Internet of Things: Essential Technology, Application Domain, Privacy and Security Challenges

Rathnakar Achary, PhD
ACED
Alliance University

Jenith Shaileshbhai Lalseta
Department of IT,
ACED
Alliance University

ABSTRACT

Internet of Things (IoT) is an ecosystem of connected physical devices and objects that are accessible through Internet. When the devices can represent themselves digitally they can be monitored, administered and controlled remotely. The proliferation of these devices creates a smart environment to have a plethora of applications. There is no doubt about these tiny devices as a transformation force that can help the companies in improving their operational efficiency through IoT analytics, and company can deliver better results. This paper focuses specifically on the essential technologies and application domain of IoT and the open issues which are to be addressed before to drive IoT application for the global acceptance. The analysis result indicates that by 2020 the technology generates a massive amount of data and revenue. Its impact will be felt across the entire big data universe forcing companies to upgrade their current tools and process and technologies to evolve to accommodate this additional data volume.

Keywords

Machine-to-Machine, wireless sensor networks, RFID, Device-to-Device, Device-to-Server, Server-to-Server, Software defined storage, object storage, Data analytics, Big data.

1. INTRODUCTION

IoT refers to the use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical objects. In consumers domain this has the potential application in the field of energy efficiency, healthcare, security education and many other aspects of daily life. The corporate sector gain advantages to deliver solutions and improve the decision making. It also enables the improved productivity in manufacturing, retail, agriculture and other related sectors. Initially IoT was developed by using RFID technologies. Now along with this a set of new technologies such as Near Field Communication (NFC), Machine-to-Machine (M2M) and Vehicular-to-Vehicular communication (V2V) are also used to implement the modern concept of IoT.

The growth of cellular and mobile communication along with Information Technology already deliver connectivity to broad range of devices across the world. This enables the development of new applications and services. A network of this dimension interconnect most of the things including connected cars and buildings, smart meters and traffic control systems. With the prospect it intelligently connecting almost anything and any one. By the exponential growth in the connected world, it is expected that in the year 2020 the growth of mobile connection is set to rise to reach 10.5 billion and that for the connected devices across all access technologies could reach 25.6 billion. This is almost 150% more than that of mobile connection. As a result of this IoT

will open up new revenue stream, new business models, drive efficiencies and improve the way existing services across many different sectors. According to the study by Machina Research, the growth of IoT applications will add an additional revenue of US$4.5 Trillion per annum. One open opportunity that IoT clearly enables due to the large amount of data emerged from IoT objects are stored in cloud servers in the Internet, so that it is accessible easily by web based tools and applications. The new business models adopted will transpose and improving business process, as a result, reducing the time for decision making. Providing new possibilities IoT also generate new challenges such as security threat and expose vulnerabilities in the explored world of interconnected objects.

The main concerns of business organization about this upcoming technology were regarding deployment strategies, and its effect on business and consumers. In this paper we have primarily made an attempt to understand the business opportunities and business landscape of IoT and the key challenges. The international context of this research is adopted from the benchmarking of international organizations and standards agencies derived for both objectives.

The rest of this paper is organized as follows; in section 2 we present Impact of M2M. Section 3 we describe the IoT trends. Section 4 provides details of the different components used in IoT. Section 5 the IoT application areas. Section 6 the IoT growth, in section 7 we extend the impact of IoT to improve current business model. Section8 the IoT challenges. Finally conclusion are presented in section 9.

2. IMPACT OF M2M

Machine-to-Machine (M2M) is a sub-set of IoT, which uses wireless network technologies to connect devices to each other and to the Internet. Having the feature of autonomous and embedded intelligence, it can be used for wide range of Industrial applications and services. The evolution of M2M, the IoT represents the coordination of multiple vendors, devices and appliances connected to the Internet through multiple networks. In 2013 M2M connection accounted for 2.8% global mobile connection (195 million). Due to the rapidly developing market, the growth in M2M connection in different regions and the annual global growth between 2010 and 2013 is shown in the table 1, which indicates an annual growth of 55%.

The market share of different countries towards this technology are given in the figure 1. Among these countries the highest proportion of operators offering M2M services are in Europe, where about two-third of operators have an M2M offering. This compares just under half of operators in the Americas, Asia and Oceania. Market survey indicates that by 2020 the total number of connected devices in the world be increased form 9 billion today to 25.6 billion, out of this about 10.5 billion connections to a mobile network. The remaining

devices will use alternative communication technologies such as short range radio connections to a communication gateway, wide area network (WAN) radio, fixed line telecommunication or Wi Fi networks. Figure 2 represents the growth of M2M applications by 2022.

