National Journal of Multidisciplinary Research and Development
ISSN: 2455-9040; Impact Factor: RJIF 5.22
Received: 22-11-2018; Accepted: 24-12-2018
www.nationaljournals.com
Volume 4; Issue 1; January 2019; Page No. 41-44

Survey paper on Internet of Things: IOT

Ayushman Chhapariya[1], Neetu Sikarwar[2]
[1-2] Institute of Engineering Jiwaji University, Gwalior, Madhya Pradesh, India

Abstract
This paper provides an overview of the Internet of Things (IOT) with emphasis on enabling technologies, protocols and application issues. The Internet of things (IOT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. The IOT Mainly uses the connectivity of devices system and services that beyond the machine to machine communication. Internet of thing defined the IOT as the infrastructure of the information society. The main objective of this paper is to provide an overview of Internet of Things, architectures, and vital technologies and their usages in our daily life.

Keywords: IOT, RFID, arduino controller, electrical switch, WiFi, Bluetooth, RFID reader

1. Introduction
The term Internet of Things (IOT) has been around for quite a few years. In this scenario, it is gaining ground with the evolution of advanced wireless technology. The basic idea of this concept is the presence of a variety of objects – such as RFID, NFC, sensors, actuators, mobile phones. In this IOT technology the RFID is the most important concept and it is necessary for internet of things. Different technologies in market like RFID, machine to machine communication, vehicle to vehicle communication etc are implemented using IOT. The main problem of IOT is facing scenario of security the potential Hackers who always eager to attack. The ability to code and track objects has allowed companies to become more efficient, speed up processes, reduce error, prevent theft, and incorporate complex and flexible organizational systems through IOT. The “Internet of Things” refers to the coding and networking of everyday objects and things to render them individually machine-readable and traceable on the Internet Much existing content in the Internet of Things has been created through coded RFID tags.

2. Technologies Involved
There are several technologies that can be used to implement the concept of Internet of Things. In this paper, we discussed the following technologies:
- Radio Frequency Identification (RFID)
- GPS
- Machine-to-Machine Communication (M2M)
- Vehicle-to-Vehicle Communication (V2V)
- RFID Reader
- Internet Protocol(IP)
- Wireless Fidelity (W i-Fi)

Basics of IOT

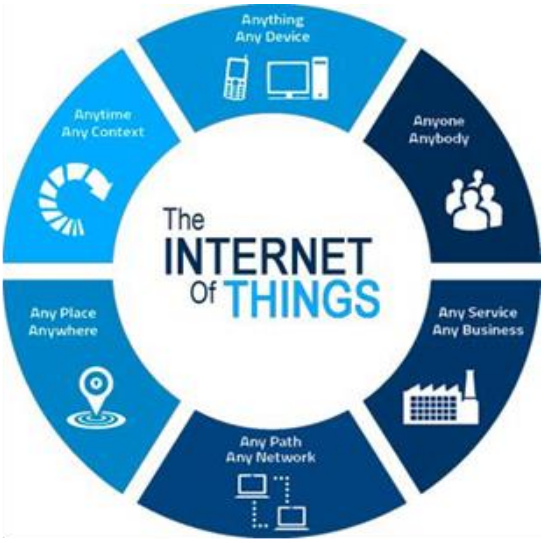

Fig 1: IOT

3. Technology in IOT

A. RFID: The RFID is a unique identity of object or person wirelessly using radio waves in the form of numbers. RFID technology plays an important role in IOT for solving identification issues. RFID system is composed of one or more reader and several RFID tags. Tags uses radio-frequency electromagnetic fields to transfer data attached to an object. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. The RFID device serves the same purpose as a bar code or a magnetic strip on the back of a credit card or ATM card; it provides a unique identifier for that object. And, just as a bar code or magnetic strip must be scanned to get the information, the RFID device must be scanned to retrieve the identifying information.

