iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IV **Month of publication:** April 2020

DOI: http://doi.org/10.22214/ijraset.2020.4044

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

Internet of Things (IoT): A Review of Enabling Technologies, Challenges and Open Research Issues

Bedford-Fubara Chioma[1], Onuodu Eleonu Friday[2]
[1]*Department of Computer Science, Ignatius Ajuru University of Education, Nigeria.*
[2]*Department of Computer Science, University of Port Harcourt, Nigeria.*

Abstract: ***The creation and introduction of the Internet to the world in the mid 90's has played a huge role in impacting the way we live. It cannot go unnoticed that presently the world is evolving and at a fast pace. This evolution can be seen when we look at the way we do some basic activities now compared to how they were done before. From the way we work, our manner of driving and even the process of making purchases have evolved into easier methods. This is as a result of the Internet of Things. The Internet previously used to be about people networking between and among people but it has now transcended into things networking between and among people or other things. In other words, we can refer to the context of the Internet as a relationship or connection between people to people, people to things and things to things. Highly developed chips and sensors that carry valuable data are embedded in almost every tangible thing that surround us. This study aims at reviewing the various technologies that enable the Internet of Things, the challenges they are likely to face and suggest research issues.***
Keywords: ***Internet of Things, Zigbee, RFID, Near Field Communication, Machine-to-Machine Communication.***

I. INTRODUCTION

A typical IoT consists mainly of numerous Radio-Frequency Identification (RFID) devices and Wireless Sensors Networks (WSN). Giving a scenario where Mr. A is taking a long road trip to another city in his car. After driving a few kilometres, he notices that the 'check' light signal has come up on his dashboard. He knows that he has to get his car checked by a mechanic but is not sure if it is an emergency or something trivial that could be dealt with at a later time. It happens that the sensor that prompted Mr. A's check light signal to come on also monitors his oil gauge. His car has alerted him that the oil level in his car is low and he needs to service his car. This sensor is one of many other sensors present in a car that communicate with each other. The data from all these sensors are gathered by an element of the car called the diagnostic bus which transmits the data to a gateway in the car. It is the duty of the gateway to organize the data collected from these sensors, transmitting only relevant information to the manufacturer's platform. The manufacturer's platform is governed by rules and logic that send a signal to Mr. A's car when his car oil level is low; this signal is what triggers the 'check' sign to come on in Mr. A's car. All of this is only possible if the car gateway and manufacturer's platform have registered with each other and establish a secure communication network. The manufacturer's platform constantly gathers and stores several bits of information from Mr. A's car and many other cars they have manufactured creating an archive of records in a secure database. The result is a better asset and inventory management for the manufacturer or car dealer and a safe ride for Mr. A to his destination.

The next big wave in smart technology is Voice Control in cars. Big car manufacturing companies are vying for premium space in our cars so as to provide us with infotainment systems. Thanks to the Internet of Things.

So whether we want to order an item from Amazon, the government notifying its citizens of real time update on train or bus schedules (as practiced in the United Kingdom), or we want to monitor our personal health; say blood pressure, we make use of devices that communicate with each other. Although all these devices (things) work and interoperate by receiving data from the Internet of Things platform, how exactly are they are able to share huge volume of data? How do they put the information generated to work?

Digital Signal Processors is the heart of most smart systems. Presently, Apple Homekit (Siri), Samsung Bixby, Google Home, Microsoft Cortana and Alexa are voice assistant applications that are commonly used. Users expect a highly intuitive and efficient design from their smart objects; hence simplicity is compulsory with any technology or digital object. At the moment, Alexa has the most compatibility with many devices but that could change in a short span of time because of the high competition among VAA manufacturers. An interesting point worthy of note is that voice assistants are now heading towards playing the hub roll too. Presently, Amazon Echo Plus and Show both offer Zigbee hubs. Hopefully they should be able to move into other protocols as well.

The name Zigbee was derived from the waggle dance of honey bees after their return to the beehive (Gislason, 2010). Zigbee communication technology is specifically built for control and sensor networks on IEEE 802.15.4 standard wireless personal area networks (WPANs). This communication standard is distinguished by its physical and Media Access Control (MAC) layers that enables it to handle many devices at low data rates.

