International Journal of Research in Advent Technology, Vol.4, No.8, August 2016
E-ISSN: 2321-9637
Available online at www.ijrat.org

Internet of Things: Scope In

Muni Prabaharan[1]
Business Consultant (Chief Design Office) / Independent Researcher, Tech Mahindra
Email: mp.me89@gmail.com

Abstract - One of the key concepts emerging in today's market across the globe is Internet of Things (IoT). It aims to connect everything in our world under a common infrastructure. The actual core strength of IoT concept is the high influence it has to everyday life by creating new dimension to the world, like Internet. This paper deals with the concept of IoT Ecosystem, working principle, applications, different internet terms, acceleration, approaching, technology, hardware, software, architecture, challenges, business models, future directions, OS and platforms. This paper actually sets the boundary of IoT and assists the following objectives,

- For readers, this paper gives some insights about the IoT system at a broader level
- For researchers, it directs you the place where there are research potentials

Index Terms – Internet of Things, IoT, Applications, OS, Platform

1. INTRODUCTION

The Internet of Things is a concept where everyday objects can be equipped with identifying, sensing, networking and processing capabilities. *i.e., the objects are equipped with microcontroller sensor devices and various software application and suitable protocol stack enable them to talk to other objects.* It allows them to communicate with one another and with other devices and services over the Internet to accomplish some objective. This concept which is the outcome of merged field of computer science and electronics. In general, IoT can be described as a combination of Sensors, Connectivity, People and Processes. Especially with the help of sensors and devices, a close connection is established between things, humans, the cyber world and the physical world. IoT combines smart devices with smart services to create compound application. Objects become 'smart' by embedding technology such as sensors, software or internet connections. IoT delivers on demand real-time services and assists in saving time, resources and even manpower. The range of IoT components in complexity, from simple identification tags to complex machine-to-machine communication. Integration of device and sensor data with big data, analytics and other enterprise applications is a core concept behind the emerging IoT. [1, 2, 3, 7, 10, 11]

Networked traffic cameras, radio-frequency identification tagging of shipments in the supply chain location tracking devices to find our car keys, remote monitoring of temperature and activity in our homes are well-established examples. This IoT technology transforms agriculture, industry, energy production and distribution by increasing the availability of information along the value chain of production using networked sensors. It also promises to transform many aspects of the way we live. [9, 10]

Due to low cost, highly capable sensors and advances in wired, wireless communication technology and network protocols that permit us to better connect sensors to the Internet, so it makes large difference today. But the term IoT has been in use since the large scale adoption of RFID began a decade ago. This is why the potential for business transformation is immense. [2]

1.1. A new ecosystem

The advent of the IoT will create a plethora of innovative applications and services, which will enhance quality of life and reduce inequalities whilst providing new revenue opportunities for a host of enterprising businesses.

The development of the IoT will occur within a new ecosystem that will be driven by a number of key players. These players have to operate within a constantly evolving economic and legal system, which establishes a framework for their endeavors. Nevertheless, the human being should remain at the core of the overall vision, as his or her needs will be pivotal to future innovation in this area. Indeed, technology and markets cannot exist independently from the over-arching principles of a social and ethical system. The IoT will have a broad impact on many of the processes that characterize our daily lives, influencing our behavior and even our values. [4]

1.2. How IoT Works

Below figure illustrates basic principle.

SENSORS → NETWORKS → DATA → APPS

Figure 1: Basic Principle

Sensors can be relative humidity, temperature, barometric pressure, distance, irradiance and light color.

Many objects and devices need separate recognizable identity or address, thus enabling more categories of things to be connected to the Internet and to each other and be locatable.

The objects then become capable of sensing activity, collecting data, exchanging this & connection with other connected objects, devices, users, smartphones and remote information systems, via the Internet, mobile phone networks, Wi-Fi or Bluetooth.

