Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 5, May-2017

Internet of Things – Technology behind, Applications and Issues

Krupa R. Trambadiya

Assistant Professor, IT Department, Vadodara Institute of Engineering, Kotambi, Vadodara, India

Abstract —*IoT covers up billions of communicating devices, people and services to be linked, exchange information and useful data and is considered as a part of the Internet of the future aspect. IoT is formed by Ubiquitous and Pervasive computing, Internet Protocol, Sensor Technologies with Communicating and embedded devices. These technologies are combined together and form a system where the real world gets benefits by digital world and interact continuously. The objects are turned into smart objects when we put intelligence with them and able not only to gather information from the environment and interact and even control the bodily world, but also to be interconnected, to each other, through Internet to exchange data and information. As IoT expands from millions of devices to tens of billions in the upcoming years, it will have crucial impacts on infrastructure, industry standards, security and business models throughout the entire IT environment. Number of security and privacy issues will arise with this [1].*

Keywords- *Internet of Things; Sensors; Protocols; RFID*

I. INTRODUCTION

The Internet of Things (IoT) is a new standard that is quickly gaining spot in the scenario of now a days communications. Things, Internet, and connectivity are the three basic components of IoT, but the goal is to close the gap between the physical and digital world in self - improving systems. The basic idea of the concept is all-encompassing existence around us of a variety of things or objects - such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile devices etc. through unique addressing methods, are able to interact with each other and cooperate with their neighbors to fulfill common goals. With the perspective of a private user, the most obvious effects of the IoT introduction will be visible in both working and domestic fields. In this context, domestics, assisted living, e-health, enhanced learning are only a few examples of possible application scenarios in which the new paradigm will play a leading role in the near future. Similarly, from the perspective of business users, the most apparent consequences will be equally visible in fields such as, automation and industrial manufacturing, logistics, business/process management, intelligent transportation of people and goods [1].

Actually, many challenging issues still need to be addressed and both technological as well as social knots have to be untied before the IoT idea being widely accepted. Central issues are making a full interoperability of interconnected devices possible, providing them with an always higher degree of smartness by enabling their adaptation and autonomous behavior, while guaranteeing trust, privacy and security. Also, the IoT idea poses several new problems concerning the networking aspects. In fact, the things composing the IoT will be characterized by low resources in terms of both computation and energy capacity. Accordingly, the proposed solutions need to pay special attention to resource efficiency besides the obvious scalability problems.

As the IoT grows, network of networks and other devices will be connected with added security, analytics and management capabilities. This will let the IoT turn into even more prevailing in what it can help people achieve. A presentation of IoT as a network of networks is given in Figure 1 [2].

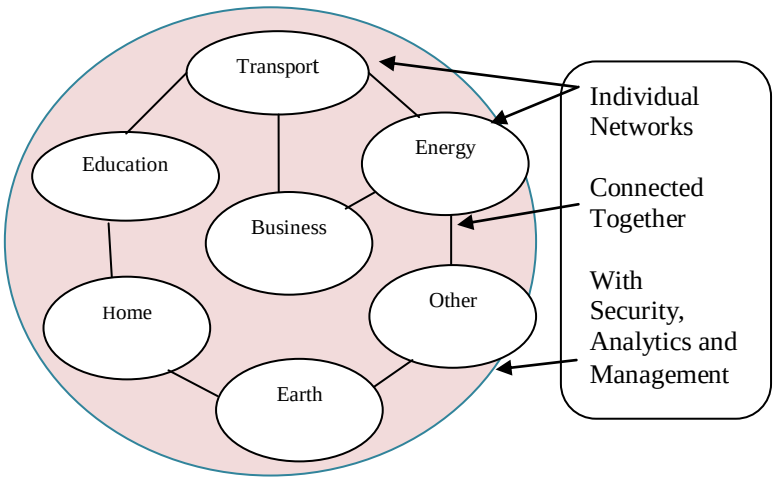

Fig 1. Internet of Things - Viewed as a network of networks

II. TECHNOLOGY BEHIND IOT

Internet of Things is formed by merging a number of technologies. Identification comes first. Each device entails a unique identification, since there will be billions of devices that will connect to the Internet. This is possible if and only if theyare IPv6 enabled, as IPv4 network has exhausted its universe of IP addresses.