Table 1. M2M connection in different regions

Region	M2M Total connection (2013)	M2M CAGR (2010 – 2013)	Connections CAGR (2010 – 2013)
Africa	1.0%	41.3%	15.0%
Asia	2.1%	55.0%	10.4%
Europe	5.1%	28.6%	2.4%
Latin America	2.1%	43.7%	7.8%
North America	9.3%	22.5%	3.6%
Oceana	5.1%	25.8%	5.5%
Global	2.8%	37.6%	8.8%

Source: GSMA Intelligence: excluding computing devices in consumer electronics
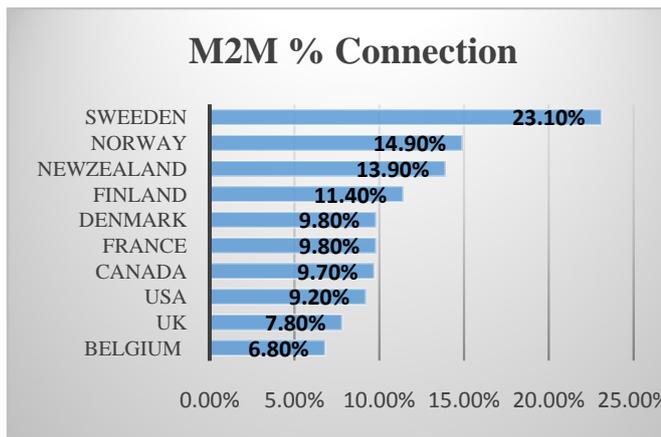
**Fig 1: M2M percentage connections**

3. IoT TRENDS

IoT has been identified as one of the emerging technologies imparting for the next few years. According to Gartner's IT Hype in 2012 IoT will benefit across different application development and services, which will benefit from cheap, small devices allowing that everything will have a radio and location capability. This is possible due to the notion of network convergence using IP. The use of common multi-user IP network supporting a wide range of applications and services. As the IoT evolves, these networks and many of this will be connected with added security, analytics and management capabilities and some of them will converge. This will explore the IoT horizon and even become powerful. This brings many business opportunities and add to the complexity of Information Technology. It enables the integration of IT, which refers to hardware and software used to store, retrieve and process data and communication technology. The convergence of information and communication technology is represented in three layers of

technology innovation as in figure 3, the cloud services, data and communication pipe/networks and devices.
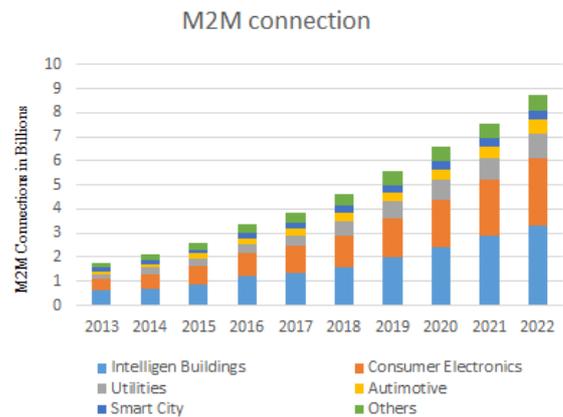
Source: Machina Research

Fig 2: M2M connection
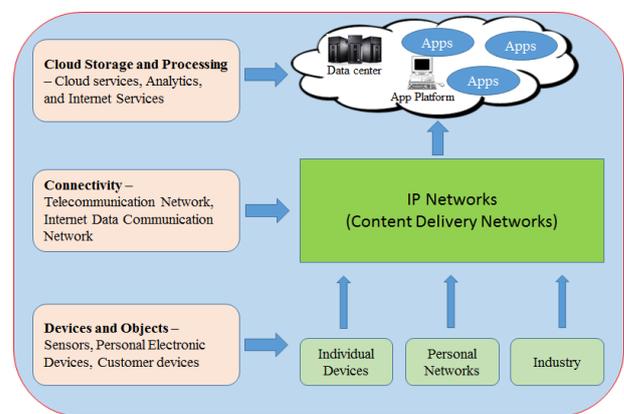
Fig 3: IoT in details

4. IoT COMPONENTS

In this section we discuss the different IoT component used under three categories as;

1. *Hardware* – made up of sensors, actuators and embedded communication hardware's.

2. *Middleware* – On-demand storage for data and computing tools for data analytics.

3. *Presentation* – Novel easy to understand virtualization and interpretation tools which can be designed for different applications.

4.1 Hardware
4.1.1 Radio Frequency Identification (RFID)
IoT requires some of the essential components to enable communication between the devices and objects. Objects need to be augmented with an auto-ID technology, typically an RFID. These RFID tags provide uniquely identifiable and allows the object to wirelessly communicate certain types of information's, which lead to another requirement the ability to monitor data. RFID tag and RFID recorders manages to gather real-time data, which is later processed and used by the managers for decision making. Both passive and active RFID tags are used to communicate the ID and signals to the RFID readers in different application.

4.1.2 Wireless Sensor Networks (WSN)

Wireless sensor networks are low power integrated circuit with wireless communications have made available efficient low cost, low power miniature devices for use in remote sensing applications. WSN also facilitate intelligent energy management. In WSN, two basic opportunities exist to harness the reliability and redundancy of the network resource, which mitigate the failure mechanism for likely problems enable systems to recover without data loss.

