© 2017 IJSRSET | Volume 3 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

The Internet of Things – The Thing to Watch

Bharathi Anbarasan

Department of Computer Applications, Dr. NGP Arts and Science College, Coimbatore, India

ABSTRACT

The Internet of Things (IoT) has gained prominence over the last decade. The driver for the growing interest on this technology has been essentially the desire to add value to products or services.IoT is among the technologies which have high expectations and is expected to reach mainstream adoption in the next 5-10 years. The IoT can be visualized to comprise of a 4-layer architecture with the sensors and other monitoring devices being a key addition to conventional Internet networks. IoT has a wide ranging application potential impacting our daily lives, personal and related to the social community. There are the inevitable risks concerning security and privacy which has to be recognized and managed. With the requisite security controls, drop in costs and prevalence of devices, IoT is bound to give a totally new better way of life.

Keywords : Internet of Things; IoT; sensor networks; network devices; network security, future networks

I. INTRODUCTION

The next wave in the era of computing will be outside the boundaries of the traditional computers and their network, being called the Internet of today. Today, computers -- and, therefore, the Internet -- are almost wholly dependent on human beings for information. Nearly all of the data available on the internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a bar code.

The problem is, people have limited time, attention and accuracy - all of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things -- using data they gathered without any help from us -- we would be able to track and count everything and greatly reduce waste, loss and cost. This is essentially the concept of the 'Internet of Things (IOT)'.

The collection of such enormous amounts of data through collection devices and efficient processing of such data in a timely manner makes it possible to provide enormous benefits, not for any corporate entity but for the general members of the society like each one of us. It's a concept that has the potential to impact how we live and how we work.

We would know when things needed replacing, repairing or recalling and whether they were fresh or past their best. The benefits can be endless in several aspects of our life like healthcare, travel, education, office productivity, entertainment and several others.
"The "Internet of things" (IoT) is becoming an increasingly growing topic of conversation both in the workplace and outside of it.

What Is The Internet of Things?

The Internet of Things has been defined by several people in several different ways. An article by the University of Melbourne defines Internet of Things as an 'Interconnection of sensing and actuating devicesproviding the ability to share information acrossplatforms through a unified framework, developing a common operating picture for enabling innovative
applications'.

This is achieved by seamless large scalesensing, data analytics and information representationusing cutting edge universal sensing and cloudcomputing.Simply put,

this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig.

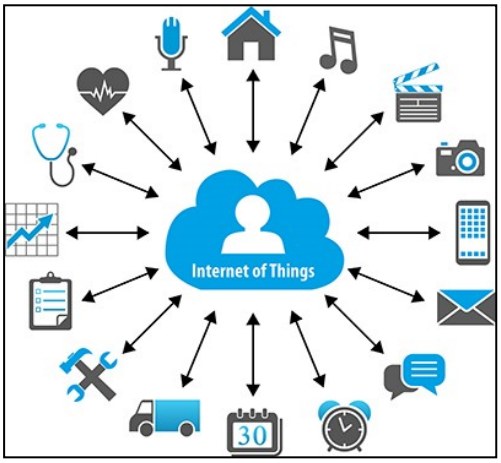

Figure 1. IoT - The Network of Connected 'Things'

The IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things.

The Outlook of IOT

IOT has been a buzzword for quite some time. Gartner Inc.'s Hype Cycle for Emerging Technologies, 2016specifically focuses on the set of technologies that is showing promise in delivering a high degree of competitive advantage over the next five to 10 years. It highlights the three overreaching technology trends likely to create new experiences - transparently immersive experiences, the perceptual smart machine age, and the platform revolution. IOT forms part of the platform revolution. The shift from technical infrastructure to ecosystem-enabling platforms is laying the foundations for entirely new business models that are forming the bridge between humans and technology.

As seen in Fig. 2, IOT is among the technologies that are very high in the hill of 'expectations' and is expected to hit mainstream adoption in a period of 5 to 10 years, delivering a high degree of competitive advantage.