Next is Sensor, as an IoT device needs to sense which is possible by putting sensors that measure numerous facets of an object. The object needs to have the ability to communicate with other objects outside the world.

Next is a central server where data from all these objects will be composed for analysis. It could be an application or an appliance that can download all data, and allow the user to access, control and evaluate it [3].

2.1. Technology for Identification

Radio Frequency Identification (RFID): It is used to uniquely identify devices and objects. Like smart card systems, data is stored on an electronic data-carrying device [4]. The technology uses radio waves to accomplish communication between the data from an electronic device for the objective of identifying and also to locate and sense the environment around.

Quick Response (QR) Code: A machine readable visual label that contains information about things to which it is attached. It uses four standardized encoding modes - numeric, alpha-numeric, byte and binary to efficiently store information about things. A QR Code on any device or thing consists of black sectored pattern organized in a rectangle which can be read by software of QR. Nowadays smartphones act as QR code readers, which understands (scans) the code and extract related information from it. QR codes can track where the thing has been scanned and find its location. In this way, they are secure to be used in real time applications.

2.2. Communication Protocols

Communication must take place between the things. Data is collected and sent to a remote server, representing device information which if required is sent back to devices with other information to generate various conclusions or actions. For this purpose numbers of protocols are used.

Message Queue Telemetry Transport (MQTT) is a protocol to gather device data and communicate it to servers. Huge networks of devices can be controlled or supervised with it. The protocol works on top of TCP providing a reliable stream of data flow.

Extensible Messaging and Presence Protocol (XMPP) is a protocol used for connecting devices with human. It's a substitute to the D2S protocol, as people are connected to servers. XMPP does great job, for example, to connect your home thermostat to a Web server so that you can monitor it with your smartphone. This protocol is ideal for consumer-based IoT uses and applications.

Data Distribution Service (DDS) is a device-to-device communication protocol. It shares device data with other devices over a network. DDS provides effective ways to filter and choose exactly which information goes where.

Advanced Message Queuing Protocol (AMQP) is a queuing protocol used to connect web servers. This protocol is suitable for server based applications.

Constrained Application Protocol (CoAP) is used in electronics devices to communicate interactively over the Internet. Such devices are low power sensors, valves, switches and related components that need to be controlled or accessed remotely, through standard Internet networks. CoAP works on application layer to be used in resource - driven internet devices, such as Wireless Sensor Networks.

IPv6 and the Internet of Things: IPv6 extends addressing space to support all growing Internet supported devices. IPv6 has been designed to provide secure communications to users and to ensure mobility for all devices connected to the user. It has been observed as the most appropriate technology for IoT as it provides scalability, end-to-end connectivity, ranged address space, etc. IPv6 integrated with Internet of Things can bring the world to a whole new level of interoperable devices.

2.3. Other Protocols and APIs

IoT uses the REST (Representational State Transfer) API architecture. To support Java programming languages, it uses JSON (JavaScript Object Notation). REST API is a platform that outlines a set of principles by which web services can

be developed focusing on resources of a system, like how the resource states are identified and transmitted over HTTP by a number of devices. REST is used in smart phone and automated business development kind of applications mostly.

Xively REST API: This API is a Platform-as-a-Service (PaaS) for Internet of Things. Xively makes interconnection of devices, data, people and places easy to form commanding alternative solutions that will make the experience of people about their world better.

2.4. Hardware to construct IOT

Both hardware and software are required to develop internet connected things. Devices like Spark Core, Smart Things, Nest, WeMo etc. designing a hardware that communicate with software and software that communicates with hardware can be achieved.