At this stage, application platforms, device manufacturers or cloud-based data analytics providers to run analytics on the data collected, design automated responses or link up to other data sets and analyses. [11]

1.3. Applications of IoT in Different Industries

This concept provides immense opportunities which enable organizations in every industry to offer new services. [2, 9]

Utilities: Consumers connected to the smart network have seen significant cost and resource savings

Manufacturing: Reduced field support costs, lower breakdowns, improved operational efficiency, optimal scheduling of production lines, anomaly detection and emission detect, improved quality and lower energy cost

Healthcare: Lower cost of care, improved patient outcomes, real-time disease management, improved quality of life for patients; other personal IoT devices like wearable fitness and health monitoring devices and network enabled medical devices are transforming the way healthcare services are delivered; this technology promises to be beneficial for people with disabilities and the elderly, enabling improved levels of independence and quality of life at a reasonable cost

Insurance: Creation of newer insurance models such as dynamic premium pricing based on condition of property and premium pricing based on usage

Consumer goods & retail: Creation of novel value-added applications for the customer, like alerts on expiry dates, avatars to check products virtually, targeted advertising

Transportation: Improved service levels, lower costs and lower carbon footprint; IoT systems like networked vehicles, intelligent traffic systems and sensors embedded in roads and bridges move us closer to the idea of "smart cities", which help minimize congestion and energy consumption

Consumer appliance: New IoT products like Internet-enabled appliances, home automation components and energy management devices are moving us toward a vision of the "smart home", which offers more security and energy efficiency

1.4. Differences

Table 1. ToI, M2M & IoE

Terms	Descriptions [6, 7, 8]
Internet for Things or Things on Internet (ToI)	The trend is to stop hosting websites on dedicated Web servers; Instead put them on more flexible and scalable cloud-computing clusters; Such techniques are custom-made and require a lot of development and maintenance; Because these services only provide connectivity for things, the overall approach is called the Internet for Things or Things on Internet (ToI). But in IoT, devices talk directly to each other, make joint decisions and exchange data between devices without the need for the cloud or servers.
Machine to Machine (M2M)	M2M solutions typically rely on point-to-point communications using embedded hardware modules and either cellular or wired networks. But IoT solutions rely on IP-based networks to interface device data to a cloud or middleware platform.
Internet of Everything (IoE)	IoE (four pillars: people, process, data, and things) builds on top of IoT (one pillar: things); In addition, IoE further advances the power of the Internet to improve business and industry outcomes, and ultimately make people's lives better by adding to the progress of IoT.

1.5. Acceleration of IoT (especially in the last few years)

A combination of factors has made it feasible both in terms of economical and technical to connect more and more devices and systems to a much wider, open network, giving rise to a rapid growth in IoT technology over the last five to seven years [11]:

- Wi-Fi and broadband connectivity are now much more widely available; More things and computers can come online due the emergence of

the IPv6 protocol22; Growing usage is 40% of the world's population; 'The cloud' or decentralised storage capacity is growing rapidly and at a much lower cost than previous hardrive solutions
- Sensor technology has become more sophisticated, requires less space, less power at lower costs, making it cheap enough to deploy in almost any location or to be pre-installed into devices; Attainability of larger sensors or displays due to the improvement of battery technology at all the time
- Data handling technology makes is able to absorb process and analyse the massive amounts of sensor-generated data at affordable cost; Costs for mobile devices, bandwidth and data processing have declined as much as 97% over the last ten years; Investment confidence – after years of anticipation, these converging conditions have led to a growth in investment in the IoT sector

2. APPROACHING IoT (also Navigating)

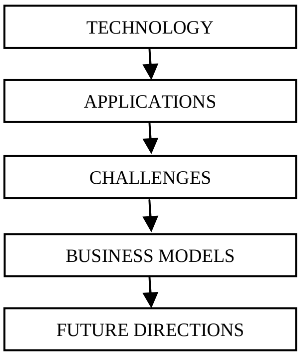

Figure 2: Approaching IoT

2.1. Technology

IoT Technology: It is classified into Hardware, Software and Architecture.
- Hardware: RFID, NFC, Sensor Networks, Actuators
- Software: Middleware, Search/Browsing, Data Processing
- Architecture: Hardware / Network Architectures, Software Architectures, Process Architectures, General

Following three steps to be consider.

Step 1: In order to connect everyday objects and devices to large databases and networks and indeed to the internet, the item identification is crucial; then only data about things be collected and processed; Radio-frequency identification (RFID) offers this functionality.
Step 2: Data collection will benefit from the ability to detect changes in the physical status of things, using sensor technologies; embedded intelligence in the things themselves can further enhance the power of the network by devolving information processing capabilities to the edges of the network.
Step 3: Advances in miniaturization and nanotechnology mean that smaller and smaller things will have the ability to interact and connect.

