Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges

Preprint · May 2016

CITATIONS
0

READS
349,327

4 authors, including:

Sunil Patel
The Maharaja Sayajirao University of Baroda
3 PUBLICATIONS **11** CITATIONS
SEE PROFILE

Carlos Salazar
Universidad Iberoamericana Ciudad de México
4 PUBLICATIONS **6** CITATIONS
SEE PROFILE

DOI 10.4010/2016.1482
ISSN 2321 3361 © 2016 IJESC

IJESC

Research Article Volume 6 Issue No. 5

Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges

Keyur K Patel[1], Sunil M Patel[2]
PG Scholar[1] Assistant Professor[2]
Department of Electrical Engineering
Faculty of Technology and Engineering-MSU, Vadodara, Gujarat, India
Keyurpatel11091@gmail.com[1], patelsunilkumarm@gmail.com[2]

Abstract:
The Internet of things refers to a type of network to connect anything with the Internet based on stipulated protocols through information sensing equipments to conduct information exchange and communications in order to achieve smart recognitions, positioning, tracing, monitoring, and administration. In this paper we briefly discussed about what IOT is, how IOT enables different technologies, about its architecture, characteristics & applications, IOT functional view & what are the future challenges for IOT.

Key Terms: IOT (Internet of Things), IOT definitions, IOT functional view, architecture, characteristics, future challenges.

I. INTRODUCTION

The IOT concept was coined by a member of the Radio Frequency Identification (RFID) development community in 1999, and it has recently become more relevant to the practical world largely because of the growth of mobile devices, embedded and ubiquitous communication, cloud computing and data analytics.[12]

Imagine a world where billions of objects can sense, communicate and share information, all interconnected over public or private Internet Protocol (IP) networks. These interconnected objects have data regularly collected, analyzed and used to initiate action, providing a wealth of intelligence for planning, management and decision making. This is the world of the Internet of Things (IOT). [12]

Internet of things common definition is defining as: Internet of things (IOT) is a network of physical objects. The internet is not only a network of computers, but it has evolved into a network of device of all type and sizes , vehicles, smart phones, home appliances, toys, cameras, medical instruments and industrial systems, animals, people, buildings, all connected ,all communicating & sharing information based on stipulated protocols in order to achieve smart reorganizations, positioning, tracing, safe & control & even personal real time online monitoring , online upgrade, process control & administration[1,2].

We define IOT into three categories as below:

Internet of things is an internet of three things: (1). People to people, (2) People to machine /things, (3) Things /machine to things /machine, Interacting through internet.

Internet of Things Vision: 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. In this context 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. [1, 2]

Figure1 Internet of things [5]

Internet of Things is refer to the general idea of things, especially everyday objects, that are readable, recognisable, locatable, addressable through information sensing device and/or controllable via the Internet, irrespective of the communication means (whether via RFID, wireless LAN, wide area networks, or other means). Everyday objects include not only the electronic devices we encounter or the products of higher technological development such as vehicles and equipment but things that we do not ordinarily think of as electronic at all - such as food , clothing ,chair, animal, tree, water etc. [1,2]

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. [1, 2]

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.

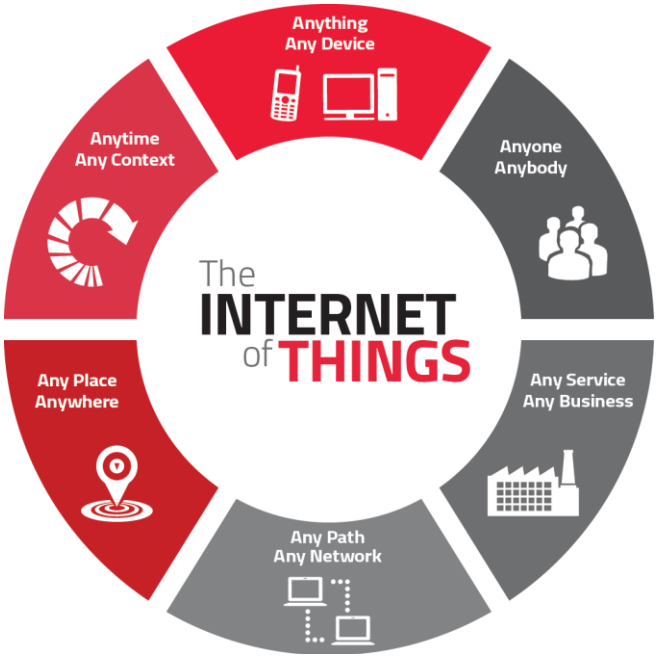

Figure2
Internet of things [11]

II. ENABLING TECHNOLOGIES FOR IOT

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.

With the Internet of Things the communication is extended via Internet to all the things that surround us. The Internet of Things is much more than machine to machine communication, wireless sensor networks, sensor networks , 2G/3G/4G,GSM,GPRS,RFID, WI-FI, GPS, microcontroller, microprocessor etc. These are considered as being the enabling technologies that make "Internet of Things" applications possible.

