications that needs to be addressed for all devices that make use of radio spectrum.

Different bands of radio spectrum have been allocated for various purposes, such as broadcast communications, mobile telephony, citizen band radio, emergency services communications, wireless internet and short-range radio.

Also the frequency band allocations are not identical between different regions of the world.

Existing standards

1. EPCglobal Standards

EPCglobal is an activity conducted by GS1. GS1 is a non-for-profit standards organization focusing on standards and solutions that improve the efficiency and transparency of supply and demand chains.

2. ETSI Standards

ETSI has published several standards concerning M2M. Machine-to-Machine (M2M) refers to common wireless and wired technologies that allow systems and devices to communicate with each other.

3. IETF Standards

Internet Engineering Task force (IETF) is the open recognized International Standards Organization (ISO) in charge of standardizing the IP protocol. IETF is organized into working groups that work on several areas including routing, transport and security.

Overview:

Organization	Std description	Nature	Early vs. late	Status
EPCglobal	Electronic Product Code	Vertical	Early	Ratified and in production use
ETSI	M2M Standards	Horizontal	Early/late	Communications: publication 2011 Functional architecture: publication 2011 Smart metering Use cases: publication 2010 M2M definitions: Stable draft 2012 mIa, dIa and mId interfaces: publication 2012
IETF	IP Protocol for Smart Objects	Horizontal	Late	6LowPAN: Proposed Standard RPL: Proposed Standard CoAP: in development

i. IEEE 802.15.4 (2.4 GHz) is now generally adopted as the Physical/Link Layer standard for low power sense and control networks, along with WiFi for content distribution networks, and Bluetooth for wearables.

ii. There is a potential war brewing at the Network/Transport Layer, where Google/Nest is trying to set the standard openly challenging the incumbent standardization body (the ZigBee Alliance). After having done the ground work, they have reformatted

themselves into an open body (the Thread Alliance). However, despite the hype and the industry politics, the Thread standard itself is incomplete and needs extending to be meaningful in the market.

iii. At the Application Layer, there is significant confusion and ongoing technology development required. Apple, Google/Nest, Intel, Qualcomm are trying to define standards. They are partially competing with the ZigBee Alliance, and at the same time, are partially complementary.

iv. The ZigBee Cluster Library is the only well developed and market proven Application Layer implementation that makes sense for any of the competing Application Layer frameworks. Embracing it can make the difference in the market acceptance for each of them.

v. Both IEEE 802.11ah (low-power WiFi for the MAC/PHY Layer) as well as Bluetooth Mesh (for the Network Layer) are late to market (2017 at the earliest).

VII. REQUIREMENT OF STANDARDS FOR FLOURISHING IoT

Standards play a central role in enabling the creation of markets for new technologies.

Standards should be designed to support a wide range of applications and address common requirements from a wide range of industry sectors as well as the needs of the environment, society and individual citizens. Through consensus processes involving multiple stakeholders, it will be possible to develop standardized semantic data models and ontologies, common interfaces and protocols, initially defined at an abstract level, then with example bindings to specific cross-platform, cross-language technologies such as XML, ASN.1, web services etc.

The use of machine-readable codification should help to overcome ambiguities resulting from human error or differences and misinterpretation due to different human languages in different regions of the world, as well as assisting with cross-referencing to additional information available through other systems.

Standards are required for bidirectional communication and information exchange among things, their environment, their digital counterparts in the virtual cloud and entities that have an interest in monitoring, controlling or assisting the things. In addition, the design of standards for IoT needs to consider efficient and judicial use of energy and network capacity, as well as respecting other constraints such as those existing regulations that restrict permitted frequency bands and power levels for radio frequency communications.

As IoT evolves, it may be necessary to review such regulatory constraints and investigate ways to ensure sufficient capacity for expansion, such as seeking additional radio spectrum allocation as it becomes available. A particular challenge in this regard is ensuring global interoperability particularly for things and devices that make use of radio spectrum.

As is typical for emerging technologies, commercial partnerships are driving competing standards for the Internet of Things. Left unchecked, this carries a risk of restrictive standards being set and enforced by monopolistic providers, and of fragmentation inhibiting the interoperability of devices, slowing growth and reducing the opportunities for entrepreneurs.