A combination of all of these developments will create an IoT. It connects the world's objects in both a sensory and an intelligent manner. [4]

2.1.1. Hardware

A) RFID

RFID is an important enabling and short range communication technology for the IoT. It is used mainly for tracking and tracing objects. It provides the ability to link all manner of inanimate objects from our daily life. A RFID tag communicates with an RFID reader via radio-frequency electromagnetic fields. Tags may contain different forms of data, but the data form most commonly used for IoT applications is the Electronic Product Code, or EPC. An EPC is a universally unique identifier for an object. These unique identifiers ensure that objects tracked with RFID tags have individual identities in the IoT. [3, 10]

B) NFC

NFC is evolved from RFID, a short-range communication standard and low-power wireless way to transfer small amounts of data between devices. The devices are able to engage in radio communication with one another when touched together or brought into close proximity to one another. Each NFC tag contains a Unique Identification (UID) that is associated with the tag. The NFC technology is frequently integrated into smart phones which are able to exchange data with one another when brought together. NFC devices are also able to make connections with passive, unpowered NFC tags that are attached to objects. [3, 10]

C) Sensor Networks

Sensors are devices that monitor characteristics of the environment or other objects such as temperature, humidity, movement and quantity. When multiple sensors are used together and interact, they are referred to as a wireless sensor network (WSN). It contains the sensors themselves and may also contain gateways that collect data from the sensors and pass it on to a server. Wireless sensors are different from RFID technologies in that they measure features of our physical environment, such as pressure, heat and humidity.

While sensors "sense" the state of an environment or object, actuators perform actions to affect the environment or object in some way. Actuators can affect the environment by emitting sound, light, radio waves or even smells. These capabilities are one way that IoT objects can communicate with people. Actuators are frequently used in combination with sensors to produce sensor-actuator networks. Thus, the combination of sensors and actuators can enable objects to simultaneously be aware of their environment and interact with people, both goals of the IoT. [3, 10]

D) Actuators

It converts information or energy from sensors into action by transmitting it to another power mechanism or system, such as heating or cooling a room. No human intervention need be involved in the decision-making process. [10]

2.1.2. Software

While the IoT may rely upon the existing hardware infrastructure to a large extent, new software must be written to support the interoperability between numerous heterogeneous devices and searching the data generated by them.

A) Middleware

The IoT will include vast numbers of heterogeneous devices generating enormous quantities of variable data. The IoT middleware sits between the IoT hardware and data and the applications that developers create to exploit the IoT. Thus, IoT middleware helps bring together a multitude of devices and data in a way that enables developers to create and deploy new IoT services without having to write different code for each kind of device or data format. *i.e., IoT middleware is software that serves as an interface between components of the IoT, making communication possible among elements that would not otherwise be capable.* Middleware connects different, often complex and already existing programs that were not originally designed to be connected. The essence of the IoT is making it possible for just about anything (any Thing) to be connected and to communicate data over a network. Middleware is part of the architecture enabling connectivity for huge numbers of diverse Things by providing a connectivity layer for sensors and also for the application layers that provide services that ensure effective communications among software. More comprehensive IoT platforms include middleware along with sensors and networking components. [3, 12]

B) Searching/Browsing

IoT browser should be capable of identifying smart objects, discovering their services and interacting with those objects. IoT search engine should capable of searching the rapidly changing information generated by IoT-enabled objects. Because the current browsers and search engines are designed to display and index relatively stable web content. However, objects in the IoT will be mobile, dynamic and will generate massive amounts of frequently changing information. Hence, there is a need for new IoT browser. [3]

C) Data Processing

Data processing in the IoT can take place in a variety of ways ranging from locally, on the device itself, to remotely, with information being sent for processing to centralized servers elsewhere. When machines communicate directly with other machines, a device collects information by means of a sensor. The sensor then uses a radio transmitter to send the data over a network. The network can be either wired or wireless. Wireless networks can be cellular, satellite, Wi-Fi for wide range communication, or Bluetooth, ZigBee and RFID for short range communication. Once the data arrives at its destination, it can be analyzed and acted upon by either another device or a human being. [10]

2.1.3. Architecture

Architectures are needed to represent, organize and structure the IoT in a way that enables it to function effectively. In particular, the distributed, heterogeneous nature of the IoT requires the application of hardware/network, software and process architectures capable of supporting these devices, their services and the work flows they will affect.