Enabling technologies for the Internet of Things are considered in [1] and can be grouped into three categories: (1) technologies that enable "things" to acquire contextual information, (2) technologies that enable "things" to process contextual information, and (3) technologies to improve security and privacy. The first two categories can be jointly understood as functional building blocks required building "intelligence" into "things", which are indeed the features that differentiate the IoT from the usual Internet. The third category is not a functional but rather a de facto requirement, without which the penetration of the IoT would be severely reduced. [2]

The Internet of Things is not a single technology, but it is a mixture of different hardware & software technology. The Internet of Things provides solutions based on the integration of information technology, which refers to hardware and software used to store, retrieve, and process data and communications technology which includes electronic systems used for communication between individuals or groups.

There is a heterogeneous mix of communication technologies, which need to be adapted in order to address the needs of IoT applications such as energy efficiency, speed, security, and reliability. In this context, it is possible that the level of diversity will be scaled to a number a manageable connectivity technologies that address the needs of the IoT applications, are adopted by the market, they have already proved to be serviceable, supported by a strong technology alliance. Examples of standards in these categories include wired and wireless technologies like Ethernet, WI-FI, Bluetooth, ZigBee, GSM, and GPRS. [1, 2]
The key enabling technologies for the Internet of Things is presented in Figure 3.

III. CHARACTERISTICS

The fundamental characteristics of the IoT are as follows [2, 6]:

Interconnectivity: With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.

Things-related services: The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.

Heterogeneity: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

Dynamic changes: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

Enormous scale: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet.

Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

Safety: As we gain benefits from the IoT, we must not forget about safety. As both the creators and recipients of the IoT, we must design for safety. This includes the safety of our personal data and the safety of our physical well-being. Securing the endpoints, the networks, and the data moving across all of it means creating a security paradigm that will scale.

Connectivity: Connectivity enables network accessibility and compatibility. Accessibility is getting on a network while compatibility provides the common ability to consume and produce data.

Figure3
Internet of things: Enabling technology.

IV. IOT ARCHITECTURE

IOT architecture consists of different layers of technologies supporting IOT. It serves to illustrate how various technologies relate to each other and to communicate the scalability, modularity and configuration of IOT deployments in different scenarios. Figure 4 shows detailed architecture of IOT. The functionality of each layer is described below [2, 12]:

A. smart device / sensor layer:

The lowest layer is made up of smart objects integrated with sensors. The sensors enable the interconnection of the physical and digital worlds allowing real-time information to be collected and processed. There are various types of sensors for different purposes. The sensors have the capacity to take measurements such as temperature, air quality, speed, humidity, pressure, flow, movement and electricity etc. In some cases, they may also have a degree of memory, enabling them to record a certain number of measurements. A sensor can measure the physical property and convert it into signal that can be understood by an instrument. Sensors are grouped according to their unique purpose such as environmental sensors, body sensors, home appliance sensors and vehicle telematics sensors, etc.

Most sensors require connectivity to the sensor gateways. This can be in the form of a Local Area Network (LAN) such as Ethernet and Wi-Fi connections or Personal Area Network (PAN) such as ZigBee, Bluetooth and Ultra Wideband (UWB). For sensors that do not require connectivity to sensor aggregators, their connectivity to backend servers/applications can be provided using Wide Area Network (WAN) such as GSM, GPRS and LTE. Sensors that use low power and low data rate connectivity, they typically form networks commonly known as wireless sensor networks (WSNs). WSNs are gaining popularity as they can accommodate far more sensor nodes while retaining adequate battery life and covering large areas.

B. Gateways and Networks

Massive volume of data will be produced by these tiny sensors and this requires a robust and high performance wired or wireless network infrastructure as a transport medium. Current networks, often tied with very different protocols, have been used to support machine-to-machine (M2M) networks and their applications. With demand needed to serve a wider range of IOT services and applications such as high speed transactional services, context-aware applications, etc, multiple networks with various technologies and access protocols are needed to work with each other in a heterogeneous configuration. These networks can be in the form of a private, public or hybrid models and are built to support the communication requirements for latency, bandwidth or security. Various gateways (microcontroller, microprocessor...) & gateway networks (WI-FI, GSM, GPRS…) are shown in figure 3.

C. Management Service Layer

The management service renders the processing of information possible through analytics, security controls, process modeling and management of devices.

One of the important features of the management service layer is the business and process rule engines. IOT brings connection and interaction of objects and systems together providing information in the form of events or contextual data such as temperature of goods, current location and traffic data. Some of these events require filtering or routing to post-processing systems such as capturing of periodic sensory data, while others require response to the immediate situations such as reacting to emergencies on patient's health conditions. The rule engines support the formulation of decision logics and trigger interactive and automated processes to enable a more responsive IOT system.

In the area of analytics, various analytics tools are used to extract relevant information from massive amount of raw data and to be processed at a much faster rate. Analytics such as in-memory analytics allows large volumes of data to be cached in random access memory (RAM) rather than stored in physical disks. In-memory analytics reduces data query time and augments the speed of decision making. Streaming analytics is another form of analytics where analysis of data, considered as data-in-motion, is required to be carried out in real time so that decisions can be made in a matter of seconds.