The first is the concept of spatial redundancy, where every wireless node has at least two other nodes with which it can communicate and routing scheme that allows data to be relayed to either node, but still reach the intended final destination. In a properly formed wireless sensor network every node can communicate with two or more adjacent nodes to provide higher reliability than a point-to-point network by automatically sending data on an alternate path if the first path is unavailable.

The second level of redundancy can be achieved by using multiple channels available in radio frequency (RF) spectrum. The concept of channel hopping involves pair of node that can change channel on every transmission, thereby averting temporary issues with a given channel in the ever-changing and punitive RF environment in Industrial applications. Within the IEEE 802.15.4, 2.4 GHz standard 15 spread-spectrum channels are available for hopping, affording channel hopping systems much more resilience than non-hopping systems. Data gathered by these sensor devices are shared with sensor nodes and sent to the cloud server for analysis.

4.2 IoT Communication protocols

IoT is a vision of connectivity at anything, at anytime and anywhere. It is considered as an extension of today's Internet to the real-world of physical objects. IoT applications has been used in many fields from the earliest wireless sensor networks such as the smart grid, smart healthcare, smart agriculture, military and so on. A combination of technologies including low-cost sensors, low power processor, scalable cloud computing and ubiquitous wireless connectivity, has enabled this revolution. Many applications using these technologies to enable intelligence and sensing capabilities in their products, thereby enabling objects to

sense, learn from and interact with their environment. IoT supports hundreds of protocols. It's important to understand the class of use that each of these important protocols addresses. A simple taxonomy of these protocols with their response time is give in figure 4.

The three categories indicated in the taxonomy are;

- Device to Device (D2D)
- Device to Server (D2S)
- Server to Server (S2S)

Device to Device (D2D) – the data collected from them are transferred to the server infrastructure by Device to Server (D2S). The server infrastructure then share the device data by Server to Server (S2S), possibly providing it back to devices, to analysis programs or to people. The protocols used under these categories are;

D2D → DDS (Data Distribution Service) – A fast bus for integrating intelligence machines

D2S → XMP (Extensible Message and Presentation Protocol) – A protocol for connecting devices to people, since people are connected to the server.

MQTT (Message Queue Telemetry Transport) – A protocol for collecting device data and communicating it to server.

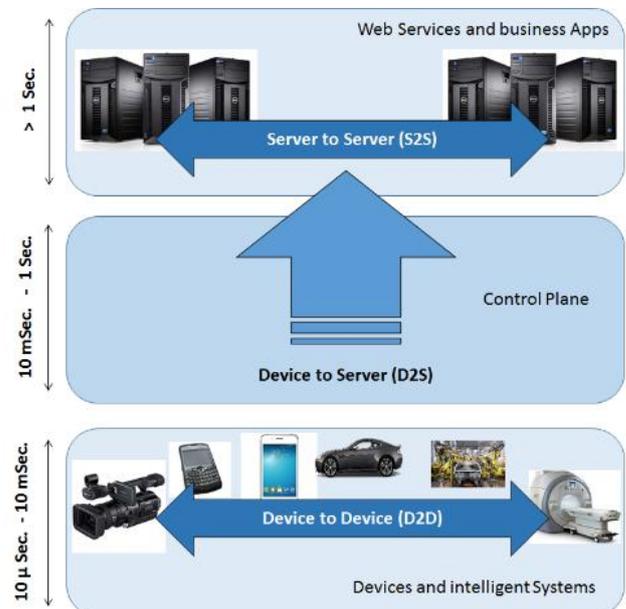S2S → AMQP (Advanced Message Queuing Protocol) – A queuing system designed to connect server to server

Fig 4: Three categories of IoT (D2D, D2S and S2S) with their response time

Depending on the types of applications, range, data requirements, security and power demands and battery life will dictates the choice of different protocols. Some of the popular protocols in use with IoT technologies are listed in the Table 2.

Table 2. IoT Protocols

Protocol	Standard	Frequency	Range	Data rate
Bluetooth	IEEE 802.15.1	2.4 GHz	100 meters	2.1 Mbit/s
ZigBee	IEEE 802.15.4	868 MHz (EU and Japan), 915 MHz (ISM, US) and 2.4 GHz(worldwide)	50 meters	20 kbit/s (868 MHz band) to 250 kbit/s (2.4 GHz band)
Z-Wave	2.4GHz ISM	908.42 MHz in the U.S. and Canada	100-meters	908.42 MHz in the U.S. and Canada
6LoWPAN	IEEE 802.15.4	868-868.6 MHz	20m	20 kbit/s
Thread	IEEE 802.15.4	2.4 GHz	100(theoretical)	250 kbps