II. LITERATURE REVIEW

Internet of Things is one of the "in things" in Computer Science and Information Technology today. It is technology which has the potential to transform real world objects into intelligent virtual objects. IoT aims to bring almost everything under a collective platform by giving things around the power to control themselves without relinquishing our control over them as it keeps us enlightened about the state of the things. Although there has been many opinions to the origin of the Internet of Things, its original use can be traced to Kevin Ashton who made a statement in 1999 stating that: "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" (RFID Journal, 2009). According to Kevin Ashton, the use of IoT devices offers outstanding opportunities that will increase productivity and ease the cost of running a home, business and organization. This is possible as we would be aware when devices needed to make work easy were at their best; if not we would know on time that they have to be recalled, replaced or repaired. What exactly is the Internet of Things? Let us begin by acknowledging a few things. The cost of acquiring Internet Broadband is reducing greatly thereby making connection to the Internet easily available. With its availability, the cost of technology is also going down. Manufacturers are beginning to create more devices with Wi-Fi facilities and sensors integrated into them. Devices such as cellphones, wearable devices like the Apple Smart watch, wireless headphones, washing machine, the drill of an oil rig, in fact just about anything you can think of is now basically connected to the Internet; most of them with on and off switches. Internet of Things goes beyond things connected to computers, smart phones or tablets. It defines a world where nearly anything can be linked and communicate in a clever way. That is to say Internet of Things transforms our physical world into one large information system (www.techopedia.com, 2019).

Goyal, Garg, Meerut and Singhal (2018) defines Internet of Things as "the interaction between two items: Internet and Things". He explained that the Internet can be seen as network of networks which connect billions of users to some standard Internet protocols; and then Things are referred to as the objects or devices that when connected to the Internet become intelligent objects.

A group of researchers, Dr. Ovidiu Vermesan and his colleagues defined IoT as the connection between the physical world and digital world using actuators and sensors (as cited in Maio, Ting, Fei, Ling and Hui, (2010, p.484)).

Even though credit is given to Kevin Ashton, the Executive Director of Auto-ID Labs in MIT for coining the term Internet of Things in 1999, the idea of communication was already in existence before then but wasn't recognized. Later, market analytics and a publication by Auto-ID centre in 2003 raised more awareness on IoT and made it popular that several organizations began to see its importance and started focusing on the concept of IoT with its future prospects. These organizations began to invest in IoT domain at different periods as seen in the table below but at regular intervals.

TABLE 1: History Of Internet Of Things

Year	Industrial Participation & Involvement
1998	Zigbee Technology was conceived
2000	LG announced its first Internet of refrigerator plans
2003	RFID is deployed in US Dept. of Defence. Zigbee Technology was standardized.
2005	UN's International Telecommunications Union (ITU) published its first report on the Internet of Things.
2006	Zigbee Technology was revised.
2008	Recognition by the EU and the First European IoT conference is held. A group of companies launched the IPSO Alliance to promote the use of IP in networks of "Smart Objects" and to enable the Internet of Things. The FCC voted 5-0 to approve opening the use of the 'white space' spectrum
2009	The IoT was born according to Cisco's Business Solutions Group
2010	Chinese Premier Wen Jiabao calls the IoT a key industry for China and has plans to make major investments in Internet of Things
2011	IPv6 public launch-The new protocol allows for 340, 282, 366, 920, 938, 463, 463, 374, 607, 431,768,211, 456 (2^{128}) addresses

(SOURCE: International Journal of Advanced Networking and Applications, 2018)

III. IOT ARCHITECTURE

In reality, IoT offers numerous possibilities and market opportunities that impact on the quality of life and globaleconomy. Healthcare and equipment manufacturers, application developers and internet service providers are the key agents expected to come up with adept innovations which will create positive developments globally. According to Manyika, Chui, Bughin, Dobbs, Bisson and Marrs (2013), it is believed that in the near future, IoT will contribute to the growth of the global economy by creating $2.7 to $6.2 trillion annually from applications involving healthcare and other IoT-based related services such as m-Health (mobile health) and telecare that support effective delivery of medical diagnosis, treatment, wellness and monitoring services via electronic media.