Data management is the ability to manage data information flow. With data management in the management service layer, information can be accessed, integrated and controlled. Higher layer applications can be shielded from the need to process unnecessary data and reduce the risk of privacy disclosure of the data source. Data filtering techniques such as data anonymisation, data integration and data synchronization, are used to hide the details of the information while providing only essential information that is usable for the relevant applications. With the use of data abstraction, information can be extracted to provide a common business view of data to gain greater agility and reuse across domains.

Security must be enforced across the whole dimension of the IOT architecture right from the smart object layer all the way to the application layer. Security of the system prevents system hacking and compromises by unauthorized personnel, thus reducing the possibility of risks.

D. Application Layer

The IoT application covers "smart" environments/spaces in domains such as: Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Healthcare, User interaction, Culture and tourism, Environment and Energy.

V. IOT FUNCTIONAL VIEW

The Internet of Things concept refers to uniquely identifiable things with their virtual representations in an Internet-like structure and IoT solutions comprising a number of components such as : (1) Module for interaction with local IoT devices. This module is responsible for acquisition of observations and their forwarding to remote servers for analysis and permanent storage. (2) Module for local analysis and processing of observations acquired by IoT devices. (3) Module for interaction with remote IoT devices, directly over the Internet. This module is responsible for acquisition of observations and their forwarding to remote servers for analysis and permanent storage. (4) Module for application specific data analysis and processing. This module is running on an application server serving all clients. It is taking requests from mobile and web clients and relevant IoT observations as input, executes appropriate data processing algorithms and generates output in terms of knowledge that is later presented to users. (5) User interface (web or mobile): visual representation of measurements in a given context (for example on a map) and interaction with the user, i.e. definition of user queries. [2]

VI. FUTURE TECHNOLOGICAL DEVELOPMENTS FOR IOT.

The development of enabling technologies such as semiconductor electronics, communications, sensors, smart phones, embedded systems, cloud networking, network virtualization and software will be essential to allow physical devices to operate in changing environments & to be connected all the time everywhere.