Wi Fi	IEEE 802.11	2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz, and 5.9 GHz bands	32 meters	54 Mbit/s to 600 Mbit/s.
Cellular	EEE 802.16m (4G)	900MHz, 1800MHz and 1900MHz	0.80 km in cities 40 km in open area 8 km rural area	100–300(download) 50-75 (upload)
NFC	ISO/IEC 14443	13.56 MHz	< 20 cm	424 kbit/s
SigFox	ATA8520	in Europe the 868MHz band is widely used and in the US it is 915MHz.	Upto 10km urban, 50km rural	100bps
Neul	Weightless	ISM	Upto 10KM	10-100kbps
LoRaWAN	LoRaWAN	Varies, sub-GHz	2km -5km urban, 15km suburban, 45km rural	0.3-50kbps adaptive
WiMAX	IEEE 802.16	2-11 GHz	50 km	5 bps/Hz and peak up to 100 Mbps in a 20 MHz channel
LR-WPAN	IEEE 802.15.4	2.4 GHz	10-20 meters	250 kbps at 2.4 GHz, 40 kbps at 915 MHz, and 20 kbps at 868 MHz
CoAP	RFC 5741	2.4 to 2.4835 GHz (World Wide)	10 meters	250kbit/s
MQTT	ISO/IEC JTC1	up to 128 bytes in a 200 msec.	5 Meters	424Kbps
XMPP	RFC 6120	2.4GHz	Wide	250Kbps
DDS	M2M	up to 62.5 MHz	100 Meters	
AMQP	ISO and IEC 19464.	2.4 GHz	Wide	1,345,531 messages per second
HTTP	RFC 2616	2.4 GHz	Wide	500 bits per second to 32,000 bits per second

4.3 Data Storage

IoT is creating an enormous amount of data from different sources and devices. To manage and access this data based on the requirement, by authorized user's digital storage become a critical factor. A prediction estimate 20 billion devices will be connected to the Internet by 2020. These inputs are from a very large number of sensors and smart devices that communicate with each other and also communicate to the broader audience. However it may make more sense for local storage and processing of data minimize the long-term aggregated data in the cloud and to control the band-width requirements. The band-width requirements will be huge if the entire data storage and data analysis performed in the data centers. This problem can be eased by performing the initial analysis of the data at the local level and only send processed result to the cloud. The cloud also provide ways to preserver privacy if this is consumer data-privacy and security of that data especially, if the data is shared anonymously versus having precise metadata tags that tells the user who and when every piece of data is associated with, which would be available in the raw data.

Lot of IoT devices have built in solid state flash memory as storage units. Their use is in smaller IoT devices, because they are least expensive, faster enough for many of those applications and it relatively consume low power. Along with some of the newly developed solid state storage technologies are also plays key roles. Some of these technologies are;

- *3D Xpoint Technology from Intel Micron* – targeting more towards server application, but they have also indicated a possibility for gaming and other purposes as well. Cost wise this technology may be bit more expensive than flash, less expensive than DRAM for the identical speed.

- *MRAM* – Magnetic Random Access Memories – that could also be used for caching and buffering

and used like that. MRAM and STT-MRAM use very low power and is a very fast technology.

4.3.1 Software Defined Storage (SDS)

SDS is another option for data storage in data centers. This approach typically shift the features found in hardware layer and moving the to the software layer. The SDS approach for the data center architecture eliminates the dependency on server applications with software hard-wired into the system. This option provides the scalability and speed that the IoT demands. Using SDS also eliminates the potential for bottlenecks caused by vertical, single entry point architecture. Its horizontal architecture streamlines and redistributes data so that it is handled faster and more efficiently. This nonhierarchical construction can be scaled out easily and cost-effectively. In the figure 5 it is clear that by 2020 the traditional storage will be down to about $20 billion, whereas the software defined storage grows over $40 billion.
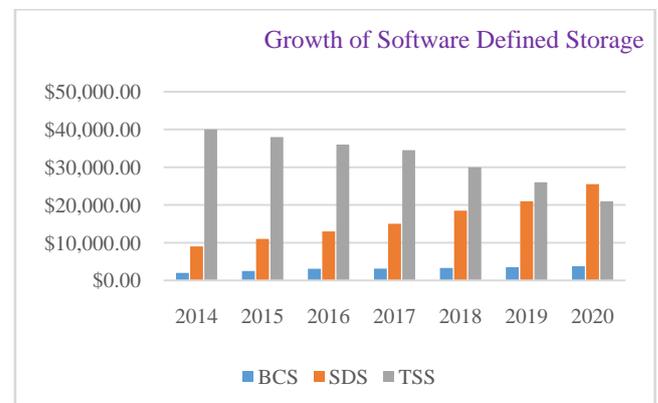
BCS – Basic Cloud Storage; SDS – Software Defined Storage; TSS – Traditional Storage System

Fig. 5 Software defined storage growth in IoT

4.3.2 Object storage

Object storage is the predominant cloud scale data storage method. In which organization deals with specific nature and rapid growth of IoT data. In object storage architecture the data are not stored in blocks, files or folders, but in flexible size containers called objects. The process of placing data items in object storage is quick and easy. Object storage is abundant for storing large volume of unstructured IoT data as its simple flat structure can scale elastically. Another important feature of object storage is that it also works well with big data analytics platforms like Hadoop.

