International Journal of Advanced Research and Development
ISSN: 2455-4030
Impact Factor: RJIF 5.24
www.advancedjournal.com
Volume 3; Issue 2; March 2018; Page No. 1238-1241

Internet of Things (IoT): Challenges and future directions

Anil Kumar
Assistant Professor, Department of Computer Science, University College, Kurukshetra University, Kurukshetra, Haryana, India

Abstract
The growth potential for the surrounded industry is enormous. And the way forward is becoming clearer day by day. It‘s time that we start building IoT systems, and provide value to our customers. The IoT is expected to connect 29 of billion “things” to the internet by 2021, range from wearable devices such as smart watches to automobiles, appliances, and industrial equipment. In this paper, we will take a look at different IoT solutions developed so far, their functionalities and technology used and thus conclude the various challenges to be focused on to give way to better solutions that will help the community.

Keywords: MANETs, IoT, RFID, WSN

1. Introduction
The term of Internet of Things (IoT) was first invented in 1998 which is a network of networks where typically, a large number of objects or sensors are connected through communications and information infrastructure to provide value-added services. It guaranteed in creating a world where all things and objects around us are connected to the internet and therefore the communication to each other with minimal human interference. The ultimate aim is to create a better world for human beings, where the objects around us understand our desire and hence act accordingly without any explicit instructions.
According to another definition, The Internet of Things (IoT) has been defined in a variety of ways. Generally Speaking, it refers to a global, distributed network (or networks) of physical objects that are capable of sensing or acting on their environment, and able to communicate with each other, other machines or computers. 'Smart' objects of large range of capacities and sizes which is including simple objects with implanted sensors, household Appliances, industrial robots, cars, trains, and wearable objects such as watches, Bracelets or shirts.
All these things have certainly changed the entire look of the word 'connectivity'. Internet of Things is highly on the rise and it can be observed from the areas that are completely under its effect. From smart cities, environment, health, energy, vehicle, transport, public safety to our daily essentials, Internet of Things has completely revitalized these areas.

2. Functionality of IoT Solutions
Sometimes IoT is understood as creature synonymous with smart systems: smart wearable, smart homes, smart city, smart environment, and smart enterprises and so on.
This Section discusses the functionality review of IoT solution available in different sectors.

2.1 Smart Wearable
Smart wearable are networked devices that can collect data, track activities, and customize experiences to users, needs and desires. Wearable solutions are designed for a variety of functions as well as for where on a different of part of body such as the head, eyes, wrist, waist, hands, fingers, legs or embedded into different element of attire. Wearable devices can be classified according to two standards. One standard is based on product forms, including head- mounted (such as glass and helmet), body-dressed (such as coat, underwear, and trousers), hand-worn (such as watch, bracelet, and gloves), and foot-worn (such as shoes and socks). Another standard is based on product functions, including healthy living (such as sport wristband and smart bracelet), information consulting (such as smart glass and smart watch), and somatosensory control (such as somatosensory controller).

2.2 Smart Home
Smart Home is the integration of technology and services through home networking for a better quality of living. A IoT technologies related to Smart Home are emerging [6]. In this category the solutions make the experience of existing things at home more convenient and pleasant for the occupants. Some smart home solutions also focus on assisting elderly Hand (Gloves), Finger (Rings), Wrist (Watch/ Bands), Eyes (Glasses), Legs (Socks), Foot (Shoes), Head (Helmet), Body (Cloth), Waist (Band), Chest (Band) people in their daily activities and on health care monitoring. According to large market potential, more and smarter home solutions are making their way into the market. From the academic point of view, smart energy and resource management, human-system interaction, and activity management have been some of the major focus.

2.3 Smart City
It is a built-up region that is highly developed in terms of overall infrastructure, sustainable real estate, communications and market viability. It is a city where information technology is the principal infrastructure and the basis for providing essential services to residents. There are many technological

platforms involved, including but not limited to automated sensor networks and data centers. Despite the fact that this may sound futuristic, it is now likely to become a reality as the smart cities association unfolds. Urban IoTs, in fact, are designed to support the Smart City vision, which aims at exploiting the most advanced communication technologies to support added-value services for the administration of the city and for the citizens. Uses of IoT standard to an urban context is of particular interest, as it responds to the strong drive of many national governments to adopt ICT solutions in the management of public affairs, thus realizing the so- called Smart City concept.

2.4 Smart Environment

The Smart Environment in a city comprises of Smart Governance, Smart Mobility, Smart Utilities, Smart Buildings. Services enabled by the IoT paradigm in smart city environment might ranges from Monitoring health building, Management of waste, Monitoring air quality, Monitoring noise, Traffic congestion, smart parking, smart lightning, water quality monitoring, natural disaster monitoring, smart farming and many more.