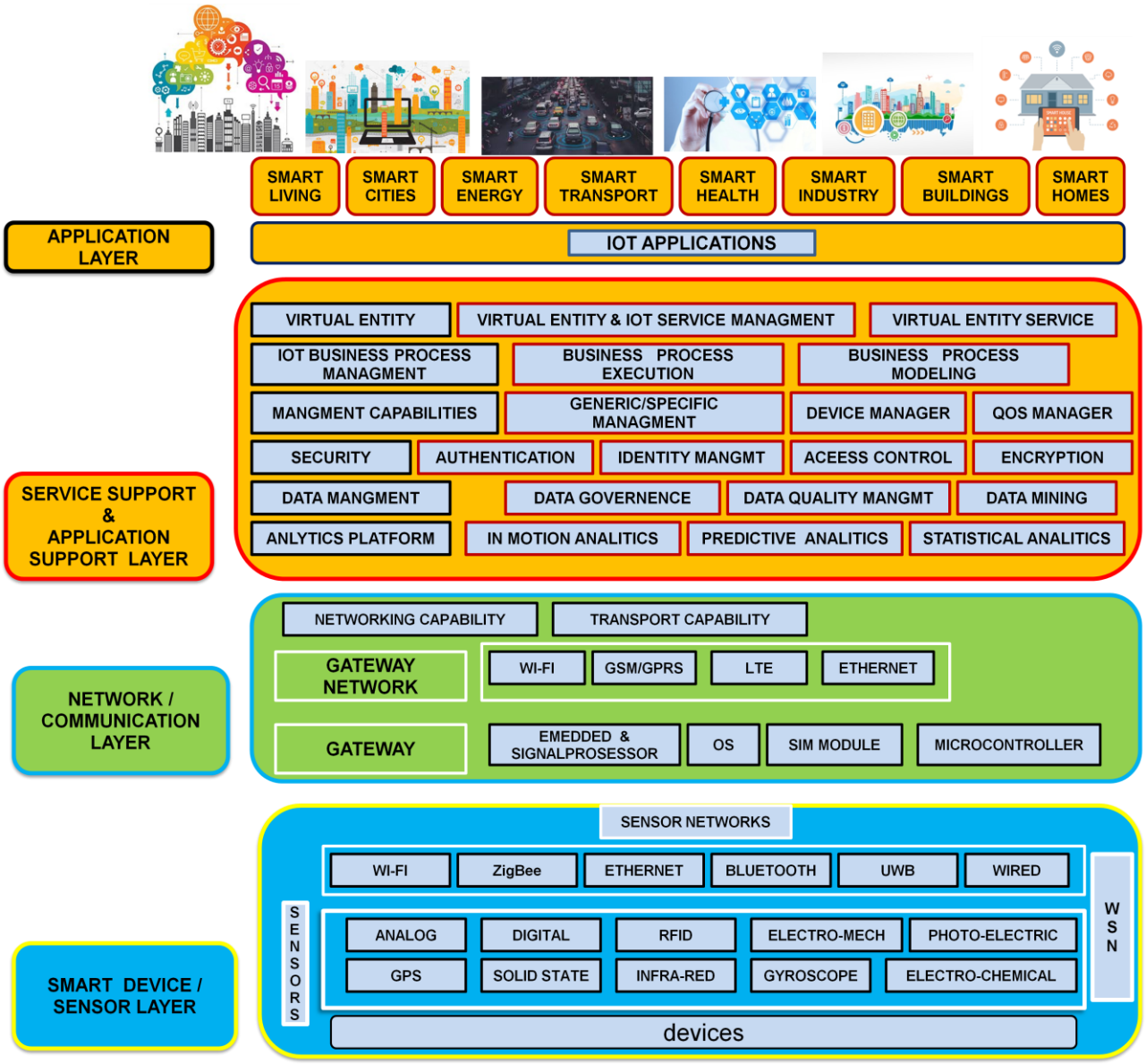

Figure 4
IOT Architecture

While IOT is architected into layers, the technologies have been categorized into three groups. []

The first group of technologies impacts the devices, microprocessor chips:
- Low power sensors for power and energy sustainability;
- Intelligence of sensors in the field;
- Miniaturization of chipsets;
- Wireless sensor network for sensor connectivity.

The second group comprises technologies that support network sharing and address capacity and latency issues:
- Network sharing technologies such as software-defined radios and cognitive networks;
- Network technologies that address capacity and latency issues such as LTE and LTE-A.

The third group impacts the management services that support the IOT applications:
- Intelligent decision-making technologies such as context-aware computing service, predictive analytics, complex event processing and behavioral analytics;
- Speed of data processing technologies such as in-memory and streaming analytics.

Below table shows future development & future research needs for enabling technologies of IOT. [1, 2]

Table 1
Future development & research needs

TECHNOLOGY	FUTURE DEVELOPMENT	RESEARCH NEEDS
Hardware Devices	•Nanotechnology •Miniaturization of chipsets •Ultra low power circuits	•Low cost modular devices •Ultra low power EPROM/FRAM •Autonomous circuits
SENSOR	•Smart sensors (bio-chemical) •More sensors (tiny sensors) •Low power sensors •Wireless sensor network for sensor connectivity	•Self powering sensors • Intelligence of sensors
Communication Technology	•On chip antennas •Wide spectrum and spectrum aware protocols •Unified protocol over wide Spectrum •Multi-functional reconfigurable chips	•Protocols for interoperability •Multi-protocol chips •Gateway convergence •On chip networks •Longer range (higher frequencies – tenths of GHz) •5G developments
Network Technology	•Self aware and self organizing networks •Self-learning, self-repairing networks •IPv6- enabled scalability •Ubiquitous IPv6-based IoT deployment	•Grid/Cloud network •Software defined networks •Service based network •Need based network
Software and algorithms	•Goal oriented software •Distributed intelligence, problem solving •User oriented software	•Context aware software •Evolving software •Self reusable software •Autonomous things: •Self configurable •Self healing •Self management
Data and Signal Processing Technology	•Context aware data processing and data responses •Cognitive processing and optimization •IoT complex data analysis •IoT intelligent data visualization •Energy, frequency spectrum aware data processing	•Common sensor ontology •Distributed energy efficient data processing •Autonomous computing
Discovery and Search Engine Technologies	•Automatic route tagging and identification management centers •On demand service discovery/integration	•Scalable Discovery services for connecting things with services
Security & Privacy Technologies	•User centric context-aware privacy and privacy policies •Privacy aware data processing •Security and privacy profiles selection based on security and privacy need	•Low cost, secure and high performance identification/ authentication devices •Decentralized approaches to privacy by information localization

VII. INTEROPERABILITY IN THE IOT

IoT aims for integrating the physical world with the virtual world by using the Internet as the medium to communicate and exchange information. However, heterogeneity of underlying devices and communication technologies and interoperability in different layers, from communication and seam-less integration of devices to interoperability of data generated by the IoT resources, is a challenge for expanding generic IoT solutions to a global scale.

As for the IoT, future networks will continue to be heterogeneous, multi-vendors, multi-services and largely distributed. Consequently, the risk of non-interoperability will increase.

Interoperability is a key challenge in the realms of the Internet of Things (IoT). This is due to the intrinsic fabric of the IoT as: (1) high–dimensional, with the co-existence of many

systems (devices, sensors, equipment, etc.) in the environment that need to communicate and exchange information; (2) highly-heterogeneous, where these vast systems are conceived by a lot of manufacturers and are designed for much different purposes and targeting diverse application domains, making it extremely difficult to reach out for global agreements and widely accepted specification; (3) dynamic and non-linear, where new Things (that were not even considered at start) are entering (and leaving) the environment all the time and that support new unforeseen formats and protocols but that need to communicate and share data in the IoT; and (4) hard to describe/model due to existence of many data formats, described in much different languages, that can share (or not) the same modeling principles, and that can be interrelated in many ways with one another. This qualifies interoperability in the IoT as a problem of complex nature. [2]

Interoperability is: "the ability of two or more systems or components to exchange data and use information". This definition is interesting as provide many challenges on how to: • Get the information, • Exchange data, and • Use the information in understanding it and being able to process it. Different types of interoperability are technical interoperability, Syntactical Interoperability, Semantic Interoperability, Organizational Interoperability. [9] A simple representation of interoperability is shown in figure 5.