In general, there is no agreement on a single architecture that best fits the IoT. A number of articles proposed various conceptual architecture designs, while others proposed criteria for the assessment of proposed architectures as well as a conceptual architecture to meet the requirements of smart objects. [3]

A) Hardware / Network Architecture

A number of hardware / network architectures have been proposed to support the distributed computing environments required by the IoT. These architectures include peer-to-peer, EPCglobal and autonomic. The varying architectures that may be used to support the IoT also highlight the importance of the issue of standardization.

B) Software Architecture

Software architectures are necessary to provide access to and enable the sharing of services offered by IoT devices. In particular, service oriented architectures (SOA) and the representational state transfer (REST) model are frequently proposed for IoT use due to their focus on services and flexibility.

C) Process Architecture

The IoT will certainly affect business processes. Process architectures are necessary to effectively structure the business processes that will incorporate the IoT. In particular, researchers have looked at how to structure workflows to support the pervasive computing environments.

2.2. Applications

The domain of the application areas for the IoT is limited only by imagination at this point. Applications of IoT in different industries are already mention in the above section 1.3.

2.3. Challenges

The challenges facing the emergence of the IoT are numerous. They are technical, social and practical. These challenges must be overcome in order to ensure IoT adoption and diffusion. [2, 3, 16, 17]

A) Security

Security is an essential pillar of the Internet. IoT devices are typically wireless and may be located in public places. Wireless communication in today's Internet is typically made more secure through encryption. Encryption is also seen as key to ensuring information security in the IoT. To enable encryption on the IoT, algorithms need to be made more efficient and less energy consuming and efficient key distribution schemes are needed. Increasing the number of connected devices increases the opportunity to exploit security vulnerabilities, as do poorly designed devices, which can expose user data to theft by leaving data streams inadequately protected and in some cases people's (implanted, Internet-enabled medical devices and hackable cars) can be put at risk.

Many IoT deployments will also consist of collections of identical or near identical devices. This homogeneity magnifies the potential impact of any single security vulnerability by the sheer number of devices that all have the same characteristics. To deal with these and many other unique challenges, a collaborative approach to security will be needed. For many users, they will ultimately need to consider the cost vs. security trade-offs associated with mass-scale deployment of IoT devices.

B) Privacy

As more and more objects become traceable through IoT, threats to personal privacy become more serious. In addition to securing data to make sure that it doesn't fall into the wrong hands, issues of data ownership need to be addressed in order to ensure that users feel comfortable participating in the IoT. The IoT creates unique challenges to privacy, many that go beyond the data privacy issues that currently exist. Much of this stems from integrating devices into our environments without us consciously using them.

This is becoming more prevalent in consumer devices, such as tracking devices for phones and cars as well as smart televisions. In terms of the latter, voice recognition or vision features are being integrated that can continuously listen to conversations or watch for activity and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. The collection of this information exposes legal and regulatory challenges facing data protection and privacy law.

In addition, many IoT scenarios involve device deployments and data collection activities with multinational or global scope that cross social and cultural boundaries.

C) Legal / Accountability

The IoT will create new legal challenges that must be addressed. In particular, governance of a global resource like the IoT should not be dictated by a single group. Rather, a broad-based stakeholder approach to governance is necessary. Thus, a shared governance structure for the IoT that includes all relevant stakeholders is needed. In addition to establishing governance, global accountability and enforcement are necessary. Accountability tends to improve the effectiveness of governance through the threat of sanctions.

Like privacy, there are a wide range of regulatory and legal questions surrounding the IoT, which need thoughtful consideration.

Legal issues with IoT devices include cross-border data flow; conflict between law enforcement surveillance and civil rights; data retention and destruction policies; and legal liability for unintended uses, security breaches or privacy lapses. Further, technology is advancing much more rapidly than the associated policy and regulatory environments.

Regulatory analysis of IoT devices is increasingly being viewed from a general, technology-neutral perspective legal lens, which seeks to prevent unfair or deceptive practices against consumers.

D) Standards

Lack of standards and documented best practices have a greater impact than just limiting the potential of IoT devices. Without standards to guide manufacturers, developers sometimes design products that operate in disruptive ways on the Internet without much regard to their impact. If poorly designed and configured, such devices can have negative consequences for the networking resources they connect to and the broader Internet.