4.4 IoT Data Analytics

The global rise of the internet in the recent years with interconnected networks and machine producing continuous data, is creating a new world of opportunity for enterprise organizations.

Fig 6: IoT data analytic

The potential of IoT is not just in the device and the networks, but also in the latest 'big data' analytics software. IoT data analytics enables organizations to analyze a mix of different varieties of data collected for connected devices, objects and from archives generates actionable insights for optimized performance and business growth. The enterprises analysis the IoT data and apply the result to provide smart products, innovative solutions and personalized customer experiences. These reports are generated by using few well established tools and services. There are nearly 47 (forty seven) analytical tools and services. The details obtained from these reports are useful to many organizations and individuals in the following manner;

1. Government organization and other NGOs that want to invest in updating their systems and services to optimize the performance and operational cost.

2. Large organization and enterprises that want to build an ecosystems of relevant and reliable IoT tools and service suppliers to establish IoT based systems. To increase efficiencies and leverage big data to drive revenue growth and innovation in new products and services.

3. Small and medium size organizations employs IoT data analytics and services to maximize their current capabilities, design new business models and gain insights from big data to support their business growth. The table 3 represents the 47 IoT data analytics products.
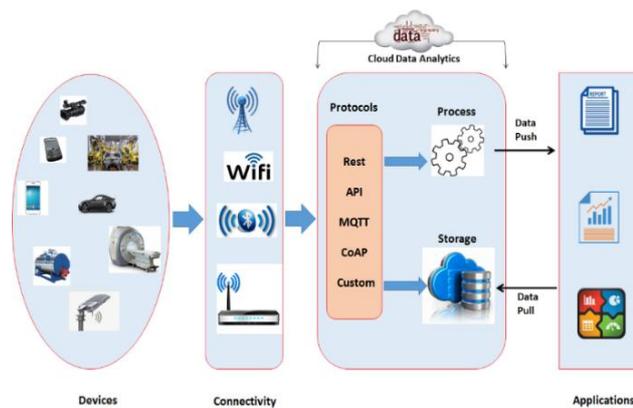
Emergence of data analytics tools and services between the years 2008 to 2016 is as shown in figure 7.

Table 3. The 47 IoT Data Analytics products

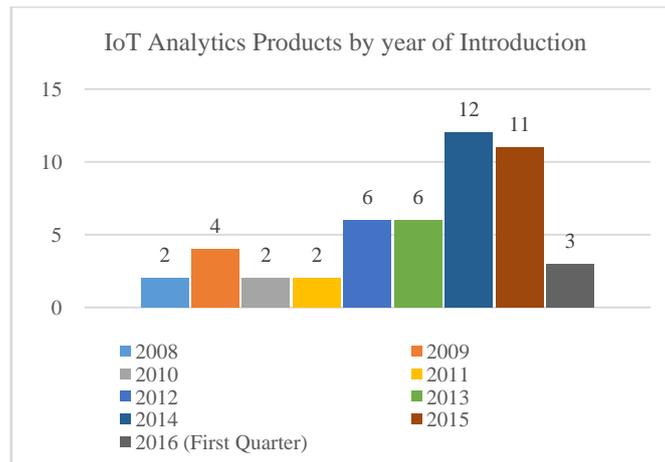|			
• Accenture Insights Platform	• Flakonry	• Mnubo SmartObjects Analytics	• Sight Machine
• Action Analytics Platform	• Glassbeam Analytics/Glassbeam Edge Analytics	• Mongo DB	• Space-Time Insight Suite
• AerVoyance IoT Analytics	• HPE Vertica Advanced Analytics Platform	• Oracle Internet of Things Cloud Service	• SpliceMachine
• AGT IoT Analytics	• IBM Waston IoT platform Analytics Real Time Insights	• Oracle Edge Analytics	• Splunk
• Angoss Analytics		• PLAT.ONE	• SQLstream Blaze
• Apama Streaming Analytics	• IBM streams	• Predixion RIOT	• Stemys.io
• Bit Stew MIxCore and MIN Director	• Quarks	• PTC IoT Solutions – ThingWorx Platform/Axeda Machine Cloud	• Tellient IoT Analytics
• Blue Yonder Platform	• Intel Internet of Things (IoT) Analytics		• TempoIQ
• Brigh Wolf Strandz IoT Platform	• Keen IO	• PTC IoT Solutions – KEPServerEX	• Teradata Listener and Teradata Aster Analytics
• Cisco ParStream	• Measurence	• RapidMiner	• Vitria IoT Analytics platform
• Datameer	• Microsoft Azure Stream Analytics	• SAP HANA Cloud platform for IoT	• Waylay
• DataStax		• Senswaves Sweave	• X15 Enterprise
• Datawatch			

Source: Ideya/Camrosh Market Report – May 2016

Fig 7: Emergence of data analytics tools and Services

The key features of these 47 IoT tools and services are compiled as in table 4.