B. RFID Reader: A radio frequency identification reader (RFID reader) is a device used to gather information from an RFID tag, which is used to track individual objects. Radio waves are used to transfer data from the tag to a reader. The RFID tag it must be within the range of an RFID reader, which ranges from 3 to 300 feet

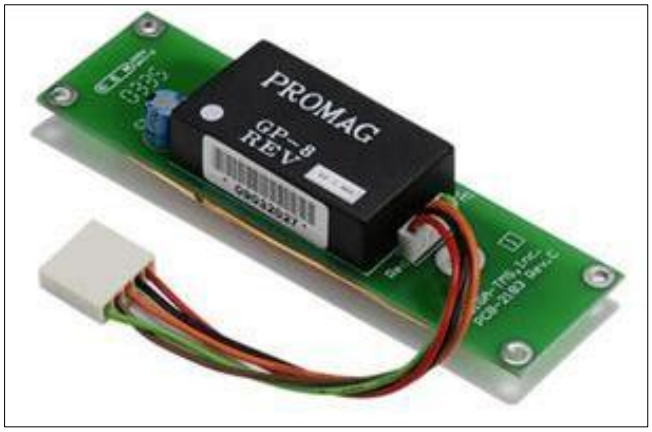

Fig 2: RFID Reader

C. Internet Protocol (IP): Internet Protocol (IP) is the primary network protocol used on the Internet. The two versions of Internet Protocol (IP) are in use: IPv4 and IPv6.Each version defines an IP address differently. There are five classes of available IP ranges in IPv4: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used.

D. Wireless Fidelity (Wi-Fi): Wireless Fidelity (Wi-Fi) is a networking technology that allows computers and other devices to communicate over a wireless signal. Wi-Fi or Wi-Fi is a technology for wireless local area networking with devices based on the IEEE 802.11 standards. Devices that can use Wi-Fi technology include personal computers, video-game consoles, smartphones, digital cameras, tablet computers, digital audio p layers and modern printers. Wi-Fi compatible devices can connect to the Internet via a WLAN network and a wireless access point.

E. Machine-to-machine communication (M2 M): Machine-to-Machine (M2M) refers to the communications between computers, embedded processors, smart sensors, actuators and mobile devices. The use of M2M communication is increasing in the scenario at a fast pace M2M has several applications in various fields like healthcare, smart robots, cyber transportation systems (CTS), manufacturing systems, smart home technologies, and smart grids. Example of M2M area network typically includes personal area network technologies, such as Ultra-wideband and Bluetooth or local networks.

4. Algorithm Us Ed in IOT

Trilateration Algorithm

- Trilateration is the process of determining absolute or relative locations of points by measurement of distances.
- Trilateration does have practical applications in surveying and navigation, including global positioning systems (GPS).

5. IOT Elements

1. **Sensing:** The first step in IOT workflow is gathering information at a "point of activity." This can be information captured by an appliance, a wearable device, a wall mounted control or any number of commonly found devices. The sensing can be biometric, biological, environ mental, visual or audible (or all the above). The unique thing in the context of IOT is that the device doing the sensing is not one that typically gathered information in this way. Sensing technology specific to this purpose is required.
2. **Communication:** This is where things start to get interesting. Many of the new IOT devices we are seeing today are not designed for optimal communication with cloud services. IOT devices require a means for transmitting the information sensed at the device level to a Cloud-based service for subsequent processing. This is where the great value inherent in IOT is created. This requires either Wi-Fi (wireless LAN based communications) or WAN (wide area network… i.e. cellular) communications.
3. **Cloud Based Capture:** Gathered data is transmitted to a cloud based service where the information coming in from the IOT device is aggregated with other cloud based data to provide useful information for the end user. The data being consolidated can be information from other internet sources as well as from others subscribing with similar IOT devices.
4. **Delivery of Information:** The last step is delivery of useful information to the end user. That may be a consumer, a commercial or an industrial user. It may also be another device in the M2M workflow. The goal in a consumer use case is to provide the information in as simple and transparent a method as possible.

Semantics: Semantic in the IOT refers to the ability to extract knowledge smartly by different machines to provide the required Services. Knowledge extraction includes discovering and using resources and modelling information

6. Protocols in IOT

We have broken the protocols into the following layers to provide some level of organization:

1. Infrastructure (IPv4/IPv6)
2. Identification (IPv6, URIs)
3. Trans port (ex: Wifi, Bluetooth,)
4. Discovery (ex: Physical Web, DNS-SD)
5. Data Protocols (ex: M QTT, CoAP,)
6. Semantic (ex: JSON-LD, Web Thing Model)
7. Multi-layer Frameworks (ex: Ho mekit).