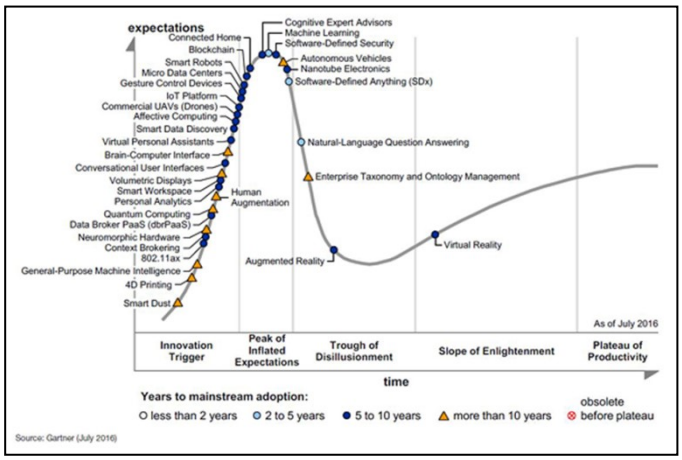

Figure 2. Gartner 2011 Hype Cycle of Emerging Technologies

The IoT Architecture

The typical architecture of IoT solutions is usually far more complex than the architecture of most enterprise systems. One of the main factors that increases the complexity of IoT systems is that backend services residing in the data center, which is the heart of most enterprise systems, are actually just a piece of the bigger IoT picture. With IoT solutions, we have to deal with a myriad of devices working in the field. The nature of these devices is very different from web, desktop, or even mobile clients.

The IOT architecture could be visualised in the form of a 4 layer architecture as depicted in Fig. 3.

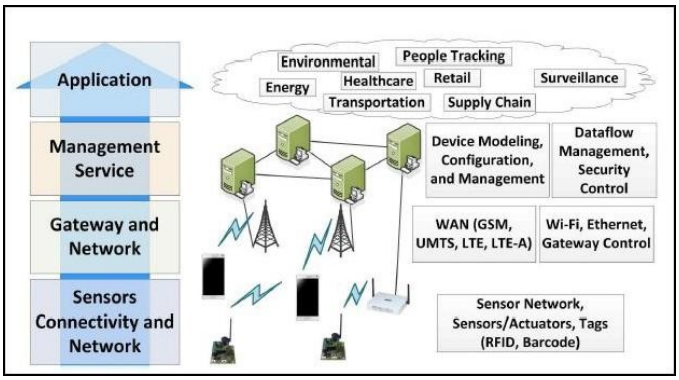

Figure 3. IOT Architecture Layers

There are four major layers. At the bottom, there's a sensor connectivity and network layer. On top of this is the gateway and network layer. Above this is the management service layer, layer three. And on top of it is the application layer. The service connectivity and network comprises of the sensor network, sensors, actuators, tags, which include RFID and barcodes, and

other types of tags as well. At the gateway and network layer, we have a wide area network, a mobile communication network, a Wi-Fi, Ethernet, gateway control and other similar network components. In the management service layer, device modelling configuring and management is a major focus. Dataflow management, security control needs to be provided at the management service layer. The constituents of the application layer include energy, environment, healthcare, transportation, supply chain, retail, people tracking, surveillance, and many, many more endless applications.

Fig.4 gives an example of a Cloud based architecture for the IoT.

