International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 5 Issue 6, June 2018

ISSN: 2394-4404

An Introduction To Internet Of Things – IOT

Ms. S. Sangeetha
Assistant Professor / MBA, Hindusthan Institute of Technology, Cbe

Ms. Queen Shanthana Mary
Research Scholar, Bharathiyar University, Cbe

Abstract: ***The Internet of Things (IoT) is an organization of interconnected computing devices, mechanical and digital machines, objects, animals or people that are provided with exclusive identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. In this paper we briefly discussed about what IOT is, how IOT integrates different technologies, its components, Internet of energy, applications & scenarios, and what are the applications for industry and challenges faced by Iot in applications to Industry.***

I. INTRODUCTION - INTERNET OF THINGS (IOT)

IoT *is short for Internet of Things.* A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.

The Internet of Things refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.

The Internet of Things extends internet connectivity beyond traditional devices like desktop and laptop computers, smartphones and tablets to a diverse range of devices and everyday things that utilize embedded technology to communicate and interact with the external environment, all via the Internet. Examples of objects that can fall into the scope of Internet of Things include connected security systems, thermostats, cars, electronic appliances, lights in household and commercial environments, alarm clocks, speaker systems, vending machines and more.

II. INTERNET OF THINGS (IOT) – DEFINITION

Internet of Things (IoT) is a concept and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services and reach common goals.

The research and development challenges to create a smart world are enormous. A world where the real, digital and the virtual are converging to create smart environments that make energy, transport, cities and many other areas more intelligent. The goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service.

Internet of Things is a new revolution of the Internet. Objects make themselves recognizable and they obtain intelligence by making or enabling context related decisions thanks to the fact that they can communicate information about themselves. They can access information that has been aggregated by other things, or they can be components of complex services. This transformation is concomitant with the emergence of cloud computing capabilities and the transition of the Internet towards IPv6 with an almost unlimited addressing capacity.

New types of applications can involve the electric vehicle and the smart house, in which appliances and services that provide notifications, security, energy-saving, automation, telecommunication, computers and entertainment are integrated into a single ecosystem with a shared user interface. Obviously, not everything will be in place straight away.

The IERC (European Research Cluster on the Internet of Things) definition: states that *Internet of things (IoT)* is "*A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual)*

things based on existing and evolving interoperable information and communication technologies".

The IERC (European Research Cluster on the Internet of Things) definition states that IoT is "*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.*"

III. INTERNET OF THINGS – INTEGRATION

The Internet of Things makes use of synergies that are generated by the convergence of Consumer, Business and Industrial Internet, as shown in Figure 2.1.

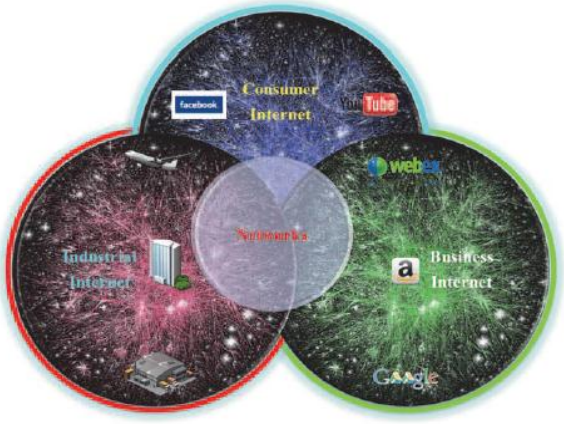


Figure 2.1: Convergence of consumer, business and industrial internet

The convergence creates the open, global network connecting people, data, and things. This convergence leverages the cloud to connect intelligent things that sense and transmit a broad array of data, helping creating services that would not be obvious without this level of connectivity and analytical intelligence. The use of platforms is being driven by transformative technologies such as cloud, things, and mobile.

The notion of network convergence using IP as presented in figure 2.1 is fundamental and relies on the use of a common multi-service IP network supporting a wide range of applications and services. The use of IP to communicate with and control small devices and sensors opens the way for the convergence of large, IT-oriented networks with real time and specialized networked applications.