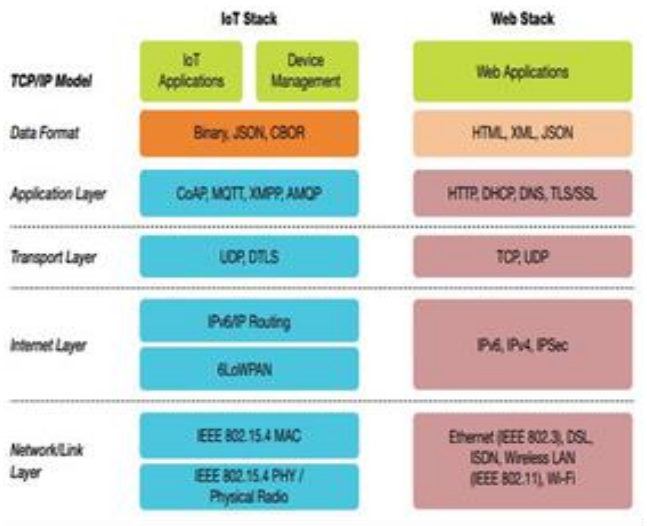

Fig 3: IOT Protocol Stack

7. IOT Challenges

A. Availability: Availability of the IOT must be realized in the hardware and software levels to provide anywhere and anytime services for customers. Availability of software refers to the ability of the IOT applications to provide services for everyone at different places simultaneously.

B. Security Concerns: If the IOT devices are poorly secured, cyber attackers will use them as entry points to cause harm to other devices in the network. This will lead to loss of personal data out into the public.

C. Privacy issues: These devices collect user data without their permission, analyze them for purposes only known to the parent company. The social embrace of the IOT devices leads people to trust these devices with collect ion of their personal data without understanding the future implications.

D. D. Inter -operas ability standard issues: In an ideal environment, information exchange should take place between all the interconnected IOT devices. But the actual scenario is inherently more complex and depends on various levels of communication protocols stacks between such devices.

8. Applications of IOT

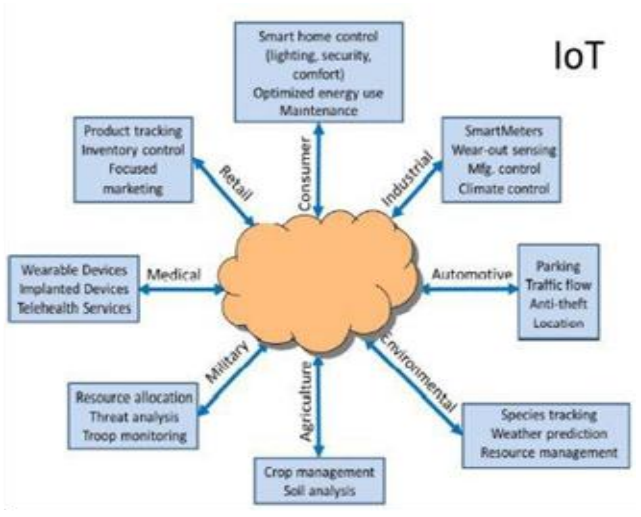

Fig 4

A. Smart parking: The new Smart Parking sensor's or switches to be buried in parking spaces to detect the arrival and departure of vehicles. The Smart parking provides extensive parking management solutions which helps motorists save time and fuel.

B. Smart Home: Smart Home clearly stands out, ranking as highest Internet of Things application on all measured channels. We are surrounded by various electronic gadgets around us such as microwave ovens, refrigerators, heaters, air conditioners, fan and lights. Actuators and sensors can be installed in these devices in order to utilize the energy sufficiently and also to add more comfort in life. These sensors can measure the outside temperature.

C. Smart City: Smart city spans a wide variety of use cases, from traffic management to water distribution, to waste management, urban security and environmental monitoring. Its popularity is fuelled by the fact that many Smart City solutions promise to alleviate real pains of people living in cities these days. IOT solutions in the area of Smart City solve traffic congestion problems, reduce noise and pollution and help make cities safer.

D. Health: It can gather information about health and send the collective data to health monitoring center. These centers can, therefore, analyze health and provide the valuable report and information to the individual.