For the Internet of Things to flourish, interoperability must apply across all parts of the system, including the transmission networks and the data being transmitted. Data and devices must have proportionate "security by default". Standards must protect against cybercrime and national security threats, and help to ensure that the system is trustworthy and trusted. They should also support energy efficiency, as this will help increase the range of potential applications and manage the burden on energy supply.

Government can shape standards and support new market entrants through its commissioning practices. Funding scalable demonstrators is an excellent way both to enable innovators to develop new business models rapidly, and to ensure that standards are fit for purpose.

Government should play a leading role in seeking to achieve wider consensus with other governments and standards bodies, and could host international events to seize the initiative and demonstrate UK leadership.

While much progress has been made in the area of standards, more is needed, especially in the areas of security, privacy, architecture, and communications. IEEE is just one of the organizations working to solve these challenges by ensuring that IPv6 packets can be routed across different network types.

It is important to note that while barriers and challenges exist, they are not insurmountable. 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.

VIII. CONCLUSION

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.

While the Internet of Things is still in its infancy, this technology is poised for massive growth in the next decade. We are already seeing computer- and sensor-infused objects in a variety of industries, including automotive, energy, consumer electronics and in-home appliances.

As it becomes less expensive to integrate technology into physical objects, we will see more application and adoption of this technology.

The Internet of Things will have major implications for both business-to-business (B2B) and business-to-consumer (B2C) companies in the next five years.

IoT will undoubtedly be an information revolution following computers and Internet. Common standardization and understanding of the IoT domain is crucial for the realization of the paradigm. IoT standards can emerge from new technology standards or they can be mandated to fulfill the needs of future technologies.

But perhaps the biggest effect on cost effectiveness and faster real life deployment of these technologies could be achieved through more standardization. The IoT presents numerous benefits to consumers, and has the potential to change the ways that consumers interact with technology in fundamental ways.

In the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend.

As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy. The Commission staff will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the IoT to promote appropriate security and privacy protections.

A key takeaway is that success in the future of IoT will stem from providing an exceptional, easy-to-use customer experience with compelling benefits, no matter the industry or type of product. This can be achieved with a solid strategy, powerful technology, efficient change management and a cutting-edge digital presence.

While the IoT vision will take years to mature fully, the building blocks to begin this process are already in place. Key hardware and software are either available today or under development; stakeholders need to address security and privacy concerns, and collaborate to implement the open standards that will make the IoT safe, secure, reliable and interoperable, and allow the delivery of secured services as seamlessly as possible.

Acknowledgment

This paper is part of academic research on IoT made in partial fulfilment of the course of Masters in Computer Applications.

References

[1] www.sciencedirect.com
[2] http://www2.alcatel-lucent.com/techzine/internet-of-things-benefit-standardization/#sthash.wRVNtd3A.dpuf
[3] http://www.cio.com/article/2872574/it-industry/5-key-challenges-facing-the-industrial-internet-of-things.html?page=2
[4] http://whatis.techtarget.com/definition/Internet-of-Things-privacy-IoT-privacy
[5] http://www.internet-of-things-research.eu/documents.htm
[6] http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6766209&url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D6766209
[7] http://www.ieee.org/publications_standards/publications/authors/author_guide_interactive.pdf
[8] http://www.indjst.org/index.php/indjst/issue/view/4802
[9] http://www.nationaljournal.com/magazine/who-hacked-my-toaster-20150227
[10] http://www.cmswire.com/cms/internet-of-things/7-big-problems-with-the-internet-of-things-024571.php
[11] https://www.indusnet.co.in/buzz/2015/03/internet-things-inevitable-future-innovation-start-ups/
[12] http://www.informationweek.com/strategic-cio/it-strategy/internet-of-things-whats-holding-us-back/d/d-id/1235043
[13] Research Directions for the Internet of Things John A. Stankovic, *Life Fellow, IEEE*
[14] http://devops.com/features/internet-of-things-challenges-devops/
[15] The Internet of Things: Five Myths and Realities freescale.com
[16] **The Internet of Things: The Future of Consumer Adoption** ACQUITY GROUP'S 2014 INTERNET OF THINGS STUDY
[17] www.mdpi.com/journal/jsan
[18] GreenPeak White Paper ; Wireless Communication Standards for the Internet of Things www.greenpeak.com
[19] http://edition.cnn.com/2014/03/28/tech/innovation/smart-device-communication/
[20] http://readwrite.com/2013/06/14/whats-holding-up-the-internet-of-things