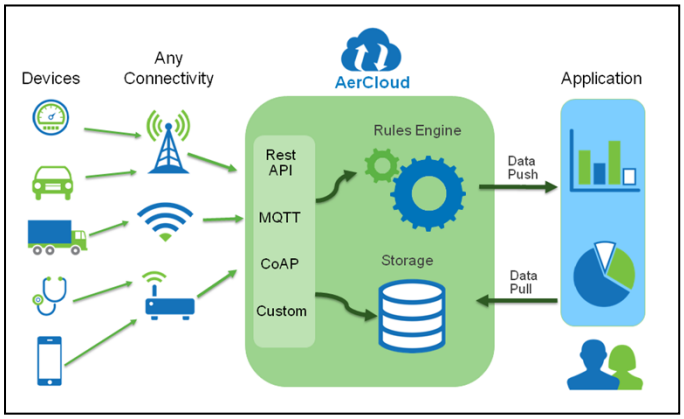

Figure 4. Cloud Based IOT Architecture from AerCloud

Potential Applications

There are several application domains which will beimpacted by the Internet of Things. Theapplications can be classified based on the type of networkavailability, coverage, scale, heterogeneity, repeatability,user involvement and mpact. Applications may be classified into four main domains: (1)Personal andHome; (2) Enterprise and Community; (3) Utilities; and (4) Transport and Logistics.

Fig 5 shows the different domains of applications and end users based on the data generated and consumed.

These application domains are, however, linked and dependant on one another, They are not isolated. For example, the Personal and Home IoT captures and generates electricityusage data in the house and makes it available to the electricity (utility) company which can in turn optimize the supply and demand in the Utility IoT. The Internet enables sharing of data between different service providers in a seamless manner creating multiple business opportunities.

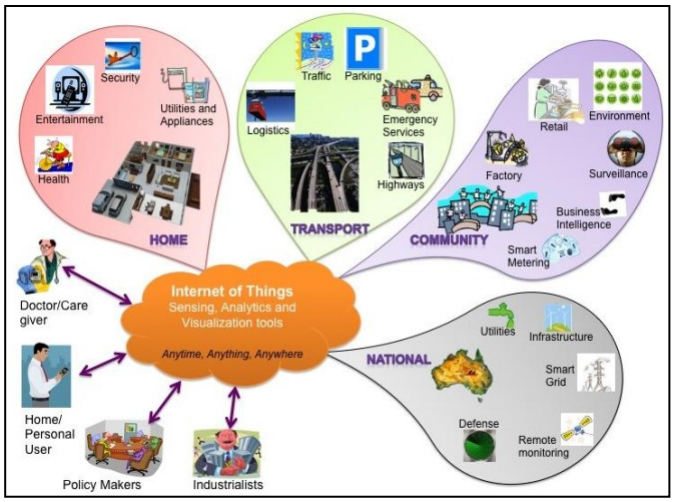

Figure 5. IoT End users and Application areas

A few typical applications in each of the domains are given below:

Personal and Home

In the personal and home environment, health care has always been envisioned as a potential area which can be benefited by the IoT technology. Already, there are several mobile applications for Android, Apple iOS and Windows operating systems which monitor several physiological parameters with the help of body level sensors. But these are just used at the localized level providing feedback to the user and are not yet connected to the external world. With the prevalence of Wifi and other powerful and inexpensive network connectivity, the collected data can be transmitted to a doctor for instantaneous assessment and feedback.

A critical use of such a facility is to maintain a home monitoring system for aged-care, whichallows the doctor to monitor patients and elderly in theirhomes thereby avoiding serious medical incidents involving them through earlyintervention and treatment and also reducing hospitalization costs.

Control of home equipment such as air conditioners, refrigerators, washing machines etc., will allow better home and energy management. Social networking is set toundergo another transformation with a huge increase in the number of interconnected objects. An interesting development could be using a Twitter like concept where individual 'Things' in the house can periodically

tweet the readingswhich can be easily followed from anywhere in the network.

With such a free flow information from an individual space to the outer world, appropriate security precautions are however essential which is discussed in the next section.