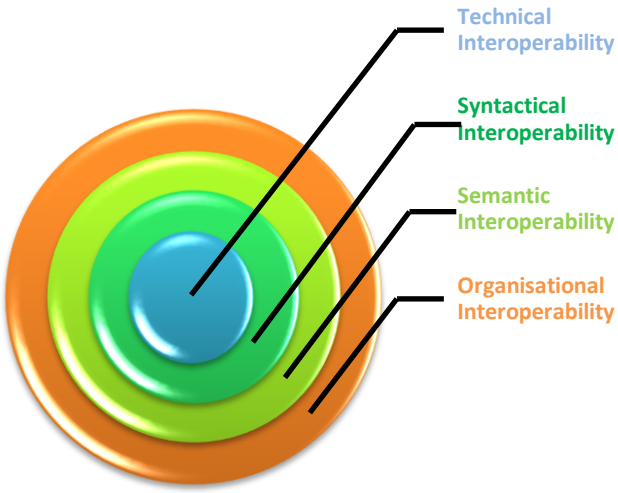

Figure 5
The Dimensions of Interoperability

Technical Interoperability is usually associated with hardware/ software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centered on (communication) protocols and the infrastructure needed for those protocols to operate. **Syntactical Interoperability** is usually associated with data for-mats. Certainly, the messages transferred by communication protocols need to have a well-defined syntax and encoding, even if it is only in the form of bit-tables. However, many protocols carry data or content, and this can be represented using high-level transfer syntaxes such as HTML, XML or ASN.1.

Semantic Interoperability is usually associated with the meaning of content and concerns the human rather than machine interpretation of the content. Thus, interoperability on this level means that there is a common understanding between people of the meaning of the content (information) being exchanged.

Organizational Interoperability, as the name implies, is the ability of organizations to effectively communicate and transfer (meaningful) data (information) even though they may be using a variety of different information systems over widely different infrastructures, possibly across different geographic regions and cultures. Organizational interoperability depends on successful technical, syntactical and semantic interoperability**.**

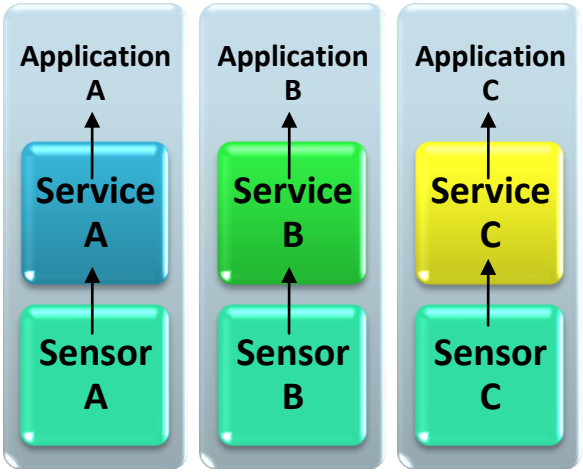

Figure 6
Non-interoperable IoT

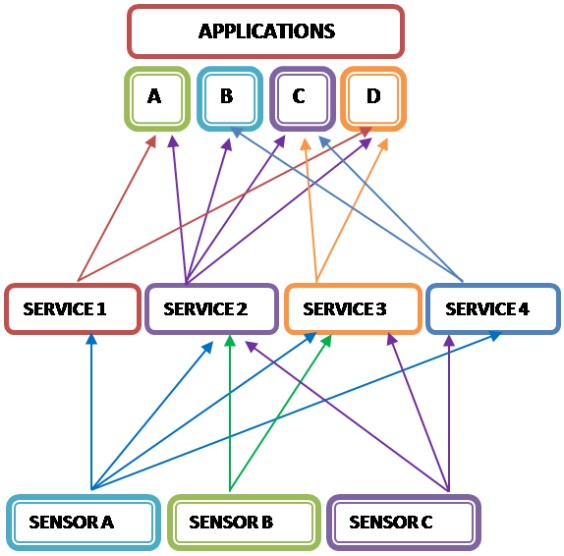

Figure 7
Interoperable IoT

Figure 6 & 7 shows difference between non interoperable & interoperable IOT.