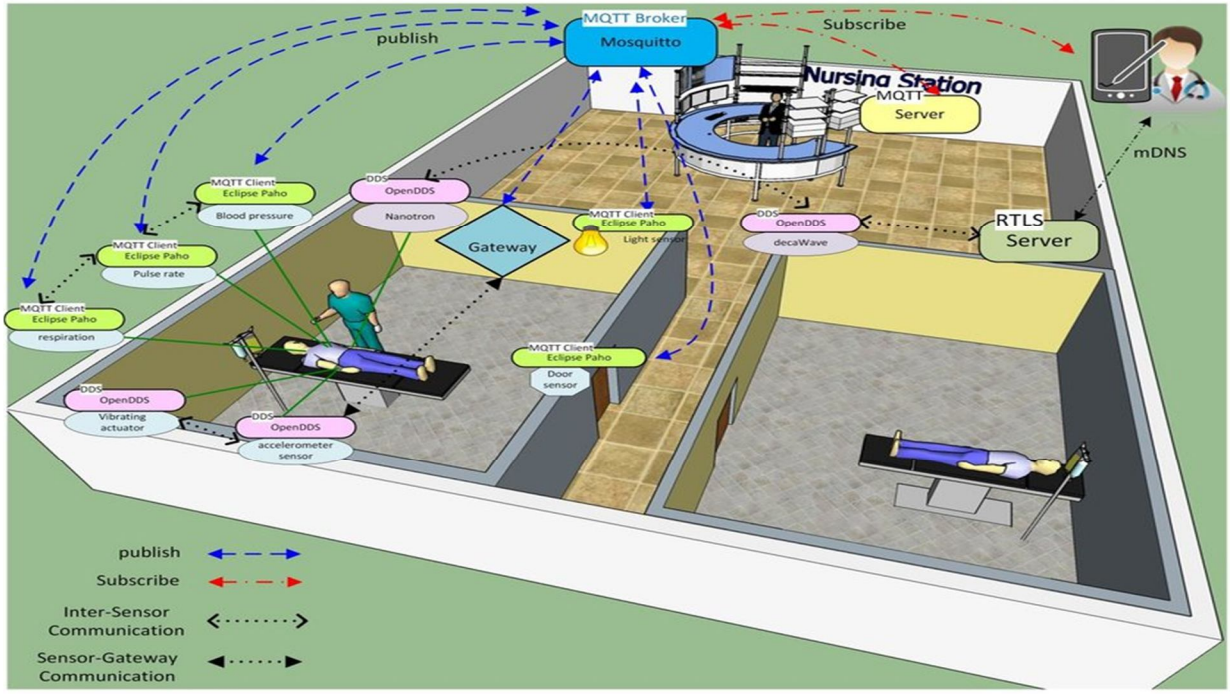


Fig. 1 The incorporation of iot protocols in medicine (source: IEEE Communications Surveys & Tutorials (2015)

The analyst firm, Gartner Inc. believes that by the year 2020, there are going to be more than 26 billion connected devices; it could even be more as almost everything is being manufactured as a smart device that can operate on its own over a network. According to Gantz and Reinsel (2012), by the later part of 2020, an estimated 212 billion IoT smart objects are going to be produced all over the world. The outcome could be that in the future smart home could enable your alarm clock which wakes you up in the morning, in the process of chiming notify the light bulb in the room to come on, the water heater to be turned on, control the temperature of the room and other appliances . Despite the fact that Internet of Things (IoT) presents substantial benefits to the real world for smart applications, its implementation is still not very common.

In order to narrow the gap between existing technologies and the prospect of them being integrated into an IoT supported environment, emerging technologies, service applications and innovations need to grow relatively to meet customers' needs and market demands. Devices should be developed so that they can be available to the customer at any point in time. Furthermore, as a result of the continuous growth in the world's population, it is expected for there to be a relative increase and evolution of people's living demands, hence new protocols intended for communication must be compatible between living things and goods, appliances, vehicles etc. Amongst the many demands likely to increase in the future is Energy. Despite the fact that the current power grids that were built decades ago are upgraded regularly, it is not certain that they will be able to satisfy future demands.

Existing fossil fuels reserves are insufficient and emit harmful substances detrimental to the environmental and social life. A better transition from this would be to replace the traditional centralized grid with a distributed hybrid energy generation system that relies heavily on renewable sources of energy such as wind and solar systems, tidal power, biomass and fuel cells (Lund, Mikkola and Ypja, (2015, p.441) . The theory behind smart grid is the fact that it aims to achieve intelligent and efficient energy consumption and generation by integrating grid power systems with information and communication technologies (ICT). Its methodology includes innovative solutions which aims to utilize the existing power grid so as to eliminate or reduce voltage sags, blackouts and overload problems.

The application of smart grid innovative solutions can be done in every part of the grid: production, transmission and distribution. Recently, smart home which is the fourth part of smart grid has become a main topic of interest in smart grid research and application (Stojkoska and Trivodaliev, 2016). Smart home has to do with the use of ICT in controlling home appliances and automation of home elements such as doors, lighting, windows etc. An important element of smart home is that it uses intelligent power scheduling algorithm which provides residents the opportunity of making appropriate and wise choices on how to consume electricity so as to reduce electricity consumption.

If the standard of IoT architecture is faultless, it gives room for a competitive environment where companies can deliver excellent products. In order to satisfy customers' demands for smart objects, most underlying protocols should run protocols that possess enough addressing space; for example IPv6 so as to accommodate the enormous amount of objects ready to be connected to the Internet. Also, monitoring and management of IoT should be done timely to make sure that customers always get high quality services from their smart objects at an efficient cost. This is achievable with the application of semantic in the IoT. Semantic in IoT signifies the clever way in which different machines discover and make use of available resources and modelling information to extract knowledge so as to provide the required services. Furthermore, it involves identifying and analyzing data to figure out how to make the right decision that will facilitate the provision of the exact service the customer desires. Hence, semantics which can also be referred to as the brain of IoT because it sends customers' demands to the right source is supported by Semantic Web technologies such as the Resource Description Framework (RDF) and the Web Ontology Language (OWL) (Barnaghi, Wang, Hencon and Taylor (2012, p.17)).Since the IoT should have the ability to interconnect billions of various objects (devices) through the Internet, it is fundamental for its architecture to be layered and flexible. Because of this, several proposed architecture that can serve as a reference model centering on the analysis and demands of the industry and researchers have been introduced; as shown in the figure below:

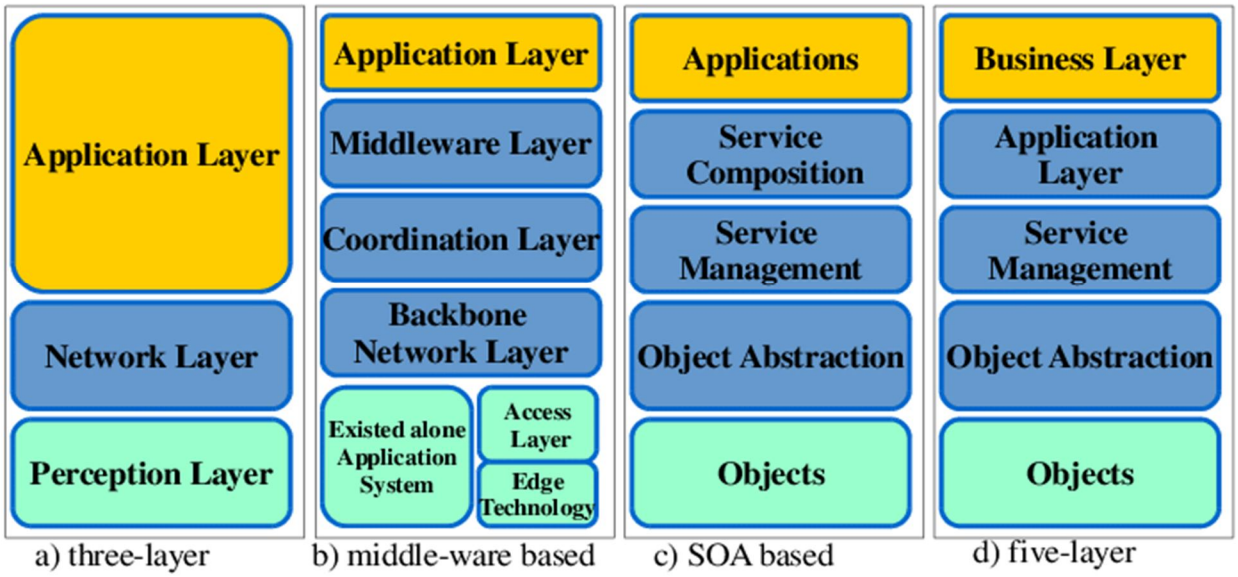


Fig. 2 Range of proposed IoT architectural models (source:www.electronicsforu.com, 2017)

Among these proposed models, the 5-layer model is widely used because it gives more detailed perception of IoT architecture as seen in its different layers explained below:

1) *The Object/ Perception/ Physical Layer*: This layer recognizes the physical world and gathers data or information from the sensors or actuators and implements it. The actuators and sensors carry out diverse tasks that range from querying temperature, location, motion, weight, humidity etc. Standard plug-and-play mechanisms are used in this layer to configure various objects. It is also in this layer that the IoT initiates the creation of big data. Finally, data is digitized here and transferred to the next layer (object abstraction layer) via secure channels.
2) *The Object Abstraction Layer*: Also called the transport layer, the object abstraction layer transports data from the object layer to the Service Management Layer and vice versa via secure channels using different technologies such as GSM, 3G, Wi-Fi, Bluetooth low energy, infrared etc. Besides this, other functions like data management processes and cloud computing are performed at this layer.

3) *Service Management Layer*: Also called the Middleware layer, this layer uses names and addresses to pair a service with its requester. In this layer, IoT application programmers are permitted to work with various objects without considering a particular hardware platform. This is the layer where data received is processed, decisions are made and then the required services are delivered in this layer over the network wire protocols.
4) *Application Layer*: It is in this layer that the IoT is implemented and services requested by customers are provided. It serves as the interface through which customers can query for interesting data and also interact with a device. For example, customers who ask for temperature and weight measurements data receive it in this layer. The application layer can be referred to as the layer where the software that works for and on the sensors in the virtually intelligent objects are applied. The significance of this layer for the IoT is the fact that it has the potential to deliver high quality smart services such as smart home, transportation, smart healthcare and industrial automation.
5) Business/ Management Layer: This is the last layer of the 5-layer architecture. Due to its enormous and complex computational needs, this layer is hosted on powerful devices. Along with many other characteristics such as giving support to processes that have to do with decision making based on Big Data analysis, it organizes the work of the underlying four layers and the overall IoT system services and activities. Other roles carried out in this layer include building business models, flowcharts, graphs etc. based on the data received from the application layer.