Enterprise and Community

Sensors have always been an integral part of a factory setup. Information collected through such devices are however used exclusively by the management of the enterprise and released selectively based on the situation needs. Environmental monitoring is a common application which is in use to keep track of the number of occupantsand manage the utilities within the building (e.g., HVAC,lighting). Other devices have also been sporadically used for collecting and managing data on security, automation, climate control, etc. These will eventually be replaced by wireless systems giving theflexibility to make changes to the setup whenever required, thus creating an IoT subnet dedicated to factorymaintenance.

One of the major IoT application areas which is already drawing attention is Smart Environment IoT. There are several testbeds being implemented and many more planned in the coming years around the world. The applications within the urban environment which can benefit from IoT are grouped in Table I.

TABLE I. POTENTIAL IOT APPLICATIONS

Citizens	
Healthcare	Patient monitoring, personnel monitoring, diseasespread modelling and containment - real-time healthstatus and predictive information to assist practitioners inthe field, or policy decisions in pandemic scenarios
Emergency services, defence	Remote personnel monitoring (health, location); resourcemanagement and distribution, response planning; sensorsbuilt into building infrastructure to guide first respondersin emergencies or disaster scenarios
Crowd monitoring	Crowd flow monitoring for emergency management; efficient use of public and retail spaces;
	workflow in commercial environments
Transport	
Traffic management	Intelligent transportation through real-time traffic information and path optimisation
Infrastructure monitoring	Sensors built into infrastructure to monitor structural fatigue and other maintenance; accident monitoring for incident management and emergency response coordination
Services	
Water	Water quality, leakage, usage, distribution, waste management
Building management	Temperature, humidity control, activity monitoring for energy usage management Ð Heating, Ventilation and Air Conditioning (HVAC)
Environment	Air pollution, noise monitoring, waterways, industry monitoring

Utilities

The information from the networks in this application domain are usually for service optimisation rather than consumer consumption. It is already being used by utility companies in several countries (smart meter by electricity supply companies)for resource management in order to optimise cost vs profit.

These are made up of very extensive networks (usually laid out by large organizations on regional and national scale) for monitoring critical utilities and efficient resource management. The backbone network used can vary between cellular, WiFi and satellite communication.

Efficient energy consumption can be achieved by continuously monitoring every electricity point within a house and using this information to modify the way electricity is consumed. This information at the city scale is used for maintaining the load balance within the grid ensuring high quality of service.

Video based IoTwhich integrates image processing, computer vision and networking frameworks will help develop a new challenging scientific research area at the intersection of video, infrared, microphone and network technologies. Surveillance, the most widely used camera network applications, helps track targets, identify suspicious activities, detect left luggage and monitorunauthorized access. In the future, this could be applied for Automatic behavior analysis and eventdetection (as part of sophisticated video analytics). Water network monitoring and quality assurance of drinking water is another critical application that can be addressed using IoT. Sensors measuring critical water parameters can be installed at important locations in order to ensure high supply quality. This avoids accidental contamination among storm water drains, drinking water and sewage disposal. The same network can be extended to monitor irrigation in agricultural land. The network is also extended for monitoring soil parameters which allows informed decision making about agriculture.

Transport and Logistics

Smart transportation and smart logistics require a totally different nature of data sharing andback bone implementation due to the continuous movement of the networking components, mainly the devices.

Urban traffic is the main contributor to traffic noise pollution and a major contributor to urban air quality degradation and greenhouse gas emissions. Traffic congestion directly imposes significant costs on economic and social activities in most cities. Supply chain efficiencies and productivity are severely impacted by this congestion causing freight delays and delivery schedule failures. Dynamic traffic information will affect freight movement, allow better planning and improved scheduling.

The transport IoT will enable the use of large scale WSNs for online monitoring of travel times, origin-destination (OD) route choice behavior, queue lengths and air pollutant and noise emissions. The IoT is likely to replace the traffic information provided by the existing sensor networks. Combined with information gathered from the urban traffic control system, valid and relevant information on traffic conditions can be presented to travelers.