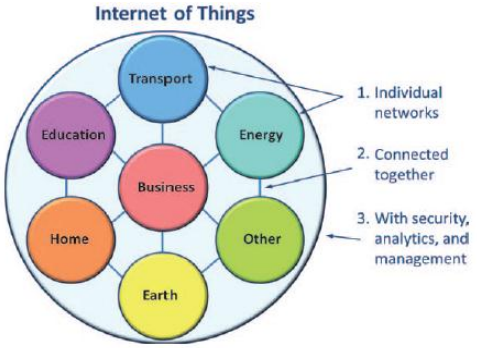
Figure 2.2: IP Convergence

Currently, the IoT is made up of a loose collection of disparate, purpose built networks, which are mostly not inter-connected. Today's vehicles, for example, have multiple networks to control engine function, safety features, communications systems, and so on.

Commercial and residential buildings also have various control systems for heating, venting, and air conditioning (HVAC); telephone service; security; and lighting.

As the IoT evolves, these networks, and many others, will be connected with added security, analytics, and management capabilities and some of them will converge. This will allow the IoT to become even more powerful in what it can help people achieve

A presentation of IoT as a network of networks is given in Figure 2.3.



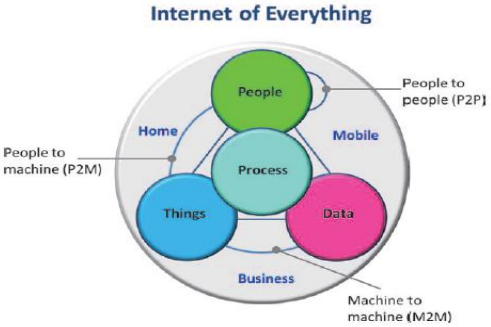
Source: Cisco IBSG, April 2011)

Figure 2.3: IoT viewed as a network of networks

The Internet of Things is not a single technology, it's a concept in which most new things are connected and enabled such as street lights being networked and things like embedded sensors, image recognition functionality, augmented reality, and near field communication are integrated into situational decision support, asset management and new services. These bring many business opportunities and add to the complexity of IT .

Distribution, transportation, logistics, reverse logistics, field service, etc. are areas where the coupling of information and "things" may create new business processes or may make the existing ones highly efficient and more profitable.

The Internet is not only a network of computers, but it has evolved into a network of devices of all types and sizes, vehicles, smartphones, home appliances, toys, cameras, medical instruments and industrial systems, all connected, all communicating and sharing information all the time as presented in Figure 2.4.



Source: Cisco

Figure 2.4: Internet of everything

IV. THE FUNDAMENTAL COMPONENTS OF THE INTERNET OF THINGS

With the changing scope of applications of internet shifting towards making physical world smarter there is no doubt that people will witness a shift in the number of connected devices soon. Within 5 years it is estimated that 50 billion devices will be online. What's more interesting is of these devices the mostly will be conventional physical objects. PCs, laptops and smart devices which dominate the internet at present will be dwarfed by these physical objects. The prerequisites of Internet of Things are many. Still the main components can be categorized into three categories i.e. intelligence, sensing and communication.

Internet of Things is going to sustain a $14 trillion market which means scope of this tech is no very large. After understanding internet of things definition you should know about the fundamentals of IoT architecture which is important to start building applications and devices.

There is no limit to applications provided prerequisites of Internet of Things are met. Healthcare, personal security, home automation, industrial automation, traffic control and environment monitoring all can be done more efficiently using this IoT tech.

INTELLIGENCE AND SENSING

Wireless networks are utmost important for the success of the IoT infrastructure. Sensors should be able to communicate without constraints of physical wiring. It makes them more independent as well as increases their domain use. Sensing of capabilities of the IoT nodes should not only be efficient but also exhibit power use efficiency. The smart connected devices will be lying down dormant for most of the period. They will activate only when there is need to read or send data or to make a decision. In simple words 90% of their time sensors will not need power for relaying data or carry out any high power-consuming function. This requires the intelligent hardware to have ultra-low energy consuming sleep mode capability. Many companies are already producing microcontrollers sporting this requirement. *W*ireless connectivity with low power consumption is vital for the success of IoT.

One important factor affecting the power efficiency of IoT devices is the architecture. While 32bit cores low cost microcontrollers have the advantage of being more compatible to large number of open-source software still they have high power consumption. Atmel, Texas Instruments, Free scale, and STMicroelectronics are offering such microcontrollers that make application building very fast. However the 8-bit AVR platform from Atmel still makes it obvious that there is scope of improvement in existing architectures.