III. IOT APPLICATIONS

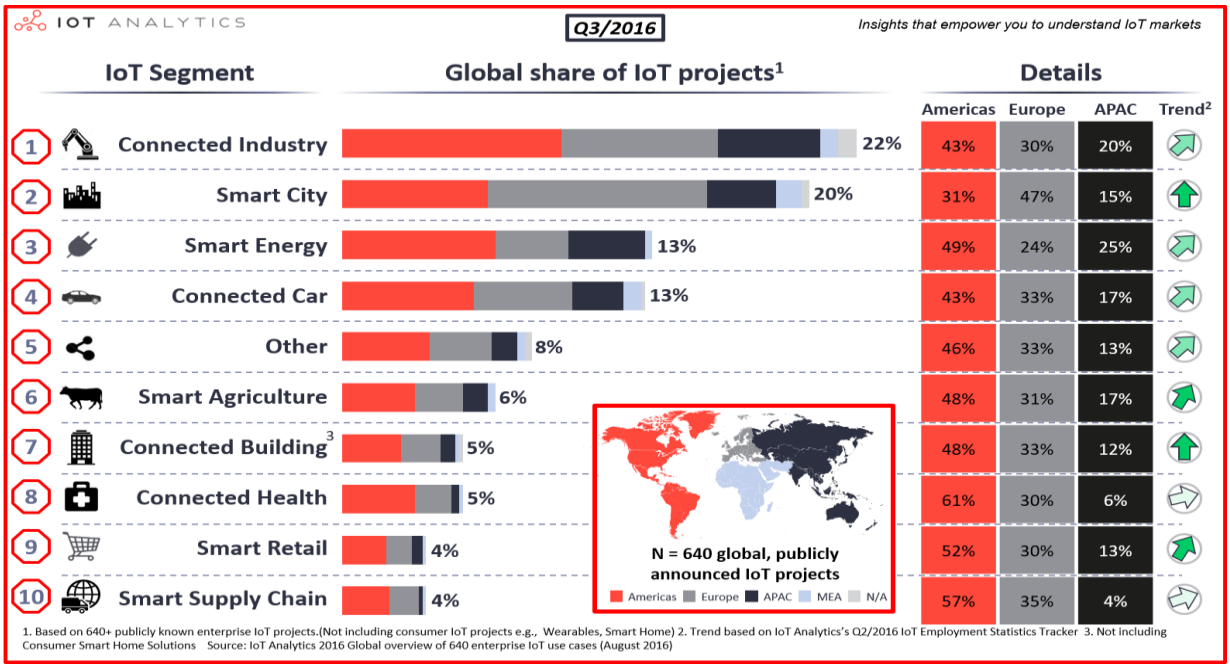

Fig 2. Top 10 IOT Application areas based on real IOT Projects [6]

Not only IoT applications are improving the comforts of our lives but also give us more control by simplifying routine work life and personal tasks [5]. Most of the IoT projects are identified in industrial backgrounds (141 projects), followed by Smart City (128) and Smart Energy IoT projects. The Americas make up most of those projects (44%), followed by Europe (34%). There are large differences between individual IoT sectors and regional IoT sectors. The Americas and particularly Northern America is strong in Connected Health (61%) and Smart Retail (52%), while the majority of Smart City projects are located in Europe (47%). The Asia-Pacific region is particularly strong in the area of Smart Energy projects (25%) [6].

Prospective of IoT markets is giant but some specific domains will mature much faster than others. Here is the discussion of some application domains for the IoT with examples that have the potential of exponential evolution.

3.1. Smart Cities

Smart cities are the real considerable solutions for the troubles people usually face due to population explosion, pollution, poor infrastructure and energy supplies shortages.Smart surveillance, safer and automated transportation, smarter energy management systems and environmental monitoring all are examples of internet of things applications for smart cities. Examples of such IoT devices are Smart Waste and Recycling System, Smart Street Lighting and Smart Parking Systems.

3.2. Connected/Smart Home

In smart home, devices have capability to communicate with each other as well as to their intangible environment. Goal behind this is to customize and control home environment for increased security and efficient energy management. There

are hundreds of IoT technologies available for monitoring and building smart homes. Such examples are Learning Thermostat, Hue-smart Lightings, Air quality Egg, Smart Speakers etc.

3.3. Healthcare

This sector is supposed to be highly boosted with benefits of internet of things applications. IoT examples in this domain are Urosense Device, Medication Dispensing Systems etc.