Table 4. Product key features and factors impacting and selection process

Data source	Data preparation	Data process and storage	Data analysis	Data presentation	Other factors impacting selection process
• Data coverage • Data type	• Data quality • Data profiling • MDM • Data virtualization • Protocol for data collection	• Technology • Data warehousing/vertical scale • Horizontal data storage and scale • Data steam processing • Data latency • Cloud computing • Query platform	• Technology and methods • Intelligence deployment • Type of analytics	• Dash board • Visualizations • Reporting • Data alerts	• Scalability/flexibility • Vendor's years in business • Product user cases • Privacy • clients

5 IoT APPLICATIONS

There are several application areas of IoT, which will imparted by the emerging IoTs. Figure 8 depicts the IoT application in different segments. These application areas are classified as below:

1. ***Smart Home***: Smart home application is considered as the highest ranked application of IoT. A large number of IoT analytics companies data base are active in this, than any other applications.

2. ***Smart City***: Smart city spans a wide variety of use cases form traffic management to urban security and pollution monitoring. Many smart city projects includes IoT solutions for solving traffic congestion problem, reduce noise and pollution and helps to make cities safer.

3. ***Smart Grids***: A smart grid approach is to intelligently manage the supply and demand of electricity. It monitors the behaviors of electricity suppliers and consumers on a real-time basis. This improves the reliability, efficiency and economics of electricity.

4. ***Industrial Internet***: The Industrial Internet is one of the wide area of IoT applications with a highest overall potential.

5. ***Connected Cars***: Connected car application of IoT also impact on the smart city applications to manage the

traffic and congestion efficiently. Many leading auto manufacturing companies like BMW and Ford with the other technology giants like Google, Microsoft and Apple shows their presence in the connected car platform.

6. ***Health Care***: The health care sector and smart medical devices bears enormous potential using IoT.

7. ***Smart Retails***: IoT application in retail sectors as proximity based advertising and popularity ranking over few of the rich segments.

8. ***Smart Supply Chain***: Supply chain management becomes smarter by the adoption of IoT solutions. Consignment tracking, while they are on the move or gathering suppliers to exchange inventory information are some of the real-time IoT applications in smart supply chain.

9. ***Smart Farming***: Due to the remoteness of farming operations and the large number of livestock that could be monitored, the IoT could revolutionize the way farms work. Smart farming will become the important application filed in the predominantly agricultural product production countries.
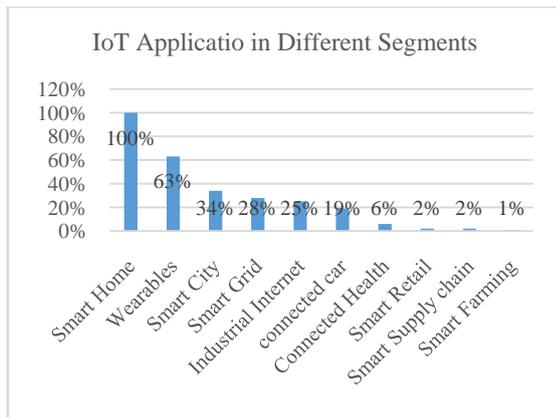
Fig 8: IoT application in different segments

6   IoT GROWTH (PROLIFERATION)

IoT has grater business potential in B2B than B2C applications. In fact in many instances such as website setting (mining, oil and gas and construction) there is no direct impact for consumers. The impact of IoT in B2B settings not only pointing to opportunity for technology suppliers, but also suggests how much IoT is likely to affect competition and requires new business models in B2B industries. Almost about two-third of the value created will be in B2B applications. B2B information involves the change of products, information or services between the organizations rather than between business and consumers. To analyze the potential impact of IoT on B2B vs B2C activities let us consider the application in three different ways.

- *By user*: As much as 69% of potential value of IoT is in use cases in which the primary users are B2B organizations.

- *By Buyers*: 79% of potential value occurs when a business in the purchaser of the IoT technology or service.

- *By setting owners*: By 2025 more than two-third of the potential value is essential for IoT applications, is generated in settings owned by businesses such as worksite, factories and offices as shown in figure 9.
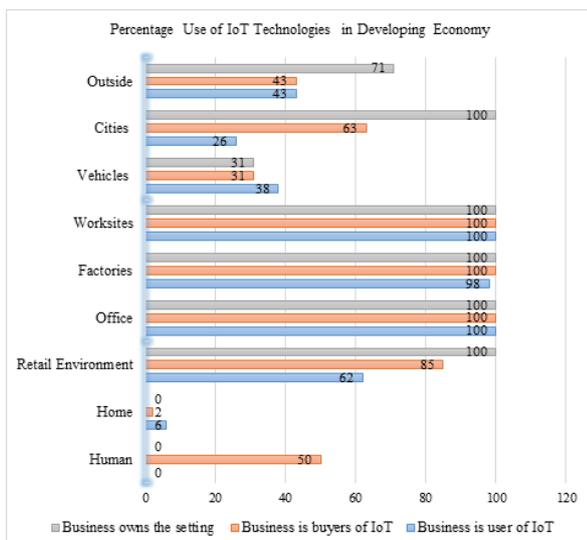