IV. A REVIEW OF ENABLING TECHNOLOGIES:

IoT is defined by various technologies; however four main technologies stand out and they are:

A. *Radio Frequency Identification (RFID)*

RFID is a system that makes use of radio wave technology to transmit the information of an object or device. It can be divided into two key components namely: radio signal transponder (tag) and the tag reader. Information of an object in the RFID is transmitted in the form of serial number which is attached to the tag.

The tag is made up of two components: a chip (stores the unique identity of an object) and an antenna (uses radio wave to enable the chip communicate with the tag reader). While the tag reader produces a radio frequency field that identifies objects reflected through radio waves of the tag.

Since the RFID is based on tag readers and tags, the initial phase of research RFID is defined in three configurations:

1) *Active RFID:* In this configuration, the tag reader is passive and the tag remains active. Information or signal from a battery-operated device is received by the tag reader. The battery run on the device is also activated by another device called active tag. Depending on the architecture, information that is exchanged here takes place in a limited range of 1 to 2000 feet of the passive readers and active tags.
2) *Passive RFID:* This common and mostly used configuration has the tag reader active and the tag passive. The tag in this configuration needs energy from the RFID reader to send data or information because it is not run on battery or any onboard power supplies.
3) *Active Reader Active TAG:* Going by its name, both the tag and tag reader in this configuration are active. Despite of this, the tags can only start sending information when incited by the reader or when it is in close proximity with the reader.

We can conclude by listing the main components of the RFID technology as tag reader, tag, power supply, software, server, antenna and access controller.

Application of RFID: Because RFID technology operates on frequency within a limited range, its use is restricted for only identification and tracking. It can be applied in smart fridge, smart grocery, smart currency, smart appliances, smart groceries etc. In these situations, products have tags on them and then the reader scans the tags as we see during check out in most grocery stores. This helps to track the products leaving the store and inventories left for the corresponding products. A common and useful application of RFID technology is at the airport where baggage that are tagged at a certain place can be read at another location. For a smart fridge using RFID technology, a fridge can sense what item is put into it and what item is taken out from it too.

Challenges of RFID Technology: Among the many concerns that have risen with the application of RFID technology is its limited frequency. If the frequencies at different places differ then there will be a challenge in reading a tag at different locations. Another problem is the challenge of reading more than one tag at the same time.

Solution: Although costly, different unique tags have to be used on a product. It is even more uncomfortable when the products to be tagged are less than the cost of the tag.

B. Near Field Communication (NFC)

Near Field Communication which was first developed by Sony and Philips companies is a short range wireless technology with a frequency of 13.56 MHz. It is usually applied within short distances of up to 4cm. NFC is a little bit like the RFID in the sense that it uses the combination of RFID reader in a mobile phone which makes it efficient, better and reliable for users. Furthermore, NFC complements Bluetooth (long distance capability of up to 10cm circa) and permits spontaneous initialization of wireless networks. Finally, during data reading the rate of power consumption in NFC is 15ma. NFC comprises of two modes which are:

1) *Active Mode:* Devices in active mode are active and communicate with each other by emitting signals.
2) *Passive Mode*: In this mode, one of the devices sends the signal and the other device receives it.

In conclusion, since NFC works within a short range and doesn't require devices to pair up, it makes this technology secure and useful for mobile payments.

Application of NFC: Because NFC works within short distances, an important application is its use in most payment Apps. Devices using NFC technology can serve as virtual cards for card less transactions. Also, by touching devices with each other, business cards can also be exchanged (Int. Journal Advanced Networking Applications, 2018). Hotels use it in their room keys. By touching the room key (most times a card) on the door of a hotel room grants access to the room.

Challenges of NFC: A major challenge is that devices using NFC technology work only within short range. Also, there can be compatibility issues between two devices of different manufacturers. This can create monopoly in the market.

C. Machine to Machine Communication (M2M)

According to Dye (2008), M2M technology is the communication between computers, embedded sensors, actuators, processors and mobile devices. As predicted in 2014 by a group of researchers, there is an increase in the use of M2M technology. In recent times, the estimated amount of connected wireless devices that can gather data from the sensors, analyze it and transmit the information to other devices to execute a given function is about 2 billion in number.

1) *Application of M2M:* M2M is used in smart home; for instance when an owner forgets to lock the door to his home, once smart home senses that there has been no motion in the house for a while, it can lock the door and send the unlock key to the owner. Likewise in industrial setting, a device can sense the work efficiency of a machine and work accordingly to produce maximum results. Furthermore, smart water helps to save water when there is water leakage in a supply by sensing the leakage and then cutting off the supply.
2) *Challenges of M2M:* The major challenge faced in M2M technology is that of Security due to the fact that different devices or group of devices can use different naming process for their work, or the same name can be assigned to different objects, devices or groups. Devices can also communicate using temporary names, identification and URI (Uniform Resource Identifier). M2M also uses IP addresses (multicast address for group of connected devices or individual device) for connection and communication among connected groups or devices. Because of the 'nameless' identification of the devices, they are prone to threats and security issues like unauthorized access, hacking and tampering of information. Devices that can be moved are at risk of being monitored. Also, a change in geographical location, may cause the network to be disconnected. Devices using M2M technology could be stationary or movable, wireless or not and need to be updated timely to be aware of security threats. Updating them is quite challenging as they could be many hence it becomes difficult to access each device manually; making the devices more vulnerable to risks.