2.5 Smart venture

Venture of IoT solutions are designed to support infrastructure and more general purpose functionalities in industrial place. Current venture strategies already acknowledge a few interfaces to smart items, but with increased computational and communication capabilities of these items, the power shifts towards the edges of the network. Intelligent mechanisms for data aggregation, filtering, fusion and conversion can be deployed to and executed at the network edge, or within the network, as appropriate. Software is already the key innovation driver in many industries and many new business models of the future will heavily rely on the use of such items. We see with the expanded definition of the Internet of Things many other interesting application domains. Some of the most promising ones are Manufacturing, supply chain integrity, energy and production, health, transportation and logistics.

3. Technical backbone

There are three IoT components which enable seamless pervasive computing: a) Hardware made up of sensors, actuators and embedded communication hardware b) Middleware - on demand storage and computing tools for data analytic and c) Presentation- novel easy to understand visualization and analysis of tools which can be widely accessed on different platforms and which can be designed for different applications. The IoT covers a huge scope of industries and applications.

This Section focuses on some of the technologies that are driving the IoT, from popular communication options to the different software and data brokerage platforms managing the data exhaust from these systems.

3.1 Radio Frequency Identification (RFID)

A radio-frequency identification system uses tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response. The researchers generally convey their observations to a computer system running RFID software or RFID middleware. RFID tags can be either passive, active or battery assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery assisted passive has a micro scale battery on board and is activated when in the presence of a RFID reader.

3.2 Wireless Sensor Network (WSN)

A wireless sensor network (WSN) is a collection of distributed sensors that monitor physical or environmental conditions, such as temperature, sound, and pressure. Data from each sensor passes through the network node-to-node. The components that make up the WSN monitoring network include: WSN nodes are low cost devices, so they can be deployed in high volume. The nodes are also operate at low power so that they can run on battery, or even use energy harvesting. A WSN node is an embedded system that typically performs a single function (such as measuring temperature or pressure, or turning on a light or a motor). The edge node of Wireless Sensor Network is a WSN node that includes connectivity of Internet Protocol (IP). It acts as a gateway between the WSN and the IP network. It can also perform local processing, provide local storage, and can have a user interface.

WSN Technologies: There are multiple candidates that can be selected as WSN technologies. Few of them are discussed here. Wi-Fi:-The first obvious networking technology candidate for an IoT device is Wi-Fi, because it is so ubiquitous. Certainly, Wi-Fi can be a good solution for many applications. Almost every house that has an Internet connection has a Wi-Fi router. However, Wi-Fi needs a fair amount of power. The level of power can't be afford by many devices such as battery operated devices for example sensors positioned in locations that are difficult to power from the grid. IEEE 802.15.4:- One of the major IoT enablers is the IEEE 802.15.4 radio standard, released in 2003. Commercial radios meeting this standard provide the basis for low-power systems. This IEEE standard was improved in 2006 and 2011 with the 15.4e and 15.4g amendments. Power consumption of commercial RF devices is now cut in half compared to only a few years ago, and we are expecting another 50% reduction with the next generation of devices.

3.3 Addressing Scheme

The ability to uniquely identify Things is critical for the success of IoT. This will not only allow us to uniquely identify billions of devices but also to control remote devices through the Internet. Most critical features of creating a unique address are: reliability, persistence, uniqueness and scalability. Every element that is already connected and those that are going to be connected must be identified by their unique identification, location and functionalities. The present IPv4 may support to a point where a group of cohabiting sensor devices can be geographically identified, but not individually. The Internet Mobility attributes in the IPV6 may alleviate some of the device identification problems; however, the heterogeneous nature of wireless nodes, variable data types concurrent operations and confluence of data from devices exacerbates the problem further IPv6‘s addressing scheme provides more addresses than there are grains of sand on earth some have calculated that it could be as high as 1030 addresses per person (compare that number to the fact that there are 1028 atoms in a human body). For an IoT device it is much simpler with IPv6 to obtain a global IP address, which enables efficient peer-to-peer communication.

3.4 Data Storage & Analytics

One challenge is that this highly measured world will create data at an astonishing rate, even if not all the data is or ever will be interesting or valuable. Ownership, storage and the expiry of the data become critical issues. Hence data centers which run on harvested energy and which are centralized will ensure energy efficiency as well as reliability. The data are stored and used intelligently for smart monitoring and actuation. The initial value in an IoT system is in the ability to perform analytics on the data which is to be acquired and extract helpful insights.