SMART COMMUNICATION

To lower the power consumption by an IoT node only hardware changes is not the way. Smart communication protocols like ZigBee help in making exchange of data between devices less power consuming.

ZIGBEE

A low power consuming IEEE 802.15.4(2003) standard based specification, ZigBee is a brain child of 16 automation companies. What makes it novel is the use of mesh networking which makes utilization of communication resources much more efficient. ZigBee based IoT nodes can connect to central controller making use of in-between nodes for propagating the data. It makes transmission and handling of data robust.

BLUETOOTH LOW ENERGY (BLE)

Nokia originally introduced this protocol as Wibree in 2006. Also known as Bluetooth Smart this protocol provides the same range coverage with much reduced power consumption as the original Bluetooth. It has similar bandwidth with narrow spacing as used by ZigBee. Low power latency and lower complexity makes BLE more suitable to incorporate into low cost microcontrollers. *L*ow power latency and lower complexity makes more suitable to incorporate into low cost microcontrollers.

As far as application is concerned BLE is in healthcare sector. As wearable health monitors are becoming prevalent the sensors of these devices can easily communicate with a smart phone or any medical instrument regularly using BLE protocol.

WI-FI

Counted as the most mature wireless radio technology, Wi-Fi is predominant communication technology chosen for IoT applications. Already existing protocols like WPS make the integration of internet of things devices easier with the existing network. If we talk about transmission then Wi-Fi offers the best power-per-bit efficiency. However power consumption when devices are dormant is much higher with conventional Wi-Fi designs. The solution is provided by protocols like BLE and ZigBee that reduce power consumption by sensors when devices are dormant.

The ideal solution is to mix the two technologies for optimum power utilization. Gain Span's GS2000 is one such tech which used both ZigBee and Wi-Fi. It makes optimum use of power by putting the device into energy-saving standby mode when no data transmission is taking place. Only when device is awaked or checked for connection failure the high power consumption connection of Wi-Fi is used. BLE and Wi-Fi together can be used without interference as they are compliable to coexistence protocols. The Bluegiga APx4 is one such solution which supports both BLE and Wi-Fi and is based on 450MHz ARM9 processor.

Most important use of Wi-Fi is in the applications where IP stack compliance is needed and there is high data transmission. For instance in applications sharing audio, video or remote device controlling.

As the prerequisites of internet of things are scaling up, companies are working on more integrated solutions. But even at present there are many solutions available for anyone who is trying to build up internet of things applications around the major three IoT components. Vendors like Atmel,

ISSN: 2394-4404

STMicroelectronics, Texas Instruments, CSR and Freescale are offering many integrated microcontrollers and support chipsets making application building a lot easier based on protocols like ZigBee, BLE and Wi-Fi.

V. INTERNET OF ENERGY

New concept of Internet of Energy requires web based architectures to readily guarantee information delivery on demand and to change the traditional power system into a networked Smart Grid that is largely automated, by applying greater intelligence to operate, enforce policies, monitor and self-heal when necessary.

This requires the integration and interfacing of the power grid to the network of data represented by the Internet, embracing energy generation, transmission, delivery, substations, distribution control, metering and billing, diagnostics, and information systems to work seamlessly and consistently.

This concept would enable the ability to produce, store and efficiently use energy, while balancing the supply/demand by using a cognitive Internet of Energy that harmonizes the energy grid by processing the data, information and knowledge via the Internet.

In fact, as seen in Figure 2.7, the Internet of Energy will leverage on the information highway provided by the Internet to link computers, devices and services with the distributed smart energy grid that is the freight highway for renewable energy resources allowing stakeholders to invest in green technologies and sell excess energy back to the utility.