A lot of this comes down to cost constraints and the need to develop a product for release quicker than competitors.

Add to this the difficulties with managing and configuring larger numbers of IoT devices, the need for thoughtful design and standardization of configuration tools, methods, and interfaces, coupled with the adoption of IPv6, will be essential in the future.

E) IoT Strategy

Many of these large companies haven't yet defined their roles in the IoT. From the big companies that currently supply a significant amount of network hardware to the world, to cellular operators; these big players will invest a lot of time and money toward finding their niches in the IoT market. It will be important for these companies to understand what customers want out of IoT - the companies that fail to do this will have to either revisit their strategies or risk getting left behind.

F) Startup Challenges

There are tons of startups in the IoT space. There has been a lot of hype in the market in the last few years. The current investment climate has made raising capital fairly easy for many companies. These startups will really need to start showing their value. Some acquisitions from bigger companies are trying to push their way into the IoT space. Probably some companies disappear if they can't figure out how to take the next steps for growth.

G) Device management

The number of sensors, gateways and devices will be extremely large and they are going to be spread over large geographical areas - often in remote, inaccessible and/or private locations. Ensuring that devices are completely automated and remotely manageable is a challenge.

H) Device diversity and interoperability

The generation, transmission and distribution functions in a complex network require different types of sensor devices from different vendors, which are sensor enabled and need to be monitored continuously in real time. As many vendors do not support any standards in their products, there are sure to be interoperability issues.

I) Integration of data from multiple sources

When deploy an IoT application, streams of data from different sources such as sensors, contextual data from mobile device information, social network feeds and other web resources. It is important to note that the semantics of the data must be part of the data itself and not locked up within the application logic in different application silos.

J) Scale, data volume and performance

Prepare the business to manage the scale, data volume, and velocity of IoT applications. As the number of users and devices scale, so will the amount of data that needs to be ingested, stored and analyzed. Then, Big Data problem, standard architectures and platforms may be inadequate. Also, where stringent real-time performance is required, network and application level latencies may be a problem.

K) Flexibility and evolution of applications

Sensors and devices are evolving with new and improved capabilities. This will result in creation of new analytics techniques, algorithms, new use cases and business models. Then, apps will need to quickly develop with minimal effort. Need ecosystems and platforms that enable and sustain this.

L) Data privacy

A good bit of data collected from devices will be sensitive personal data that must be protected from unauthorized access and used only for the specific purpose for which the user has allowed that data to be collected. Users have to be provided with necessary tools that enable them to define the policies for sharing their personal data with authorized persons and applications.

M) Stakeholders

Another challenge, though not a technological one, is that we will have to work with a number of stakeholders. IoT works in a complex ecosystem and an end-to-end IoT application touches several technologies, engineering activities and other entities. Our maturity as a collaborative player becomes significant, as we need to work with different types of entities and organizations such as silicon chipset vendors, embedded boards and device vendors, IoT platform providers, communication service providers, system integrators, app developers, industry alliances as well as niche technology companies and start-ups.

N) Standardization

Many connected product developers have to move to different platforms due to 2G cellular is phased out across the globe. This can be very labor intensive at times and cost prohibitive. This issue has caused some major traditional cell carriers and infrastructure providers to begin fighting over the establishment of an IoT standard. LTE-M and LTE-NB have emerged as potential candidates.

2.4. Business Models

Changes in technology clearly require changes in business models. The IoT will certainly drive the development of new business models that capitalize on its pervasiveness and ubiquity. [3]

The value chain is perhaps the most important part of the business model. It defines how the service is delivered. IoT has a very complex value chain due to the fact it impacts a large number of processes. The large opportunity also means multiple stakeholders who would need to work together to deliver on the promise of IoT.

There are five key groups of players, viz., device providers, operators, platform providers, systems integrators and application providers. Each of this group would have various companies depending on the target industry. Each of the players brings unique strength to further the IoT but not everyone is on an equal footing.

2.5. Future Directions

Since the IoT has not yet been realized, it might seem precocious to forecast the future directions of the IoT. However, future visions of the IoT will affect its current development and must therefore be considered. Future vision that involves integrating even more devices into the IoT is the Internet of Nano-Things. [3]

2.5.1. Market Opportunities

The technologies of the IoT offer immense potential to consumers, manufacturers and firms. However, for these ground-breaking innovations to grow from idea to specific product or application for the mass market, a difficult process of commercialization is required, involving a wide array of players including standard development organizations, national research centres, service providers, network operators and lead users.