D. Vehicle to Vehicle Communication (V2V)

In V2V technology, vehicles are used as objects to communicate with each other or the sensors around them. Communication of objects (vehicles) over V2V are efficient and can work for long distances. The primary aim behind the design of this technology is to control traffic, to avoid accidents and for safety.

1) *Application of V2V:* V2V is mainly applied in smart cars especially the cars that can operate without drivers. These smart cars with sensors can sense the speed of a nearby car that is uncertainly getting slow and then slow down itself to avoid accidents.
2) *Challenges of V2V:* The primary area of concern in V2V is the loss of communication when another object (vehicle) comes in between the connected devices. Also, since the means of communication in this technology is between moving objects or with the sensors on the roadside, there could be low or no network which makes it difficult to send or receive data properly or find a suitable way to define the protocols used. The result of this could be quite bad (Int. Journal Advanced Networking and Applications, 2018).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

V. METHODOLOGY OF ZIGBEE TECHNOLOGY

A. ZigBee Wireless Technology Architecture and Applications

Zigbee WPANs operate at 868 MHz, 902-928 MHz and 2.4 GHz frequencies. Its data rate of 250kbps makes it appropriate for periodic and intermediate two way data transmission between sensors and actuators. Its communication offers numerous advantages over other proprietary short range wireless sensor networks such as Wi-Fi and Bluetooth because it is less expensive and exist in small simple forms. Zigbee supports different network configurations and can be operated in different modes, conserving battery power at the same time. Because it allows many nodes to interconnect with each other it gives room for building a wider area network.

Fig.3 Zigbee modem (source: www.elprocus.com, 2019)

The structure of Zigbee architecture comprises of three different types of devices such as Zigbee coordinator, Zigbee Router and End device. It is compulsory for all Zigbee communication network to contain at least one coordinator which serve as a root and bridge of the network. The role of the coordinator is mainly to handle and store the information while executing the task of receiving and transmitting data operations. Zigbee routers function as intermediary devices because they allow data from other devices to navigate to and fro through them. As shown in the figure below, end devices allow limited communication with the parent nodes in an effort that saves the battery power. The amount of routers, coordinators and end devices is dependent on the type of network; which could be star, mesh or tree networks.

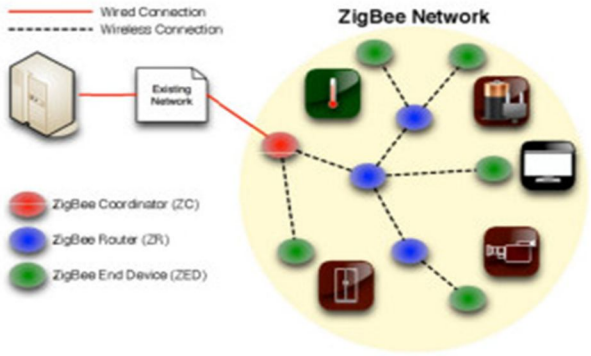


Fig.4 Zigbee system structure (source: www.elprocus.com, 2019)

B. Zigbee Operating Modes and Its Topologies

Zigbee technology operates a two way data transmission system. It traffics in two modes: Beacon mode and non-beacon mode. In beacon mode, coordinators and routers go into sleep state when there is no data communication from end devices. Occasionally, the coordinator in the network wake up to transmit the beacons to the routers. Communication over this network in this mode operate in time slots and this results in longer battery usage and lower duty cycles. Whereas, in non-beacon mode, more power is consumed because the coordinators and routers constantly monitor the active state of incoming data. Most of the time, devices in this mode are in an inactive state in the network therefore the overall power consumption is low and more power supply is required.

Zigbee beacon and non-beacon modes manage the transmission of periodic (sensors data), intermittent (Light switches) and repetitive data types.