Technical interoperability only guarantees the correct transmission of bits but does not tell anything about the meaning of these bits and what they represent, not even whether it is voice, video, or data. This is the task of standards on the syntactic layer, which define the syntax of particular services. While standards for technical and syntactic interoperability provide for content independent data exchange, semantic interoperability is highly application-specific and thus depending on the service-specific content. Like semantic interoperability Organizational interoperability is application or service-specific. Below figure shows the role of interoperability at different IOT layer. [7]

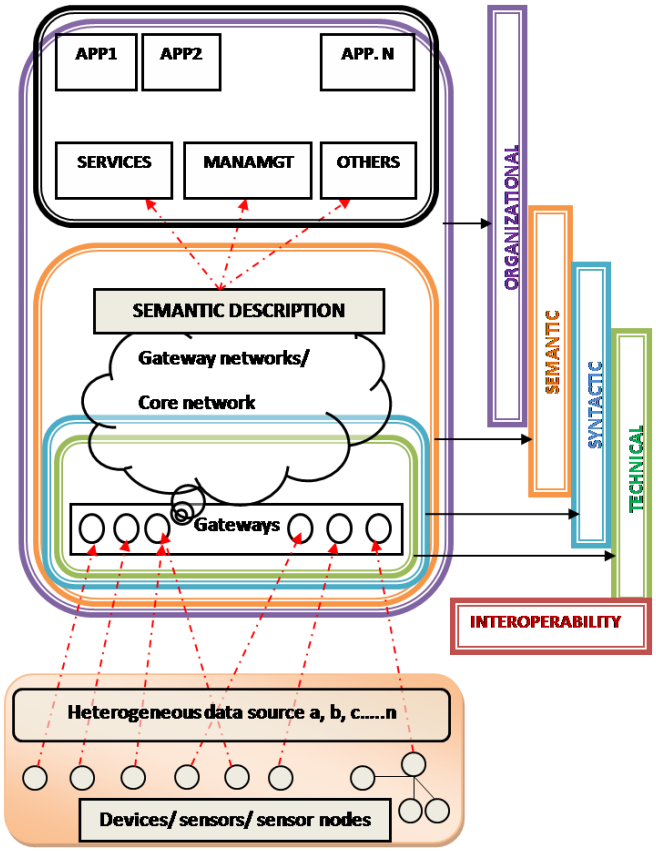

Figure 8
The role of interoperability for IoT applications and services

In a fully interoperable environment, any IoT device would be able to connect to any other device or system and exchange information as desired. In practicality, interoperability is more complex. Interoperability among IoT devices and systems happens in varying degrees at different layers within the communications protocol stack between the devices. Technical interoperability ensures basic connectivity: mechanism to established physical& logical connection between systems, network interoperability: to exchange data between multiple systems across variety of networks. Syntactic interoperability ensures understanding of data structure in data exchanged between systems. While semantic ensures understanding of concept contained in data structure. [4, 8]

VIII. FUTURE CHALLANGES FOR IOT

There are key challenges and implications today that need to be addressed before mass adoption of IOT can occur. [1, 2, 12]

A. Privacy and Security

As the IoT become a key element of the Future Internet and the usage of the Internet of Things for large-scale, partially mission-critical systems creates the need to address trust and security functions adequately. New challenges identified for privacy, trust and reliability are: • providing trust and quality-of-information in shared information models to enable re-use across many applications. • Providing secure exchange of data between IoT devices and consumers of their information. • Providing protection mechanisms for vulnerable devices.
Table 2 shows various security & privacy requirement at different layers of IOT.

Table 2
The security requirements at different layer of IOT

IOT LAYER	SECUREITY REQUIREMENTS
Application	**• Application-specific Data Minimization • Privacy Protection and Policy Management •Authentication •Authorization, Assurance •Application specific encryption, cryptography.**
Services support	**• Protected Data Management and Handling (Search, Aggregation, Correlation, Computation) • Cryptographic Data Storage • Secure Computation, In-network Data Processing, Data aggregation, Cloud Computing**
Network layer	**• Secure Sensor/Cloud Interaction; • Cross-domain Data Security Handling • Communication & Connectivity Security**
Smart object/sensor	**• Access Control to Nodes • Lightweight Encryption • Data Format and Structures • Trust Anchors and Attestation**

B. Cost versus Usability

IOT uses technology to connect physical objects to the Internet. For IOT adoption to grow, the cost of components that are needed to support capabilities such as sensing, tracking and control mechanisms need to be relatively inexpensive in the coming years.

C. Interoperability

In the traditional Internet, interoperability is the most basic core value; the first requirement of Internet connectivity is that "connected" systems be able to "talk the same language" of protocols and encodings. Different industries today use different standards to support their applications. With numerous sources of data and heterogeneous devices, the use of standard interfaces between these diverse entities becomes important. This is especially so for applications that supports cross organizational and various system boundaries. Thus the IOT systems need to handle high degree of interoperability.

D. Data Management

Data management is a crucial aspect in the Internet of Things. When considering a world of objects interconnected and constantly exchanging all types of information, the volume of the generated data and the processes involved in the handling of those data become critical.

E. Device Level Energy Issues

One of the essential challenges in IoT is how to interconnect "things" in an interoperable way while taking into account the energy constraints, knowing that the communication is the most energy consuming task on devices.