Changing business strategies is the name of the game, in particular in the retail, automotive and telecommunication industries. Firms are embracing the underlying technologies of the IoT to optimize their internal processes, expand their traditional markets and diversify into new businesses. [4]

2.5.2. Why Companies have been slow in adopting IoT

The IoT creates significant technical challenges:

- Existing IT Infrastructure is not suited to manage rapidly growing volumes of Sensor Data
- Organization\s lack real-time data analytics technologies critical to drawing insights from IoT
- The IoT magnifies data security and privacy challenges

Any bold new idea that promises to transform the way organizations operate is bound to come with as many potential challenges and risks as opportunities and benefits. The impact of IoT on a company’s business operations goes far beyond previous technology innovations. Unlike past shifts in computing that primarily affected the way software and systems were deployed to support internal business functions, IoT calls on every department within an organization to rethink how they design, develop, sell, support products and services being delivered to their customers. This raises a myriad of technical, operational and ethical questions about security, privacy, data governance, monetization and other critical issues. [5, 14]

2.5.3. Organizations Need New Skill Sets across a Range of Functions:

- Organizations lack capabilities in Developing and Marketing IoT Services
- Sales Force is not equipped to sell IoT Services
- IoT places new demands on Customer Support Capabilities

The IoT is in the midst of an explosion, as more connected devices proliferate. But there's not enough talent with the right skills to manage and execute on IoT projects. In fact, insufficient staffing and lack of expertise is the top-cited barrier for organizations currently looking to implement and benefit from IoT.

Tech companies around the globe are getting organized and creating IoT strategies, but where they're struggling is they don't have the processes and talent in-house to make these things happen.

Emphasizing the lack of needed skills within organizations, one third of IT projects require external support from vendors and other third party resources. This only lends to business low confidence in their ability to properly and effectively adopt the IoT. Without the right talent, taking on a project as big as IoT adoption can be daunting at best. [5, 15]

3. OVERVIEW OF OPERATING SYSTEM FOR IoT

IoT includes wide range of machines from sensors powered by microcontrollers to other devices and sensors powered by processors which has similar capability as we have those in smart phones. As more and more devices are getting connected to IoT the need for operating services are also increasing. The traditional operating system and OS for sensor network cannot fulfill diverse requirement of the devices connected to IoT. The devices in IoT need to be up and connected to network and other devices all the time in order to transmit and receive real-time data. For such a Real-Time Operating System is required which can manage low energy devices which can run continuously for a year or more on AA battery or other low powered sources. Currently many operating systems for IoT are in use which supports many devices. [1]

Table 2. Types of IoT OS (to mention few)

OS	Descriptions
Contiki	It is an open source operating system, connects tiny low-cost, low-power microcontrollers to the Internet. It provides fast and easy development. It supports wide range of platform and can be easily ported to new platform.
mbed OS	It is especially designed to run in low cost energy environment. The OS provides connectivity, security and device management functionalities required by IoT devices.
TinyOS	It is for low-power wireless devices, such as those used in sensor networks, ubiquitous computing, personal area networks, smart buildings and smart meters.
µC/OS (MicroC/OS)	It is the real-time operating system for the embedded devices used in IoT. It supports wide range of microcontroller devices and designed for low energy devices.
RIOT	It is designed for energy efficiency and supports hardware independent development. RIOT is the only OS that provides a high degree of modularity for IoT devices. This OS also have built in multithreaded support which manage devices resources more efficiently.
Brillo	It is based on the lower levels of Android which can run on minimal system requirements. It offers a protocol for synchronizing data between devices called Weave. With weave a Brillo device can talk to each other and cloud and also able to identify other devices such as android phone on the Internet.