**Fig 9: Percentage Use of IoT Technologies in Developing Economy**

7.   IMPACT OF IoT TO IMPROVE CURRENT BUSINESS MODEL

The business and other organizations that IoT sequences are faced with a multitude of opportunities and may be just as many challenges. Depending on the industry IoT applications to adopt the companies even force to change their business models. The implication of IoT for Business is analyzed in three different ways;

1.   Using IoT to improve current business model.

2.   New business models enabled by IoT

3.   Organization issues related to IoT implementation

7.1 Using IoT to improve current business models

Companies have to analyze the opportunities to enable IoT in the business applications to improve performance to have an edge over their current operations. These opportunities are the extensions of the opportunities that have been identified with the use of big data and advanced analytics. IoT data and the analysis report will be useful to the companies to personalize the services based on customer's behavior, usage and context. To analyze the performance enhancement using IoT, consider some of the broad categories of applications. The results provides details about the potential impact on performance optimization of the different applications. We have considered 11 broad categories of applications which uses IoT technology. The annual revenue by 2025 is about $11.1 trillion. Its share with different categories is shown in figure 10.
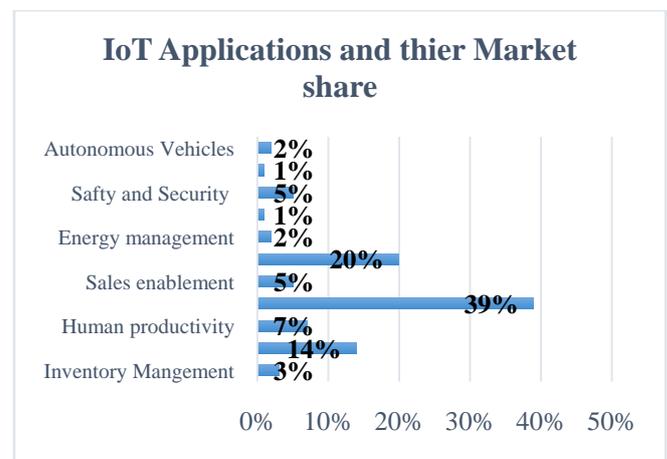
Source: McKinsey Global Institution Analysis

Fig 10: Economic Potential of IoT in 2025

7.2 New business model for companies that use IoT

Another advantage of IoT, in addition to gaining operating efficiency is to develop new business models. These business models are; new revenue model, service based business model and monetization of IoT data.

7.2.1   New Revenue Model

The massive data generated by IoT and the analysis results provides an insight into customer's behavior. This information is useful to the companies for customization, dynamic pricing models based on specific customer preferences, as well as the

usage context. This provide benefits for both companies and customers.

7.2.2 *Service Based Business Model*

IoT based business model enables the companies to shift from selling products to selling services based on their products. This model can transfer large capital expenditure into a pay-by-usage operating expense.

7.2.3 *Monetization of IoT Data*

The large volume of data generated by IoT applications can become an intangible asset to the organization. Data belongs to the organization could be another company's gold mine, and that value could be monetized by the originator of the data.

7.3 Organization Implication of IoT

For companies to make most of the IoT technology their organization must adopt data driven decision making capabilities and create environments in which relevant information is made available to the right decision makers in a timely manner. This is possible only by rigorous analytics. The organization analytics capabilities will bridge the gap between the data source and the decision makers and to apply insights from large real-time data stream in a timely manner.

8. IoT CHALLENGES

The IoT opens a completely new dimension to security, it is where the Internet meet the physical world. As the IoT continues to gain traction and major connected devices come to market, security become a major concern. Business are increasingly being breached by attackers via vulnerable web facing assets. A similar effect is to the consumers end also. The consumers IoT devices are targeted, since they are connected to the Internet. The design priority of the manufacturer is on the performance and effectiveness without focusing more on the security and privacy. The research conducted on different IoT devices and other domains. Data are gathered for analysis from different sources such as; user facing cloud services, back-end cloud services, mobile application interface, and device debugging interfaces. In most of the cases the devices exhibit vulnerabilities. This indicates that there is a need to perform security review of device architecture and accompanying applications to minimize the risk of users. In this paper we have summarized result of security analysis conducted on IoT devices.

To protect IoT from security breaches, it requires an integrated home cyber security approach. The solution must be shifting from device oriented security to a solution able to protect an unlimited number of objects by intercepting attacks at their core. The table 5 shows the security challenges and vulnerabilities on IoT devices.