IoT has penetrated widely in a number of digital products such as mobile phones, car hands-free sets, navigation systems, etc., a fact reflected by the prevalence of the Blue tooth technology devices. Blue tooth devices emit data with unique identification codes, which can be read by readers placed at several locations thus mapping the movement of the devices. Complemented by other datasources such as traffic signals, or bus GPS, researchproblems that can be addressed including vehicle travel time on highway and other main roads.

Efficient logistics management is another important area in this domain which can benefit from the use of IoT. This includes monitoring the items being transported as well as efficient transportation planning. The monitoring of items is carried out more locally, say, within a truck but transport planning is carried out using a large-scale IoT network.

II. SECURITY, PRIVACY AND SAFETY

The Internet of Things (IoT) presents numerous benefits to consumers, and has the potential to change the ways that consumers interact with technology in fundamental ways. In the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. IoT devices are poised to become more pervasive in our lives than mobile phones and will have access to the most sensitive personal data such as identity numbers and banking information. As the number of connections are also exponentially multiplied, a couple of security concerns on a single device such as a mobile phone can quickly turn to 50 or 60 concerns when considering multiple IoT devices in an interconnected home or business. In light of the importance of what IoT devices have access to, it's important to understand their security risk.

Security

The IoT will have critical infrastructure components and hence it presents a good target for national and industrial espionage, as well as denial of service and other attacks.

Privacy

With the IOT, a lot of personal information is going to reside on networks which is a likely target for criminals.

Safety

Many things are connected to the Internet now, and we will see an increase in this with time. Enormous data gets shared and machine actions will be automated based on that information, This may lead to very physical threats, around national infrastructure, possessions [for example, cars and homes], environment, power, water and food supply, etc.

We should understand that IOT is still a Work in Progress and hence till the technology acquires a maturity with adequate security built around all the devices and information, the threats are real.

There have been some serious recent reports of security breaches involving such devices. There have been reports of researchers hacking into cars and wirelessly disabled the brakes, turned the lights off and switched the accelerators full on – all beyond the control of the driver. In another case, a luxury yacht was lured off course through a hack of the GPS signal used for navigation.

In a home environment attackers can tamper with heatng, lighting, power and door lock.

While threats will always exist with the IoT as they do with other technology endeavors, it is possible to bolster the security of IoT environments using security tools such as data encryption, strong user authentication, resilient coding and standardized and tested APIs that react in a predictable manner.Security needs to be built in as the foundation of IoT systems, with rigorous validity checks, authentication, data verification, and all the data needs to be encrypted

III. CONCLUSION

Devices capable of acquisition, communication as well as actuation provides a plethora of additional information sources creating a new Internet – the Internet of Things. In the future, technology is not likely to be a limitation and the usability of data is totally dependent on the creativity and resourcefulness of application developers. There is also no shortage of need to improve the quality of living and consequently IoT should develop into the main solution source meeting such needs.

It is however imperative that adequate security provisions are built into the systems thereby ensuring that there is no compromise on the security and privacy of an individual and the society in large. The outlook of such a totally secure connected network improving our way of life and work is quite exciting and deserves pursuance.

IV. REFERENCES

[1] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic,Marimuthu Palaniswami, “Internet of Things (IoT): A Vision, Architectural Elements, andFuture Directions”, Future Generation Computer Systems, Vol 29 Iss 7, Sept 2013

[2] Gartner Inc. “Hype Cycle for Emerging Technologies”, Special Report, 2016

[3] Ahmed Banafa, “Internet of Things (IoT): Security, Privacy and Safety”, Datafloq Article, datafloq.com,

[4] Internet Society, “The Internet of Things (IoT): An Overview”, Whitepaper, 2015

[5] Jacob Morgan, “A Simple explanation of the Internet of Things”, Forbes Article, 2014

[6] “AerCloud™ – M2M Cloud Platform / IoT Platform”, www.aeris.com

[7] Henryk Konsek, “The Architecture of IOT Gateways”, www.dzone.com, 2015