IX. APPLICATION AREAS

Potential applications of the IoT are numerous and diverse, permeating into practically all areas of every-day life of individuals, enterprises, and society as a whole. The IoT application covers "smart" environments/spaces in domains such as: Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Healthcare, User interaction, Culture and tourism, Environment and Energy. Below are some of the IOT applications. [2]

A. IOsL (Internet of smart living):

Remote Control Appliances: Switching on and off remotely appliances to avoid accidents and save energy**, Weather:** Displays outdoor weather conditions such as humidity, temperature, pressure, wind speed and rain levels with ability to transmit data over long distances, **Smart Home Appliances:** Refrigerators with LCD screen telling what's inside, food that's about to expire, ingredients you need to buy and with all the information available on a Smartphone app. Washing machines allowing you to monitor the laundry remotely, and. Kitchen ranges with interface to a Smartphone app allowing remotely adjustable temperature control and monitoring the oven's self-cleaning feature, **Safety Monitoring**: cameras, and home alarm systems making people feel safe in their daily life at home, **Intrusion Detection Systems**: Detection of window and door openings and violations to prevent intruders, **Energy and Water Use**: Energy and water supply consumption monitoring to obtain advice on how to save cost and resources, & many more…

B. IOsC (Internet of smart cities):

Structural Health: Monitoring of vibrations and material conditions in buildings, bridges and historical monuments, **Lightning**: intelligent and weather adaptive lighting in street lights, **Safety**: Digital video monitoring, fire control management, public announcement systems, **Transportation:** Smart Roads and Intelligent High-ways with warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams, **Smart Parking**: Real-time monitoring of parking spaces availability in the city making residents able to identify and reserve the closest available spaces, **Waste Management**: Detection of rubbish levels in containers to optimize the trash collection routes. Garbage cans and recycle bins with RFID tags allow the sanitation staff to see when garbage has been put out.

C. IOsE (Internet of smart environment):

Air Pollution monitoring: Control of CO2 emissions of factories, pollution emitted by cars and toxic gases generated in farms, **Forest Fire Detection:** Monitoring of combustion gases and preemptive fire conditions to define alert zones, **Weather monitoring:** weather conditions monitoring such as humidity, temperature, pressure, wind speed and rain, Earthquake Early Detection, **Water Quality**: Study of water suitability in rivers and the sea for eligibility in drinkable use, **River Floods**: Monitoring of water level variations in rivers, dams and reservoirs during rainy days, **Protecting wildlife:** Tracking collars utilizing GPS/GSM modules to locate and track wild animals and communicate their coordinates via SMS.

D. IOsI (Internet of smart industry):

Explosive and Hazardous Gases: Detection of gas levels and leakages in industrial environments, surroundings of chemical factories and inside mines, Monitoring of toxic gas and oxygen levels inside chemical plants to ensure workers and goods safety, Monitoring of water, oil and gas levels in storage tanks and Cisterns, **Maintenance and repair:** Early predictions on equipment malfunctions and service maintenance can be automatically scheduled ahead of an actual part failure by installing sensors inside equipment to monitor and send reports.

E. IOsH (Internet of smart health):

Patients Surveillance: Monitoring of conditions of patients inside hospitals and in old people's home, **Medical Fridges:** Control of conditions inside freezers storing vaccines, medicines and organic elements, **Fall Detection:** Assistance for elderly or disabled people living independent, **Dental:** Bluetooth connected toothbrush with Smartphone app analyzes the brushing uses and gives information on the brushing habits on the Smartphone for private information or for showing statistics to the dentist, **Physical Activity Monitoring:** Wireless sensors placed across the mattress sensing small motions, like breathing and heart rate and large motions caused by tossing and turning during sleep, providing data available through an app on the Smartphone.

F. IOsE (internet of smart energy):

Smart Grid: Energy consumption monitoring and management, **Wind Turbines/ Power house**: Monitoring and analyzing the flow of energy from wind turbines & power house, and two-way communication with consumers' smart meters to analyze consumption patterns, **Power Supply Controllers:** Controller for AC-DC power supplies that determines required energy, and improve energy efficiency with less energy waste for power supplies related to computers, telecommunications, and consumer electronics applications, **Photovoltaic Installations:** Monitoring and optimization of performance in solar energy plants.

G. IOsA (internet of smart agriculture):

Green Houses: Control micro-climate conditions to maximize the production of fruits and vegetables and its quality, **Compost:** Control of humidity and temperature levels in alfalfa, hay, straw, etc. to prevent fungus and other microbial contaminants, **Animal Farming/Tracking:** Location and identification of animals grazing in open pastures or location in big stables, Study of ventilation and air quality in farms and detection of harmful gases from excrements, **Offspring Care:** Control of growing conditions of the offspring in animal farms to ensure its survival and health, **field Monitoring:** Reducing spoilage and crop waste with better monitoring, accurate ongoing data obtaining, and management of the agriculture fields, including better control of fertilizing, electricity and watering.