4. PLATFORM FOR IoT

Collecting data from sensor devices and sending it to cloud server for processing and store it for future use is one of the major task of the IoT system. For this purpose a cloud server must be loaded with services which communicate with such devices and offer data management, application development and other data related services. Following are some of the platform which enable user to build such services. [1]

Table 3. Types of IoT Platforms (to mention few)

Platforms	Descriptions
Xively	It enables users to connect their devices to IoT and help manage connected things. It offers secure, scalable and reliable connectivity. It also helps in building business applications and data processing services.
Kaa	Kaa servers provide data management, integration, visualization and many other data related services. Kaa Data Processing services helps in collecting data from the connected devices which is one of the crucial task in the IoT world.
IBM Bluemix	It enables users to deploy and manage hybrid applications which can be on public, personal and local Bluemix instances. It helps users to integrate application and system running elsewhere via secure environment and share and synchronize data and to create and expose enterprise APIs.
Carriots	It allows user to collect data from various devices, store it and build power applications using SDK engine and deploy and scale services to variety of devices.
Nimbits	It allows users to store sensor data on

	cloud. Nimbits Server enables users to record, store and process data from IoT sensor devices and defines and executes business rules. It enables user to control, manage and monitor IoT devices from cloud.

5. CONCLUSION

Future will be many more connected objects per person. Although IoT technology is in initial stage but it will transform future and the way we live soon. So, it is a technology for future. Just like smart phones have made a big change in the way we communicate and deliver information with the help of large number of application available. Since IoT offers vast area of research in many fields, so this paper will help researchers to understand the boundary of IoT and to identify potential research areas. Like internet has transformed businesses and lifestyles in the last twenty years, IoT will disrupt our organization's relationship with its stakeholders. IoT can help us to innovate new processes and initiatives to increase our organization's business performance and create customer delight with new products and services.

REFERENCES

[1] Timothy Malche, Priti Maheshwary, "Harnessing the Internet of Things (IoT): A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Aug 2015, Vol.5, Issue 8
[2] Prateep Misra, Arpan Pal, Balamuralidhar P, "Unlocking the Value of the Internet of Things (IoT) - A Platform Approach", White Paper
[3] Andrew Whitmore, Anurag Agarwal, Li Da Xu, "The Internet of Things - A survey of topics and trends", Information Systems Frontiers, April 2015, Volume 17, Issue 2, pp 261-274
[4] "The Internet of Things - Executive Summary", International Telecommunication Urban, ITU Internet Reports 2005
[5] Karthik Vutukuru, Ramachandra Mannava, Sai Akshith Bhagavatula, Xerxes Patel, "IoT Presentation", Logan Data
[6] Chris Muench, "What's the Difference Between the Internet of Things and the Internet for Things?", Machine Design, July 22, 2014
[7] Chantal Polsonetti, "Know the Difference Between IoT and M2M", Automation World, July 15, 2014
[8] Dave Evans, "What is the difference between IoE and the Internet of Things (IoT)", Cisco Blogs, Digital Transformation, Mar 18, 2013
[9] The Internet of Things: An Overview, Understanding the Issues & Challenges of a More Connected World, Internet Society, Oct 2015
[10] The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments, Policy & Research Group, Canada, Feb 2016
[11] The Internet of Things and challenges for consumer protection, Consumers International, April 2016
[12] IoT middleware (Internet of Things middleware), IoT Agenda
[13] Internet of Things - Business Model, Telecom Circle
[14] IoT Adoption Has Been Slower Than Expected - Here's Why, Dataversity
[15] Business leaders lack confidence in IoT technology, CIO from IDG
[16] 5 Challenges of the Internet of Things, APNIC, Oct 2015
[17] Critical Internet of Things Challenges You'll See in 2016, Link Labs, Nov 2015

AUTHOR'S BIOGRAPHY

Muni Prabaharan is currently associated with Tech Mahindra, Business Excellence as Business Consultant (Chief Design Office Practice). He has over 6+ years' dominant experience in New Product Design, Value Engineering, Lean Six Sigma and Connected Engineering. His primary consulting areas are Internet of Things / Digital / Connected Engineering, Strategy Consulting, Value Engineering and Time to Market. He is certified professional of Six Sigma Black Belt, Associate Value Specialist Process, Lean Design, Management Knowledge and Certified Manager of Quality / Organizational Excellence. He has 10 Organizational level honors in his credits.

He has been written around 100 scientific papers and 2 books at International levels. Holding as Panelist, Keynote / Guest Speaker, Associate Editor, Technical Reviewer and Editorial Board Member of several International Journals and Conferences. He has 15+ International honors in his credits. Offered as Honorary Doctorate from UK based community.

He holds BE in Mechanical Engineering as Gold Medalist from Sri Ramakrishna Engineering College, Anna University, Coimbatore.