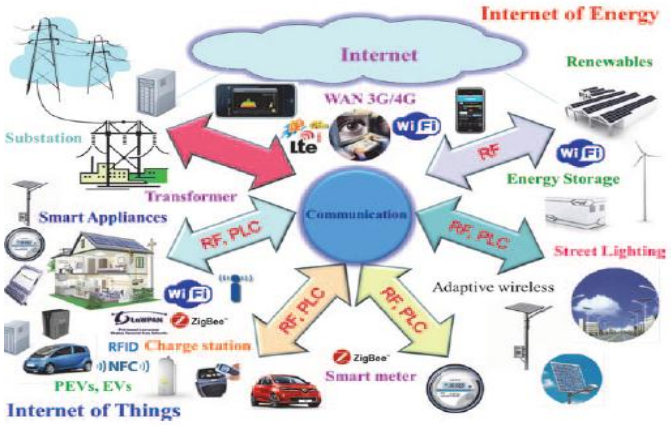


Figure 2.7: Internet of Things embedded in internet of energy applications

The Internet of Energy applications are connected through the Future Internet and Internet of Things enabling seamless and secure interactions and cooperation of intelligent embedded systems over heterogeneous communication infrastructures.

It is expected that this "development of smart entities will encourage development of the novel technologies needed to address the emerging challenges of public health, aging population, environmental protection and climate change, conservation of energy and scarce materials, enhancements to safety and security and the continuation and growth of economic prosperity."

The IoT applications are further linked with Green ICT, as the IoT will drive energy-efficient applications such as smart grid, connected electric cars, energy-efficient buildings, thus eventually helping in building green intelligent cities.

VI. APPLICATIONS & SCENARIOS

The IoT vision is that "the major objectives for IoT are the creation of smart environments/spaces and self-aware things (for example: smart transport, products, cities, buildings, rural areas, energy, health, living, etc.) see figures 2.5 and 2.6.

Figure 2.5: Internet of Things — smart environments and smart spaces creation

The outlook for the future is the emerging of a network of interconnected uniquely identifiable objects and their virtual representations in an Internet alike structure that is positioned over a network of interconnected computers allowing for the creation of a new platform for economic growth.

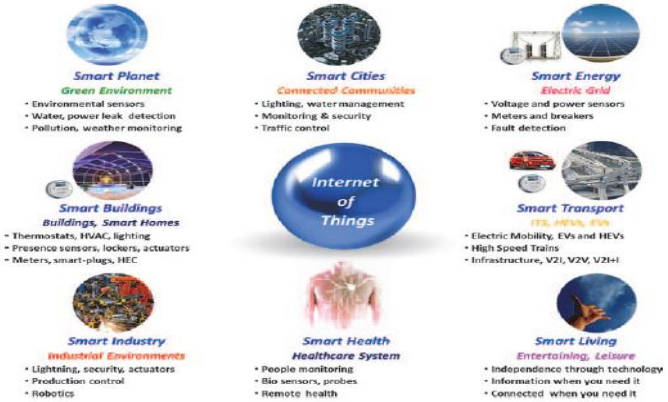


Figure 2.6: Internet of Things in the context of smart environments and applications

VII. IOT APPLICATIONS FOR INDUSTRY

The expectations toward IoT applications in industry are high. The capabilities they have to offer are depending strongly on the industrial area and the concrete application. For example the environment where IoT application may be used may range from clean room condition and normal ambient temperatures to heavy and dirty environment, locations with high temperatures, areas with explosion risk, areas with metallic surroundings, and corrosive environment on sea or underground.

A list of a set of industry related capabilities and requirements are presented below, without claiming completeness.

Areas	Supply Chain	Industry	Lifetime
Activities	Logistics	Manufacturing	Services
IoT present Application and Value	Many	Some	Few
IoT additional Applications Potential	Increase	Strong	Strong

Table 1: Status and estimated potential of IoT applications

The list items are related to the IoT hardware, software and to serviceability and management aspects. Comments have been added to all items to make the requirement more specific. The IoT application capabilities for industrial application should meet requirements such as:

- ✓ Reliability: Reliable IoT devices and systems should allow a continuous operation of industrial processes and perform on-site activities.
- ✓ Robustness: The IoT application and devices should be robust and adapted to the task and hard working conditions. This should include also the certifications for the specific work environment where they are used.
- ✓ Reasonable cost: Cost aspects are essential and should be fully justifiable and adapted to the benefit. It is basically about the right balance between cost and benefit rather than low cost. Also the costs are related to a more holistic view and life costs and consider the impact on the whole industrial installation in case of a failed IoT device or application.
- ✓ Security and safety: Security requirements are related to the cyber security threats and have to be part of the entire security strategy of the company. Safety is mainly related to the device construction and the area of use but also to usability such that no safety threats occur due to use of the IoT applications and devices.
- ✓ Simple use: Simple, intuitive use and (almost) self-explaining are important for the overall IoT application acceptance. The IoT application should ideally be context aware and adapt to the skills of the user and location or environment aspects.
- ✓ Optimal and adaptive set of features: The IoT application should allow to perform desired task with the sufficient, not-richer-then-necessary, set of features
- ✓ Low/No maintenance: Maintenance free or reduced maintenance IoT applications and devices over operational life would be ideal. Maintenance over lifetime is an important aspect impacting the life cycle costs of IoT based solutions. It is affected by the sometimes high number of IoT devices in place, the fact that they are typically distributed over large areas, the required skills, tools and time needed for any type of IoT maintenance operation. This is valid for all devices but especially for active IoT devices or active wireless sensing.
- ✓ Standardization: IoT devices and applications should be using a set of standards to support interoperability of IoT devices, easy exchange and multivendor possibilities.
- ✓ Integration capabilities: Easy integration in the IT and automation and process landscape of the industrial plant are required and may decide if a IoT solution will be used. This is particularly important for brown-field projects but also for green field in the view of future plant extensions.
- ✓ Reach sensing and data capabilities: IoT applications will relay more and more on complex sensing allowing distributed supervision and data collection and data capabilities. This is a chance in terms of additional data and real-time information but also a challenge in terms of data and processing.
- ✓ Industry grade support and services: The IoT applications should be supported over years in operation by a set of rich tools and continuously updated services. Typically industry application requires also a centralized management of devices and systems, managed access rights; this might apply to some of IoT devices too.

VIII. CHALLENGES FACED BY IOT INDUSTRY APPLICATIONS

The challenges for IoT industrial applications can be subject of a more extended treatment, however for the needs of present IoT applications and value creation they have been divided in 4 groups:

- ✓ IoT device technical challenges
- ✓ Lifetime and energy challenge
- ✓ Data and information challenge
- ✓ Humans and business

The IoT devices technical challenges are numerous and subject of intense research. Some aspects will be addressed also in the following sections.

- ✓ A set of technical features will be especially needed in industrial applications, depending on application, such as extended capabilities for sensing in terms of sensor types and high sampling rate, communication, wireless data transfer and precise time synchronous collection of data both in single-hop and multihop industrial networks.
- ✓ Another aspect is related to the easy deployment, configuration and re-use of non-permanently attached devices, such as the ones used for ad-hoc sensing. One critical and often neglected aspect is the device packaging for the industrial application needs which is essential for reliable operation.
- ✓ Last but not least is the heterogeneity aspect which is a problem even today. In industrial environments often encountered are combinations of one or more of: of passive and active RFID with or without sensing, various fix or mobile RFID readers, wireless sensor nodes and networks, wired and wireless technologies in factory automation, use of different frequency bands 13.5 MHz, 433 MHz, 860–925, 2.4 GHz, use of various “languages” — ISO standards, and different mobile devices and ecosystems. A special challenge related to IoT devices is related to lifetime of the IoT device which is less than of the normal industrial installation.
- ✓ The IoT devices are important sources of rich and spatial distributed identification, historical and sensor data in industrial environment. With the advent of more intensive use in industry and taking as an example an industrial supervision case the data amounts can really explode.

- ✓ IoT technologies can help to support the humans and to disburden them from doing hard routine work or wasting their time searching for information. New types of industrial and business processes for operation and for servicing machineries have to be put in place, considering IoT technologies supported approaches which otherwise would not have been possible.
- ✓ It is also challenging to integrate new IoT applications into existing running and producing plant systems with minor drawbacks – to handle brown field applications.

REFERENCES

[1] Dr. Ovidiu Vermesan SINTEF, Norway, Dr. PeterFriessEU, Belgium, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems", river publishers' series in communications, 2013.
[2] https://www.iis.se/docs/The-Internet-of-things.pdf
[3] https://www.webopedia.com/TERM/I/internet_of_things.html
[4] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
[5] https://dzone.com/articles/introduction-to-iot-sensors
[6] https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf
[7] https://internetofthingswiki.com/requirements-internet-of-things/236/
[8] http://www.internet-of-things-research.eu/