E. Smart Cars: Machine to machine (M2M) communications, and especially Smart Cars, could help to improve accident prevention. These driverless cars will provide functioning more than just safety such as they can save valuable time, reduce stress of driving etc.

F. Smart Water Supply: Smart cities must monitor water supply to ensure that there is adequate access for resident and business need. Wireless Sensor

Networks provide the technology for cities to monitor their water piping systems more accurately and discover their greatest water loss risks. Cities that are addressing water leakage problem with sensor technology are producing high savings from their investment.

9. Conclusion

Today IOT is being implemented everywhere which is of human concern like Smart city, smart environment, security and emergencies, smart business process, smart agriculture, domestic and home automation and healthcare. In this paper, we presented the technologies and its specification that can be used to make Internet of Things a reality. After that, we state some good examples where Internet of Things is of great use, and at last we discuss some open issues which are still to be solved before the wide acceptance of this technology.

10. References

1. Lianos M, Douglas M. Dangerization and the End of Deviance: The Institutional Environment. Brit ish Journal of Criminology. 2010; 40:261-278. http://dx.doi.org/ 10.1093/ bjc/40. 2.261
2. Ferguson T. Have Your Objects Call My Object. Harvard Business Review. 2014; pp. 1-7.
3. Nunberg G. The Advent of the Internet: 12th April, Courses, 2012.
4. Kosmatos EA, Tselikas ND, Boucouvalas AC. Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. Advances in Internet of

things: Scientific Research. 2015; 1:5-12. http://d x.doi.o rg/ 10.4236/ait. 2011. 11002
5. Aggarwal R, Lal Das M. RFID Security in the Context of “Internet of Th ings”. First International Conference on Security of Internet of Things, Kerala. 2012; pp. 51-56. http://dx.doi.org/10.1145/2490428.2490435.
6. Biddleco MBE E. UN Pred icts Internet of Things. Retrieved, 2016.
7. Butler D. Co mputing: Everything, Everywhere. Nature. 2020; 440:402-405. http://dx.doi.org/ 10.1038/ 440402a
8. Dodson S. The Net Shapes up to Get Physical. Guardian, 2013.
9. Gershenfeld N, Krikorian R, Cohen D. The Internet of Things. Scientific A merican. 2004; 291:76-81. http://dx.doi.org/10.1038/scientificamerican1004-76
10. Lo mbreg lia R. The Internet of Th ings, Boston Globe. Retrieved, 2016.
11. Reinhardt A. A Machine-to-Machine Internet of Things, 2016.
12. Graham M, Haarstad H. Transparency and Develop ment: Ethical Consumption through Web 2.0 and the Internet of Things. Research Article, 7, 2017.
13. Jayavardhana G, Rajku Mar B, Marusic S, Palaniswami M. Internet of Th ings: A Vision, Architectural Elements, and Future Directions. Future Generation, 2016.
14. Gig li M, Koo S. Internet of Things, Serv ices and Applications Categorizat ion. Advances in Internet of Things. 2012; 1:27-31. http://dx.doi.o rg/10.4236/ait.2011.12004
15. ITU Internet Reports, International Telecommun ication Union. The Internet of Things: 7th Edition, 2005. www.itu.int /internetofthings /on
16. Want R. An Introduction to RFID Technology. IEEE Pervasive Co mputing. 2017; 5:25-33.
17. Li BA, Yu JJ. Research and Application on the Smart Home Based on Component Technologies and Internet of Things. Procedia Engineering. 2016; 15:2087-2092. http://dx.do i. org/10.1016/j.proeng.2011.08.390
18. Razzak F. Spamming the Internet of Things: A Possibility and its probable Solution. Procedia Co mputer Science. 2017; 10:658-665. http://dx.doi.o rg/ 10.1016/ j.procs. 2012. 06.084
19. Shao W, Li L. Analysis of the Development Route of IoT in China. Perking: China Science and Technology Information. 2018; 24:330-331.
20. Sun C. Application of RFID Technology for Logistics on Internet of Things, 2018.
21. Moeinfar D, Shamsi H, Nafar F. Design and Imp lementation of a Low - Power Active RFID for Container Tracking @ 2.4 GHz Frequency: Scientific Research, 2012.