Table 5. IoT Security Challenges

Authentication and Communication			
Cryptography Allowed (TLS/SSL)	**Cryptography Required**	**Password Protection**	**Certificate Validation**
This protect user data during transit, also lack of such mechanism allows the impostor to access the network and capture data.	Need of strong cryptography to reduce the chance of data loss.	Enforcing to user a complex password protection, which minimizes the effect if brute-force and dictionary attacks.	Improper validation of certificate results in man-in-the- middle attack.
Device-to-Service Authentication	**Encryption Employed**	**Man-in-the-Middle Attack**	**Relay Attack**
If the devices fails to authenticate themselves, during communication process, it could be vulnerable to impersonation from an attacker.	Unencrypted message communication may be passively monitor the traffic would gain access to all sensitive data sent by the device	Without proper protection an intruder may intercept the traffic and forward traffic between the devices and its service could receive and modify traffic sent in both directions.	Having in-adequate protection the intruder are able to ruse a previously captured data to perform the relay attack.

(Left side row labels: "User faced cloud servers" for first data row; "Back end Cloud Service" for second data row.)

9. CONCLUSION

In 2020 world of interconnected smart devices will be made up of 26 billion units according to Gartner. The IoT promises to deliver a step change in individual quality of life and company's productivity. These smart devices embedded with intelligence has the potential to enable extension and enhancement of essential services in transportation, logistics, security, utilities, education, health care and other areas, while providing a new ecosystem for application development. The IoT market has a distinct characteristics. A rigorous effort is required to move the industry beyond the early stage of market development towards maturity, driven by common understanding of the distinct nature of the opportunity.

IoT devices often have less memory and slower processor. So they may be unable to use the same security and encryption methods as a traditional computer does. These tiny devices connected in the network are vulnerable for many security threats. The analysis report indicates that, using a compatible cryptographic technique such as Elliptical Curve

Cryptography may be adopted to secure these devices before the consumers are at risk.

10. REFERENCES

[1]. L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Computer Networks 54 (2010) 2787–2805. Gartner's hype cycle special report for 2011, Gartner Inc., 2012.

[2]. S. Bainbridge, C. Steinberg, M. Furnas, GBROOS—an ocean observing system for the Great Barrier Reef, in: International Coral Reef Symposium, 2010, pp. 529–533.

[3]. Y. Bengio, Learning Deep Architectures for AI, first ed., Now Publishers Inc., 2009.

[4]. R. Caceres, A. Friday, Ubicomp systems at 20: progress, opportunities, and challenges, IEEE Pervasive Computing 11 (2012) 14–21.

[5]. A.T. Campbell, S.B. Eisenman, N.D. Lane, E. Miluzzo, R.A. Peterson, Peoplecentric urban sensing, ACM, 2006.

[6]. J. Gubbi, K. Krishnakumar, R. Buyya, M. Palaniswami, A cloud computing framework for data analytics in smart city applications, Technical Report No. CLOUDS-TR-2012-2A, Cloud Computing and Distributed Systems Laboratory, The University of Melbourne, 2012.

[7]. A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, T. Razafindralambo, A survey on facilities for experimental Internet of Things research, IEEE Communications Magazine 49 (2011) 58–67.

[8]. Hernández-Muñoz, J. Vercher, L. Muñoz, J. Galache, M. Presser, L. Gómez, J. Pettersson, Smart cities at the forefront of the future Internet, in: J. Domingue, A. Galis, A. Gavras, T. Zahariadis, D. Lambert (Eds.), TheFuture Internet, Springer-Verlag, Berlin, Heidelberg, 2011, pp. 447–462.

[9]. H. Jun-Wei, Y. Shouyi, L. Leibo, Z. Zhen, W. Shaojun, A crop monitoring system based on wireless sensor network, Procedia Environmental Sciences 11 (2011) 558–565.

[10]. X. Li, R.X. Lu, X.H. Liang, X.M. Shen, J.M. Chen, X.D. Lin, Smart community: an Internet of Things application, IEEE Communications Magazine 49 (2011) 68–75.

[11]. V. Mayer-Schönberger, Failing to forget the ''Drunken Pirate'', in: Delete: the Virtue of Forgetting in the Digital Age (New in Paper), first ed., Princeton University Press, 2011, pp. 3–15.

[12]. H.S. Ning, Z.O. Wang, Future Internet of Things architecture: like mankind neural system or social organization framework? IEEE Communications Letters 15 (2011) 461–463.

[13]. H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things—CERP IoT, 2010.

[14]. E. Vera, L. Mancera, S.D. Babacan, R. Molina, A.K. Katsaggelos, Bayesian compressive sensing of wavelet coefficients using multiscale Laplacian priors, in: Statistical Signal Processing, 2009, SSP'09, IEEE/SP 15th Workshop on., 2009, pp. 229–232.

[15]. M. Yun, B. Yuxin, Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, in: Advances in Energy Engineering, ICAEE, 2010, pp. 69–72.

[16]. M. Zhang, T. Yu, G.F. Zhai, Smart transport system based on ''The Internet of Things'', Applied Mechanics and Materials 48–49 (2011) 1073–1076.

[17]. M. Zorzi, A. Gluhak, S. Lange, A. Bassi, From today's Intranet of Things to a future Internet of Things: a wireless-and mobility-related view, IEEE Wireless Communications 17 (2010) 43–51.