3.4. Wearables

These are the hottest trends in IoTnowadays. Numerous companies are surviving in a cut throat competition. Wearable devices include fitness, health and entertainment requirements. The prerequisite from internet of things technology for wearable applications is to be highly energy efficient or ultra-low power and small sized. Some top examples of wearable IoT devices are Tracker devices for sleep patterns and monitoring, Activity Tracking, Heart Rate Tracking, Workout Tracking and Smart Watches etc.

3.5. Retail

Smart supply chains,applications for tracking goods, information exchange about inventory among suppliers and retailers and automated delivery are the examples of smart Retails.

3.6. Agriculture

Highly scalable technology solutions of Internet of things applications can deliver exactly the same to farmers. Example of such application are monitoring crucial vitals of soil like humidity, air temperature and soil quality using remote sensors and monitoring the crop nutrients making use of a carbon nanotube-based sensor system more effective than conventional systems.

3.7. Automotive/Transportation

Google's self-driving cars are well-known. IoT is making connected cars a possibility but this new technology will take least a couple of years to propagate in automotive industry. Companies are announcing innovative technologies and ideas to support connected car platforms.

3.8. Industrial Automation

With help of IoT foundation supported with cutting edge sensor systems, remote network, creative equipment and machine-to-machine communication, ordinary mechanization procedure of businesses will change totally. Examples are Embedded Data Collector, Sensor Nodes etc.

3.9. Energy Management

Future Power grids won't only be smart but also highly reliable. Smart grid concept is becoming very popular. The basic idea behind the smart grids is to collect data in automated fashion and analyze the behavior or electricity consumers and suppliers for improving efficiency as well as economics of electricity use. Examples are Smart Grid and Smart Metering.

IV. ISSUES AND OPEN ENDED PROBLEMS IN IOT SYSTEMS

Security and privacy are mainly two concerns in IoT based systems [7].

4.1. Security Issues in IoT

Security issues are categorized based on the type of system accommodation whether it is at Front End, at Network or at Back End like Database.

4.1.1. Threats at Front End Sensors and Devices

- Denial Service Attack
- Unauthorized access to Data
- Threats to Internet
- Attacks of Analysis of Machine to Machine Information
- Attacks to availability of Machine to Machine Information

4.1.2. Threats at Network

- Unauthorized access to Data
- Unauthorized access to Service
- Security breaches in network
- Communication Information stealing
- Modification in Communication Information
- Virus or Malware Attack

4.1.3. Threats at Backend

- Modification in Database Algorithms
- Replacing Operators
- Compromising safety of Code Resources

4.2. Privacy Issues in IoT

Privacy of an entity or object can be defined as the degree to which it interacts and willing to share information about itself with others. There are number of privacy issues arise in IoT based systems which are categorized as per below:

4.2.1. Privacy of Device

The delicate data might be spilled out if there should arise an occurrence of unauthorized control or manipulation of equipment and programming in these devices.

4.2.2. Privacy of Data and Storage

If strong algorithm for data privacy is not implemented, the database or storage system could be compromised.

4.2.3. Privacy of Processing

Users and developers are provided with the restricted access and with effective access control mechanisms.

4.2.4. Privacy of Communication

Encryption and proper tracing methodologies should be applied in order to achieve privacy while communicating.

V. CONCLUSION

Demanded by our living style, the internet and its use changed and enhanced drastically. Devices are made smart and interconnected taking the benefits of technology for betterment in proffessional, personal and industrial environments. The IoT is a new era of technological benefits for betterment of society. Although, there are number of issues to be fixed and addressed with this emerging technology.

REFERENCES

[1] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." *Computer networks* 54.15 (2010): 2787-2805.
[2] Friess, Peter. *Internet of things: converging technologies for smart environments and integrated ecosystems*. River Publishers, 2013.
[3] http://www.pcquest.com/the-tech-behind-internet-things/.
[4] Klaus F., Giesecke & D. *RFID Handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication, third edition*. Wiley Publication, 2011.
[5] http://internetofthingswiki.com/iot-applications-examples/541/.
[6] https://iot-analytics.com/top-10-iot-project-application-areas-q3-2016/
[7] Kumar, J. Sathish, and Dhiren R. Patel. "A survey on internet of things: Security and privacy issues." *International Journal of Computer Applications*90.11 (2014).