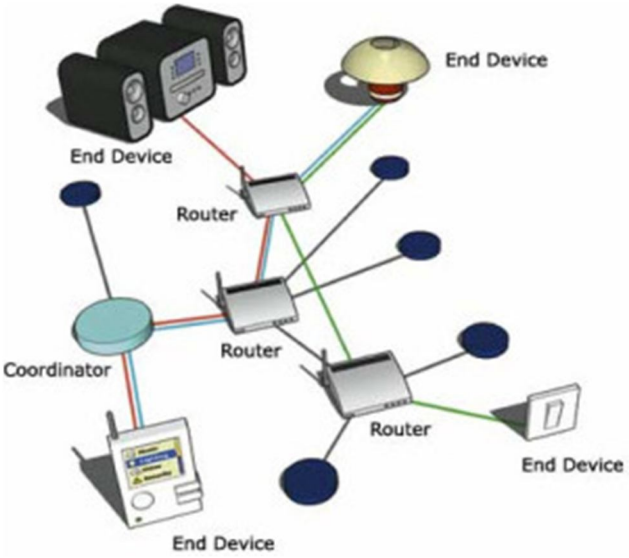


Fig.5 Zigbee communication operation (source: www.elprocus.com, 2019)

VI. OPEN RESEARCH ISSUES/DISCUSSION

The aspect of IoT that requires more research is the need for better horizontal integration between application layer protocols. We can classify IoT devices into two groups: (i) resource- rich devices and (ii) resource-constrained devices.

Resource-rich devices are those devices that have the software and hardware capability to support TCP/IP protocol suite. IoT is implemented on these devices on top various frameworks and application level protocols such as AMQP, MQTT, MQTT-SN, CoAP, REST etc. While the resource-constrained devices are end nodes with sensors /actuators that can handle a specific application process (Nagasai, 2017). These devices communicate mainly through low power wireless protocols such as BLE, LPWAN etc. and they are usually battery powered with low data rate.

Hence devices lacking the required resources to support TCP/IP protocol suite cannot easily work together with resource-rich devices which support the TCP/IP suite. For instance, microcontroller based gadgets and appliances should have the proficiency to work together with other IoT elements that are enabled with TCP/IP protocol suite. Aside this issue, TCP/IP enabled devices operate various protocols leading to numerous interoperability issues that results in the limitation of the potential application of the IoT. I do not foresee the division between the protocols used for communication across and within resource-rich and resource-constrained devices to change anytime soon.

Furthermore, despite the fact that we have several existing high data rate communication standards, they actually don't meet the actuators and sensors communication standards. For these communication standards to fully meet the standard for implementation in actuators and sensors, they would need to operate at lower bandwidths that require low latency and low energy consumption.