4. Challenges in developing IoT

This section discusses some of the major challenges that need to be addressed in order to build the IoT. The solutions for these issues need to be come from technological, social, legal, financial, and business backgrounds in order to receive wide acceptance by the IoT community.

4.1 Standards and interoperability

Standards are important in creating markets for new technologies. If devices from different manufacturers do not use the same standards, interoperability will be more difficult, requiring extra gateways to translate from one standard to another. In addition, a company that controls different parts of a vertical market (e.g. the acquisition of data, its integration with other data streams, and the use of those data streams to come up with innovative solutions or to provide services) may dominate a market, stifling competition and creating barriers for smaller players and entrepreneurs. Differing data standards can also tend to lock consumers into one family of products: if consumers cannot easily transfer their data when they replace one device with another from a different manufacturer, they will in effect drop to any benefit from data they have been accumulate over time.

4.2 Security

As the IoT connects more devices together, it provides more decentralized entry points for malware. Less expensive devices that are in physically compromised locales are more subject to tampering. Many layers of software, APIs, integration middleware, one machine to another machine communication, etc. create more complexity and new security risks. Expect to see many different techniques and vendors addressing these issues with policy-driven approaches to security and provisioning.

4.3 Privacy and Trust

With the help of remote sensors and monitoring a core use case for the IoT, there will be heightened sensitivity to controlling access and ownership of data. (Note that two latest new securities breach at Target and Home Depot, both were achieved by going through 3rd party vendors‘stolen credentials to gain access to payment systems. Partner vetting will become ever more critical.) Compliance will continue to be a major issue in medical and assisted-living applications, which could have life and death ramifications. Latest observance frameworks to the address of IoT’s unique issues will develop. Social and political concerns in this area may also hinder IoT adoption.

4.4 Confusion, complexity and integration issues

With multiple platforms, frequent protocols and large numbers of APIs, IoT systems integration and testing will be a challenge to say the least. The uncertainty around developing standards is almost sure to slow adoption. The rapid evolution of APIs will likely consume unanticipated development resources that will diminish project team’s abilities to add core new functionality. Slower acceptance and unexpected development resource necessities will likely slip schedules and slow time to revenues, which will require additional funding for IoT projects and longer runways for startups.

5. Conclusions

The potential of the IoT appears to be great, despite the range of issues that need to be addressed. This paper has sought to highlight the IoT concept in general through the four sections namely; section I, reviewed an overview about the IoT concept. Section II reviewed a set of the popular applications which are offered by IoT namely in the domain of Smart Homes, Smart Wearable, Smart Environment, Smart Enterprises. Section-III focuses on technical backbone for the realization of IoT. Section-IV and V reviewed a set of challenges faced and future impact of Internet of things. Based on above, It can be considered that new research problems arise due to the large scale of devices, the connection of the physical and internet of the systems of systems, and continuing problems of privacy and security.

6. References

1. Perera C, Member C, Harold Liu, Jayawardena S. The Emerging Internet of Things Market place from an Industrial Perspective: A Survey.
2. Zanella A, Bui N, Castellani, A, Vangelista L, EZorzi M, Internet of Things For Smart Cities Ieee Internet of Things Journal, 2014; 1(1).
3. Rajguru S, Kinhekar S, Pati S. Analysis of Internet of Thing sina Smart Environment. 2015; 4(4):40-43). Availableonlineat: www.erpublications.com
4. Air Quality Egg. Air Quality Egg, 2013. Retrieved From. http://airqualityegg.com/
5. Amrita Vishwa Vidya Peetham. Amritawna: Amrita center for wireless networks and applications,2013.
6. Saini Anil, Nath Rajender. Performance Evaluation of AODV, DSR and DSDV Protocols Based On Network Size & Density of Nodes, International Research Journal of Engineering and Technology (IRJET), 2016; 3(7):1367-1372.

7. Saini A, Nath R. Performance Evaluation of AODV and DSR Routing Protocol on Varying Speed and Pause Time in Mobile Ad Hoc Networks. In: Lobiyal D., Mansotra V., Singh U. (eds) Next-Generation Networks. Advances in Intelligent Systems and Computing, Springer, Singapore, 2018, 638.
8. Dr. Upadhyaya S, Saini A. Improving the Quality of CGSR Routing Protocol by Electing Suitable Cluster head Using Fuzzy Logic System in MANET, IJARCSSE, 2013, 369-375.
9. Saini A, Vinod K. Mobile ad -hoc network routing protocols: Comparative study. International Journal of Enhanced Research in Science Technology and Engineering. 2013; 3(12):57-62.