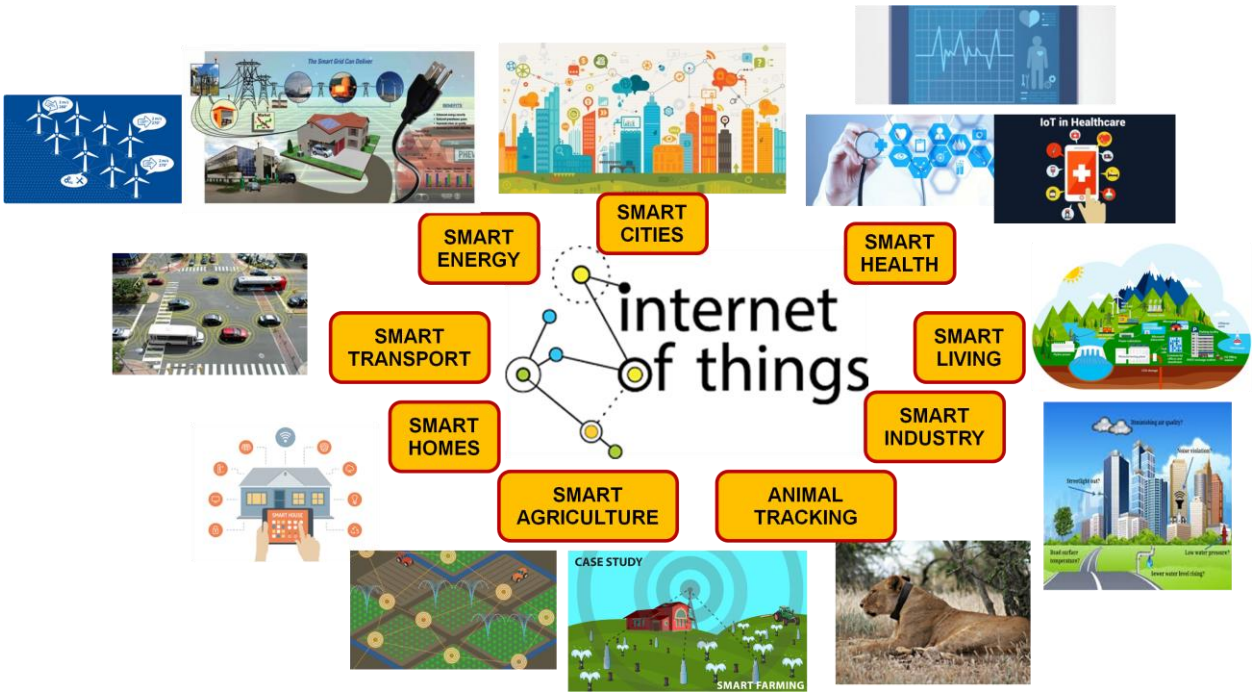

Figure 9
IoT applications

The IoT application area is very diverse and IoT applications serve different users. Different user categories have different driving needs. From the IoT perspective there are three important user categories: (1) The individual citizens, (2) Community of citizens (citizens of a city, a region, country or society as a whole), (3) The enterprises.

X. CONCLUSION

Internet of Things is a new revolution of the Internet & it is a key research topic for researcher in embedded, computer science & information technology area due to its very diverse area of application & heterogeneous mixture of various communications and embedded technology in its architecture.

REFERENCES

[1] Dr. Ovidiu Vermesan SINTEF, Norway, Dr. Peter FriessEU, Belgium, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems", river publishers' series in communications, 2013.

[2] Dr. Ovidiu Vermesan SINTEF, Norway, Dr. Peter FriessEU, Belgium, "Internet of Things–From Research and Innovation to Market Deployment", river publishers' series in communications, 2014.

[3] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., "Internet of Things Strategic Research Agenda", Chapter 2 in Internet of Things -Global Technological and Societal Trends, River Publishers, 2011.

[4] Martin Serrano, Insight Centre for Data Analytics, Ireland ,Omar Elloumi, Alcatel Lucent, France, Paul Murdock, Landis+Gyr, Switzerland, "ALLIANCE FOR INTERNET OF THINGS INNOVATION, Semantic Interoperability" , Release 2.0, AIOTI WG03 – IoT Standardisation,2015.

[5] IoT: https://dzone.com/articles/the-internet-of-things-gateways-and-next-generation.

[6] [http://www.reloade.com/blog/2013/12/6characteristics-within-internet-things-iot.php].

[7] Martín Serrano, Payam Barnaghi, Francois Carrez Philippe Cousin, Ovidiu Vermesan, Peter Friess, "Internet of Things Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps", European research cluster on the internet of things, IERC,2015.

[8] Karen Rose, Scott Eldridge, Lyman Chapin, "The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World", The Internet Society (ISOC), 2015.

[9] H. van der Veer, A.Wiles, "Achiveing Technical Interoperability —the ETSI Approach", ETSI White Paper No.3, 3rd edition, April 2008, http://www.etsi.org/images/files/ETSI WhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf

[10] ITU-T, Internet of Things Global Standards Initiative, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

[11] http://tblocks.com/internet-of-things

[12] https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/InternetOfThings.pdf