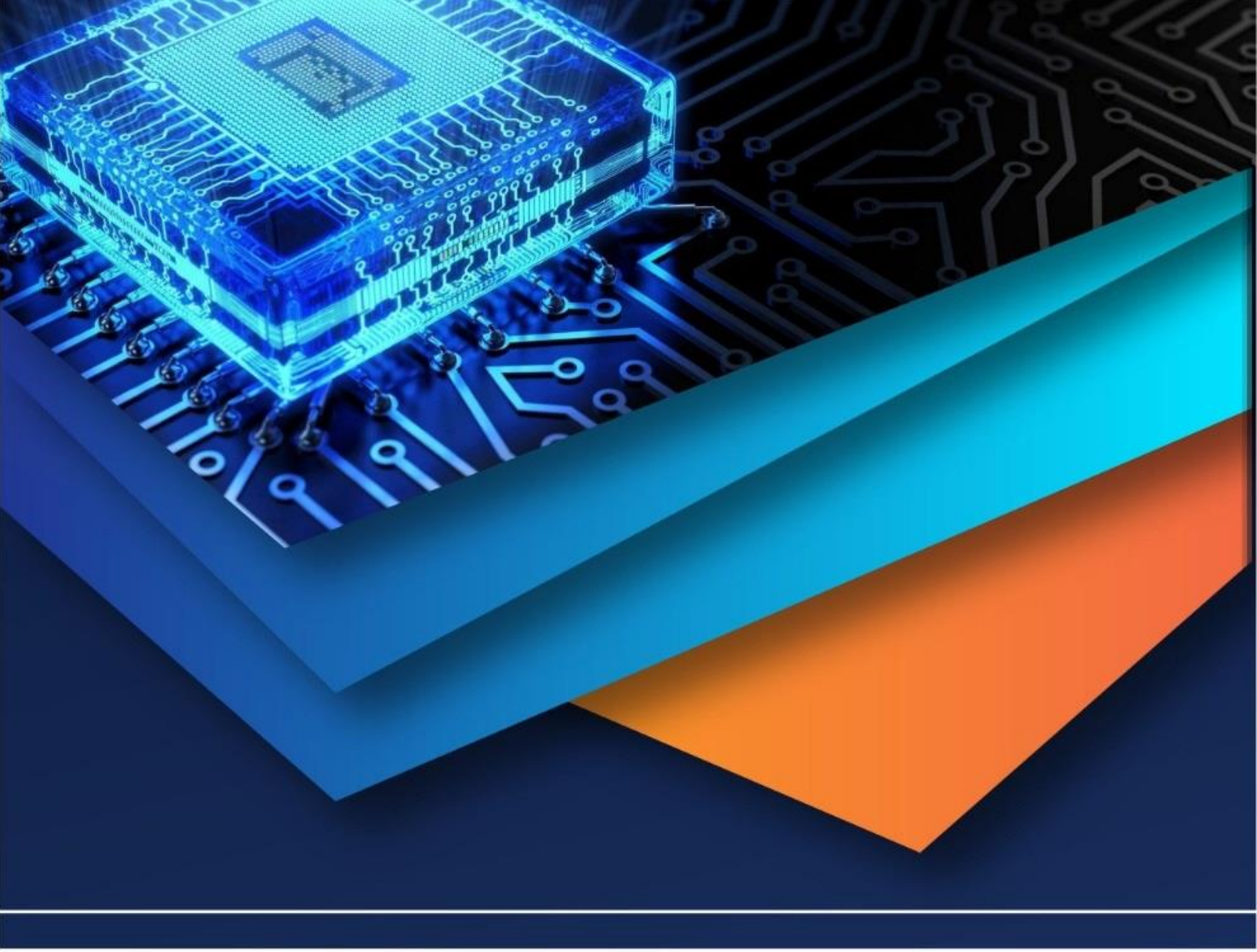
VII. CONCLUSION

Although IoT offers lots of opportunities, it also has many challenges. The main backbone for IoT is in the standard of its architecture; and this is where most of its challenges are faced. Furthermore, the conventional Internet architecture has to be updated to meet the IoT challenges.

A major challenge faced in Internet of Things is the issue of Security. Insecurity is a global threat faced by most companies around the world. Taking into account the amount of shared data and large number of objects that are connected in a network, privacy becomes an area of concern. This concern is likely to escalate when billions of devices become connected in the future as predicted earlier in this article. Customers' would be satisfied if and only if they are sure their information remains secure. A possible solution to this can come about if IoT stakeholders can decipher safer ways to analyze, track and store the huge amount of data likely to be generated (Faqaha, Guizani, Mohammadi, Aledhari and Ayyash, 2015). I believe that further enhancing the application of Zigbee communication technology by allowing customers select their alert method in the case of security threat to lives and property will go a long way to curb insecurity issues in IoT. Zigbee wireless technology has an excellent low power and low cost consumption characteristics that make its communication best suited for communicating in several applications, home automation, medical device data collection, industrial control etc.

REFERENCES

[1] Barnaghi, P, Wang, W, Henson, C and Taylor, K Semantics for the Internet of Things: Early Progress and Back to the Future. International Journal on Semantic Web and Information Systems (IJSWIS), 8(1), 1-21, 2012.
[2] Dye, S. (2008). Machine to Machine Communications. Retrieved from www.mobilein.com//M2M.
[3] Fuqaha, A, Guizani, M, Mohammadi, M, Aledhari, M and Ayyash, M. A Survey of Enabling Technologies, Protocols and Applications: Internet of Things. IEEE Communications, Surveys and Tutorials, 2015 17(4), 2347-2376. doi: 10.1109/COMST.2015.2444095.
[4] Gantz, J. & Reinsel, D. The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the Far East. Analyze the Future, 6(1), 1-16. Retrieved from www.sciepub.com, 2012.
[5] Gislason, D. Zigbee Applications- Part 1: Sending and receiving data. EE Times. 2010. Retrieved from www.eetimes.com.
[6] Goyal, K., Garg, A., Meerut, A. and Singhal, S. A Literature Survey on Internet of Things. Int. J. Advanced Networking and Applications 9(6), 3663-3668. 2018. Retrieved from www.semanticscholar.org.
[7] Lund, P.D., Mikkola, J., Ypyä, J. Smart energy system design for large clean power schemes in urban areas. Journal of Cleaner Production. 103, 437–445
[8] Manyika, J., Chui, M., Bughin, J., Dobbs, R.., Bisson, P., and Marrs, A.. Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy. 2013. San Francisco, CA. McKinsey Global Institute Press.
[9] Miao W., Ting L., Fei L., ling S. & Hui D. Research on the architecture of Internet of things. (Report No. 486). Sichuan province, China: IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE). 2010.
[10] Nagasai, P. Classification of IoT devices. Retrieved from www.cisoplatform.com. 2017
[11] Stojkoska, B. & Trivodaliev, K. A review of Internet of Things for smart home: Challenges and solutions. Skopje, Macedonia. Elsevier Ltd. 2016.
[12] Definition of Internet of Things. Retrieved from www.techopedia.com. 2019.
[13] That 'Internet of Things' Thing. Retrieved from www.rfidjournal.com. 2009.
[14] 6 Awesome and Useful IoT Protocols. Retrieved from www.electronicsforu.com. 2017.
[15] Zigbee Modem, Zigbee System Structure and Zigbee Communication Operation diagrams, retrieved from www.elprocus.com 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY