International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Review: A Concise Review on Internet of Things (IoT) and Future Technologies

Ojasvi Savlani[1], Mohit Sood[2]

[1, 2]Department of Information Technology, Invictus International School, Amritsar, India
[1]Email: *ojasvisavlani[at]invictusschool.edu.in*
[2]Email: *mohit[at]invictusschool.edu.in*

Abstract: ***The Internet of Things (IoT) is the internetworking of physical devices, vehicles and other objects which consists of an embedded system with sensors, actuators and network connectivity that enable to collect and exchange data. Internet of Things (IoT) is fast becoming a disruptive technology business opportunity, with standards emerging primarily for wireless communication between sensors, actuators and gadgets in day - to - day human life, all in general being referred to as "Things". The IoT is comprised of smart machines interacting and communicating with other machines, objects, environments and infrastructures. The IoT is a rapidly increasing and promising technology which becomes more and more present in our everyday lives. Radio Frequency identification assigns a unique identification to the objects. RFID technology is used as more secure identification and for tracking/locating objects, things, vehicle. In this paper, we survey about components, application in the new emerging area. This survey paper proposes for IoT technologies, highlights for some important technologies and applications.***

Keywords: IOT (Internet of Things), IOT definitions, IoT components, applications, future technologies

1. Introduction

Today, Internet application development demand is very high**. So** IoT is a major technology by which we can produce various useful internet applications. Basically, IoT is a network in which all physical objects are connected to the internet through network devices or routers and exchange data. IoT allows objects to be controlled remotely across existing network infrastructure. The Internet of Things (IoT) can be defined as a network of physical objects or people called "things" that are embedded with software, electronics, network, and sensors which allows these objects to collect and exchange data. The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first internet - connected appliance, able to report its inventory and whether newly loaded drinks were cold. Kevin Ashton (born 1968) is a British technology pioneer who is known for inventing the term "the Internet of Things" to describe a system where the Internet is connected to the physical world via ubiquitous sensors.

Figure 1: Internet of things

So, "The Internet of Things refers to the ever - growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet - enabled devices and systems". This includes everything from cell phones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of.

Over 9 billion 'Things' (physical objects) are currently connected to the Internet, as of now. In the near future, this number is expected to rise to a whopping 20 billion.

2. How IOT Works?

As we know that, "The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human - to - human or human - to - computer interaction. "

A complete IoT system integrates four distinct components: sensors/devices, connectivity, data processing, and a user interface.

Below I will briefly explain each component and what it does:

Figure 2: Components of IOT

(A) Sensors/Devices

First, sensors or devices help in collecting very minute data from the surrounding environment. All of this collected data can have various degrees of complexities ranging from a feed. These sensors are built in the devices which collects all the data to be used later. For instance, our phone is a device with built - in sensors like GPS, camera, etc.

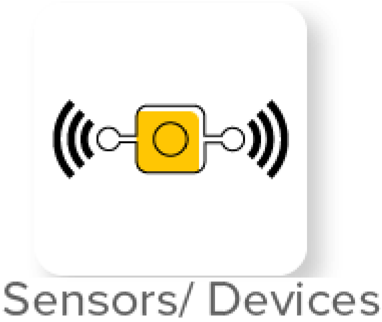

Figure 3: Sensors

(B) Connectivity:

Second, after you have chosen the sensor or actuator, you will need to connect it reliably to the Internet. Since wireless connectivity is central to the success of the IoT. We will establish that connecting all objects in the long - term future with cellular mobile phone technology is probably the best business proposition since it is a technology which ensures availability, reliability and viability all ingredients which we need for a successful IoT uptake. Low Power Wifi, a new system, is also a great contender since Wifi already enjoys global coverage today. Furthermore, an exciting class of Low Power Wide Area networking technologies is also emerging, diversifying the connectivity portfolio. On the other hand, whilst the initial technology of choice, known as Zigbee, is suitable for sporadic short - range connections, it is surprisingly unfit to meet the demands for a viable Internet of Things at global scale. So watch out when building a future - proof IoT business.

Figure 4: Connectivity

(C) Data Processing:

Once the data is collected and it gets to the cloud, the software performs processing on the acquired data.

The analysis can be as simple as checking the temperature of the AC or a complex one such as a situation where an intruder comes in and the device has to identify it through cameras.

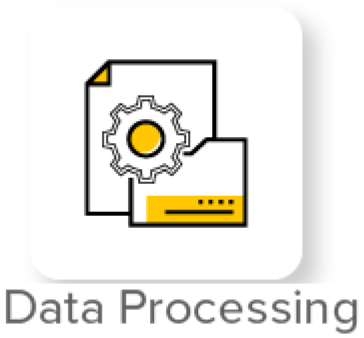

Figure 5: Data Processing

(D) User Interface:

Next, the information made available to the end - user in some way. This can achieve by triggering alarms on their phones or notifying through texts or emails. However, this isn't as easy as it seems. It all depends on what is IoT platform and how the technology has been developed.

Finally, an important component is how the data is presented to the final users. Make sure your IoT product has a very appealing user interface, both web based as well as smart phone or tablet based.

Fortunately, there are many open - source as well as paying front - end products available today. For Example, sometimes the system doesn't need the interference of humans to work; like in home automation system if no one is in the home and the system detects any intruders then they are sensed, then the system generate an alert to the owner of the house and also to the concerned authorities.
This is how iot works.

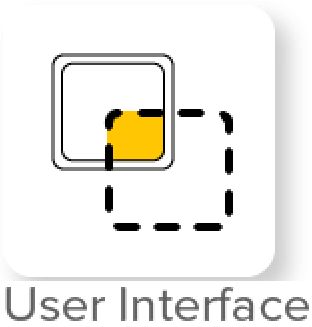

Figure 6: User Interface

3. Internet of Things Applications

A. Smart Cities

Smart cities use a combination of the internet of things (IoT) devices, software solutions, user interfaces (UI) and communication networks. However, they rely first and foremost on the IoT. The IoT is a network of connected devices - - such as vehicles, sensors or home appliances - - that can communicate and exchange data. Data collected and delivered by the IoT sensors and devices is stored in the cloud or on servers.

Figure 7: Smart City

For example, New York Smart City, Amsterdam Smart City, Copenhagen Smart City etc….
Application of IoT to achieve smart cities would require using radio frequency identification and sensors.

B. Smart Home and Buildings
Now a days, smart home is becoming a need of fast life. Smart home allows many household devices to be connected with internet for the communication. In smart home, the various home equipment's like air conditioning, doors, windows, lighting, washing machine, and refrigerator can be controlled manually as shown in Fig - 8. IoT in integration with wireless sensor network can give intelligent solution for energy management of buildings. With the help of laptop or smart phones, we can access energy information and control system of buildings. Wi - Fi's technologies in home automation has been used primarily due to the networked nature of deployed electronics where electronic devices such as TVs, mobile devices, etc are usually supported by Wi - Fi.

Figure 8: Smart Home

Wi - Fi have started becoming part of the home IP network and due the increasing rate of adoption of mobile computing devices like smart phones, tablets, etc

C. Smart Energy and the Smart Grid
A smart grid is related to the information and control and developed to have a smart energy management. A smart grid that integrate the information and communications technologies (ICTs) to the electricity network will enable a real time, two way communication between suppliers and consumers, creating more dynamic interaction on energy flow, which will help deliver electricity more efficiently and sustainably.

Figure 9: Smart Energy and Smart Grid

Project related to smart energy and the smart grid are Salt River Project, Entergy AMI, AEP Ohio gridSMART PHASE 2 project etc …. Application of internet of things such as industrial, solar power, nuclear power, power control etc. .

D. Smart HealthCare
Most healthcare systems in many countries are inefficient, slow and inevitably prone to error. This can easily be changed since the healthcare sector relies on numerous activities and devices that can be automated and enhanced through technology. Additional technology that can facilitate various operations like report sharing to multiple individuals and locations, record keeping and dispensing medications would go a long way in changing the healthcare sector.

Figure 10: Smart Health Care

Remote health monitoring could be used to monitor non - critical patients at home rather than in hospital, reducing strain on hospital resources such as doctors and beds. It could be used to provide better access to healthcare for those living in rural areas, or to enable elderly people to live independently at home for longer. Essentially, it can improve access to healthcare resources whilst reducing strain on healthcare systems, and can give people better control over their own health at all times.

Thus far, most IoT initiatives in healthcare revolved around the improvement of care as such with remote monitoring and telemonitoring as main applications in the broader scope of telemedicine. A second area where many initiatives exist is tracking, monitoring and maintenance of assets, using IoT and RFID. This is done on the level of medical devices and healthcare assets, the people level and the non - medical asset level (e. g. hospital building assets).

E. Smart Transportation and Mobility

Smart transportation, a key internet of things vertical application, refers to the integrated application of modern technologies and management strategies in transportation systems. These technologies aim to provide innovative services relating to different modes of transport and traffic management and enable users to be better informed and make safer and 'smarter' use of transport networks.

Smart Transportation. Intelligent Transportation Systems are advanced applications that aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated, and smarter use of transport networks.

Application of internet of things a that can handle smart transportation like road safety, traffic management, autonomous driving etc.

The intelligent transportation technology can be wireless communication, sensors, Bluetooth, video vehicle, audio detection, floating car data etc. . .

Figure 11: Smart Transportation and Mobility

Congestion, accidents, and pollution issues due to transportation are becoming more severe as a result of the tremendous increase in various travel demands, including vehicular traffic, public transportation, freight, and even pedestrian traffic. To resolve such issues, ITSs have been developed that are able to integrate a broad range of systems, including sensing, communication, information dissemination, and traffic control.

Three essential components are necessary for any ITS to perform its function (s): data collection, data analysis, and data/information transmission.

Intelligence transportation system is a future transportation system comprised of an advanced information and telecommunication for roadstead and vehicles Intelligence Transportation system is a application of advance technologies using electronics divide, communication and advance sensors. These application provides passenger with important information while improving the status and efficiency of the transportation system.

Application of internet of things that can handle smart transportation like road safety, traffic management, autonomous driving etc…

The intelligent transportation technology can be wireless communication, sensors, bluetooth, video vehicle, audio detection, floating car data etc….

F. Smart Factory and Smart Manufacturing

Smart manufacturing allows factory managers to automatically collect and analyze data to make better - informed decisions and optimize production. The data from sensors and machines is communicated to the Cloud by Iot connectivity solutions developed in the factory. That data is analyzed and combined with contextual information and then shared with authorized stakeholders.

Iot technology, leveraging both wired and wireless connectivity, enables this flow of data, providing the ability to remotely monitor and manage processes and change production plans quickly, in real time when needed. It greatly improves outcomes of manufacturing reducing waste, speeding production and improving yield and the quality of goods produced.

Effect of smart manufacturing are: -

(i) Greater operating efficiency:

The ability to understand what is happening at each stage of the manufacturing process allows plant managers to implement real - time solutions and minimize machine downtime. This leads to greater efficiency and reduced costs.

(ii) Minimal machine downtime:

Artificial intelligence algorithms can use operation and failure logs to turn real - time IoT sensor data into predictive maintenance insights. This allows human workers to be warned of potential component failures, or even enable these components to be "self - healing".

(iii) Increased worker safety:

Automated tracking and analysis of people's movements and activities inside a smart factory can help mitigate risks. Safety systems warn persons inside the factory about specific injury risks, surveying for lapses in focus or mistakes during new or routine tasks. These systems could also administer or send for medical assistance if needed.

(iv) Supply chain management:

Manufacturers can use IoT device geolocation to track shipments, parts, and products. This data can then be used to adjust scheduling on parts orders and provide insights that make products easily recycled or reused, lowering the cost of materials for manufacturers.

Figure 12: Smart Factory and Manufacturing

Smart factory added a new values in manufacturing revolution by integrates artificial intelligence, machine learning, and automation of knowledge work and M2M communication with the manufacturing process.

G. Smart Environment

Environment plays a major effect in human life. People, even animals, birds, fishes and plants may be affected in unhealthy environment. There were many researches efforts has been paid to solve the problems of environmental pollution and waste resources. Creating of a healthy environment is not easy because of industries and transportations wastes, with irresponsible human activities are daily factors that make the environment damaged.
Using IoT to create smart environments, smart office and smart buildings can yield benefits for enterprises beyond energy cost savings. Smart environments not only attract top talent but real - time data gathered from facilities can help organizations make informed decisions related to productivity, innovation, safety, and efficiency.

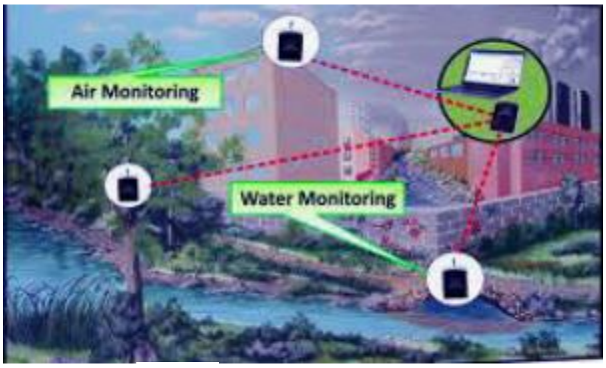

Figure 13: Smart Environment

Smart environment is an important technology in our everyday life which provides many facilities and solutions for many environmental applications such as water and air pollution, weather and radiation monitoring, waste management, natural disaster, and many other environment indicators.

The resources management relates to all natural resources include animals, planets and forests, birds and fishes, coal, petroleum, land, freshwater, air and heavy metals including gold, copper and iron. All these resources are likely to decrease significantly or affected by several factors, including pollution, waste and abuse. Smart environment strategies integration with IoT technology should be created for sensing, tracking and assessment of objects of the environment that offer potential benefits in achieving a sustainable life and a green world. Through IoT technology, weather systems can collect information such as barometric pressure, humidity, temperature, light, motion and other information, from vehicles in motion and transmit the information wirelessly to weather stations.

Therefore, some other applications of internet of things are smart lighting, smart parking, smart refrigerator, smart watches etc…. SO, these are the some applications of internet of things.

H. Smart Agriculture and Water Management

According to, the IoT has the capacity to strengthen and enhance the agriculture sector through examining soil moisture and in the case of vineyards, monitoring the trunk diameter.

IoT would allow to control and preserve the quantity of vitamins found in agricultural products, and regulate microclimate conditions in order to make the most of the production of vegetables and fruits and their quality.

Furthermore, studying weather conditions allows forecasting of ice information, drought, wind changes, rain or snow, thus controlling temperature and humidity levels to prevent fungus as well as other microbial contaminants.

Figure 14: Smart Agriculture

When it comes to cattle, IoT can assist in identifying animals that graze in open locations, detecting detrimental gases from animal excrements in farms, as well as controlling growth conditions in offspring to enhance chances of health and survival and so on. Moreover, through IoT application in agriculture, a lot of wastage and spoilage can be avoided through proper monitoring techniques and management of the entire agriculture field. It also leads to better electricity and water control.

4. Future Technologies in IOT

Many new technologies are related to IoT to prove the integration of wired as well as wireless control, communication and IT technologies together which are responsible for connecting several subsystems and things which operate under a unified platform controlled and managed smartly.

A. Cloud Computing: The two worlds of Cloud and IoT have seen a rapid and independent evolution. These worlds are very different from each other, but their characteristics are often complementary in general, in which IoT can benefit from the virtually unlimited capabilities and resources of cloud to compensate its technological constraints for example storage, processing, and communication. Cloud computing is the delivery of on - demand computing services - - from applications to storage and processing power - - typically over the internet and on a pay - as - you - go basis. Cloud computing services cover a vast range of options now, from the basics of storage, networking, and processing power through to natural language processing and artificial intelligence as well as standard office applications. Pretty much any service that doesn't require you to be physically close to the computer hardware that you are using can now be delivered via the cloud. All we need to have a web browser like chrome to use cloud computing. Following are the key features of cloud computing:

a) Resource Pooling and Elasticity
b) Self - Service and On - Demand Services
c) Pricing
d) Quality of Service

Figure 15: Network of Cloud

The basic examples of cloud computing which are used by general people in daily life are Facebook, YouTube, Dropbox, and Gmail etc. It offers scalability, flexibility, agility, and simplicity that's why its use is rapidly increasing in the enterprises.

Characteristics of cloud computing are multi sharing, high scalability, performance, maintenance.

Advantages of cloud computing are cost efficiency, unlimited storage, backup and recovery. There are various challenges while working on cloud computing like privacy, trust, availability, audit, confidentiality, integrity.

B. Big Data

Due to the rapid expansion in the networks nowadays, the number of devices and sensors in networks are increased more and more in the physical environments which will change the information communication networks, services and applications in various domains. The term "big data" refers to data that is so large, fast or complex that it's difficult or impossible to process using traditional methods. The act of accessing and storing large amounts of information for analytics has been around a long time. But the concept of big data gained momentum in the early 2000s when industry analyst Doug Laney articulated the now - mainstream definition of big data as the three V's: volume, velocity, variety.

Figure 16: Big Data

Examples of big data are New York Stock Exchange, Facebook, Jet Engine.

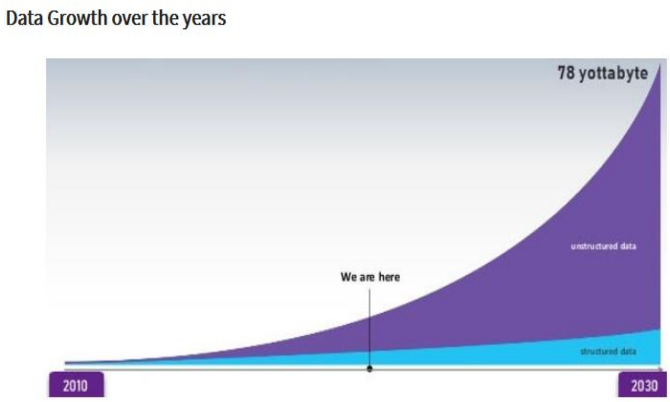

Figure 17: Graph of Big Data

Characteristics of big data includes volume, variety, variability**,** velocity. Improved customer services, better operational efficiency, better decision making are few advantages of big data. With large volumes of distributed and heterogeneous IoT data, issues related to interoperability, automation, and data analytics will require common description and data representation frameworks in addition to machine readable and interpretable data descriptions.

C. Security and Privacy

Due the fact that IoT applications able to access the multiple administrative domains and involve to multiple ownership regimes, there is a need for a trust framework to enable the users of the system to have confidence that the information and services being exchanged can indeed be relied upon. The trust framework needs to be able to deal with humans and machines as users, for it needs to convey trust to humans and needs to be robust enough to be used by machines without denial of service. Recently, the IoT becomes a key element of the future internet, the need to provide adequate security for the IoT infrastructure becomes ever more important. A large scale applications and services based on the IoT are increasinglyvulnerable to disruption from attack or information theft. Many advanced security methods are required in several areas to make the IoT secure from attacks, thefts and many other security problems such as DoS/DDOS attacks, compromised nodes, and malicious code hacking attacks, that because the IoT is susceptible to such attacks and will require specific techniques and mechanisms to ensure that transport, energy, city infrastructures cannot be disabled or subverted. Owing to the fact that IoT has become a vital element as regards the future of the internet with its increased usage, it necessitates a need to adequately address security and trust functions. Researchers are aware of the weaknesses which presently exist in many IoT devices. Furthermore, the foundation of IoT is laid on the existing wireless sensor networks (WSN), IoT thus architecturally inherits the same privacy and security issues WSN possesses

There is a need for more research to be conducted on cryptographic security services that have the capability to operate on resource constrained IoT devices. This would enable different skilled users to securely use and deploy IoT systems regardless of the inadequate user interfaces that are available with almost all IoT devices. In addition to the protection and security aspects of the IoT, additional areas like confidentiality in communication, trustworthiness, and authenticity of communication parties, and message integrity, and supplementary safety requirements should also be incorporated. These may include features like being able to prevent communication of various parties. As an example, in business transactions, smart objects must be prevented from facilitating competitors' access to confidential information in the devices and thus using this information maliciously.

D. ZigBee

Zigbee is a wireless personal area network (WPAW's) and is specially built for control network sensors. This communication standard defines physical and Media Access Control (MAC) layers to handle many devices at low - data rates. These Zigbee's WPANs operate at 868 MHz, 902 - 928MHz and 2.4 GHz frequencies. The date rate of 250 kbps is best suited for periodic as well as intermediate two way transmission of data between sensors and controllers. This communication has less cost and less power mesh network for developing for controlling and monintoring. Zigbee is based on the IEEE's 802.15.4. Zigbee does not focus on point - to - point communication, such as Bluetooth, where one high - powered device sends data to another high - powered device over a short range, put it operates in a mesh network, which is why it's great for the smart home. The Zigbee 3.0 protocol is designed to communicate data through noisy RF environments that are common in commercial and industrial applications. Version 3.0 builds on the existing ZigBee standard but unifies the market - specific application profiles to allow all devices to be wirelessly connected in the same network, irrespective of their market designation and function. Furthermore, a ZigBee 3.0 certification scheme ensures the interoperability of products from different manufacturers. Connecting ZigBee 3.0 networks to the IP domain opens up monitoring and control from devices such as smartphones and tablets on a LAN or WAN, including the Internet, and brings the true Internet of Things to fruition.

Figure 18: Zigbee

Why zigbee is better than wifi?
WiFi and ZigBee both have their positive qualities, but they obviously come with negatives. What you gain in bandwidth with WiFi is lost in battery power and range, and what you gain with ZigBee's battery life you lose in range and bandwidth with ZigBee. So like any decision based around link budgets, tradeoffs are crucial to understand. ZigBee's best quality is its low power - consumption rate and battery life. Its protocol was designed as "assemble and forget", meaning once you set it up, it can last for months. Zigbee is mesh topology. Bandwidth is high—up to 2MHz—which is why it's perfect for streaming music and checking email on your phone or tablet. maximun transfer speed of wifi is 11mbps. Wifi is a star topology.

E. Fog Computing

Fog computing is related to the edge computing in the cloud. In contrast to the cloud, fog platforms have been described as dense computational architectures at the network's edge. Characteristics of such platforms reportedly include low latency, location awareness and use of wireless access. While edge computing or edge analytics may exclusively refer to performing analytics at devices that are on, or close to, the network's edge, a fog computing architecture would perform analytics on anything from the network center to the edge. IoT may more likely be supported by fog computing in which computing, storage, control and networking power may exist anywhere along the architecture, either in data centers, the cloud, edge devices such as gateways or routers, edge equipment itself such as a machine, or in sensors.

F. SigFox

Sigfox is an ultra - narrowband technology. It uses a standard radio transmission procedure called binary phase - shift keying, and it takes very narrow chunks of the spectrum and transformation the phase of the carrier radio wave to encode the data. The Sigfox uses low data rate transmission and sophisticated signal processing to effectively keep away from network interference, and ensures the integrity of the transmitted data show in figure 19. This IoT wireless technology solution permits bidirectional communication, but always commence by the device. The Sigfox is emphatic for communications from endpoints to base stations (uploads). However, it is not emphatic for communications from base stations to endpoints (downloads Sigfox consumes a fraction (1%) of the power used via cellular communication. This network solution would be perfect for one - way systems, including environmental sensors, basic alarm systems, and agricultural and simple metering as well as this technology is a good fit for any application that needs to send small, unusual bursts of data.

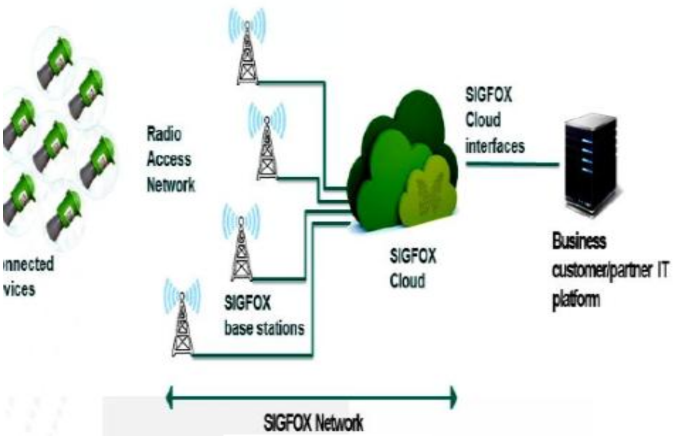

Figure 19: Sig Fox

G. Z - Wave

Z - Wave is a low - power, IoT wireless technology, mainly designed for home automation. It is a possessory solution, originally developed by Zen - Sys and later acquired by Sigma Designs. The Z - Wave proposed authentic and low - latency communication with data rates up to 100kbit/s [32]. A Z - Wave network consists of internet of things (IoT) devices and a mainly controller, also known as a smart home hub, which is the only device in a Z - Wave network that is normally connected to the internet. When a Z - Wave hub receives a command from a smart home application on a user's tablet or computer, smartphone, it routes the command to its destination device across networks of upto 232 devices including hub.

Figure 20: Z - Wave

H. RFID

Radio Frequency Identification (RFID) technology uses radio waves to recognize people or objects. There is a device that reads information contained in a wireless device or tag from a distance without making any physical contact or need a line of sight. The tags contain electronically stored information cross - source reader. The RIFD functions per second, despite the fact that, it is not a very high data rate system; it is enough for most data monitoring applications.
Passive tags collect energy from a nearby RFID reader's cross - examines radio waves. The active tags have a local power source and may operate hundreds of meters from the RFID. The RFID is able to endue several write and reads The RFID technology was first appeared in 1945, as an espionage tool for the Soviet Union, which retransmitted incident radio waves with audio information. Similarly, the IFF (Identification Friend or Foe) transponder developed in the United Kingdom was routinely used by the allies in World War II to identify aircraft as friend or foe.

Every RFID system consists of three components: a scanning antenna, a transceiver and a transponder. When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator. The RFID reader is a network - connected device that can be portable or permanently attached. It uses radio frequency waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.

Figure 21: RFID

5. Future Challenges of Internet of Things (IOT)

The fact that Internet of things applications and scenarios outlined above are very interesting which provides technologies for smart every things., but there are some challenges to the application of the Internet of Things concept in cost of implementation. The expectation that the technology must be available at low cost with a large number of objects. Even though the current IoT enabling technologies have greatly improved in the recent years, there are still numerous problems that require attention, hence paving the way for new dimensions of research to be carried out. Since the IoT concept ensues from heterogeneous technologies that are used in sensing, collecting, action, processing, inferring, transmitting, notifying, managing, and storing of data, a lot of research challenges are bound to arise. These research challenges that require attention have consequently spanned different research areas.

IoT are also faced with many other challenges such as:

A. Scalability

Internet of Things has a big concept than the conventional Internet of computers, because of things are cooperated within an open environment. Basic functionality such as communication and service discovery therefore need to function equally efficiently in both small scale and large scale environments. The IoT requires a new functions and methods in order to gain an efficient operation for scalability. To handle their distribution is not a convenient task. Besides, IoT applications should be tolerant of new services and devices continually joining the network and, consequently, must be designed to enable extensible services and operations.

B. Self - Organizing

Smart things should not be managed as computers that require their users to configure and adapt them to particular situations. Mobile things, which are often only sporadically used, need to establish connections spontaneously, and able to be organize.

C. Data Volume

Some application scenarios of the internet of things will involve to infrequent communication, and gathering information's form sensor networks, or form logistics and large scale networks, will collect a huge volumes of data on central network nodes or servers. The term represent this phenomena is big data which is requires many operational mechanism in addition to new technologies for storing, processing and management.

D. Data interpretation

To support the users of smart things, there is a need to interpret the local context determined by sensors as accurately as possible. For service providers to profit from the disparate data that will be generated, needs to be able to draw some generalizable conclusions from the interpreted sensor data.

E. Interoperability

Each type of smart objects in Internet of Things have different information, processing and communication capabilities. Different smart objects would also be subjected to different conditions such as the energy availability and the communications bandwidth requirements. To facilitate communication and cooperation of these objects, common standards are required. The interoperability means that miscellaneous devices and protocols need to be able to interwork with each other. This is challenging due to the huge number of various platforms used in IoT systems. Interoperability should manage by both the application developers and the device manufacturers.

F. Power supply

Things typically move around and are not connected to a power supply, so their smartness needs to be powered from a self - sufficient energy source. Although passive RFID transponders do not need their own energy source, their functionality and communications range are very limited. Hopes are pinned on future low power processors and communications units for embedded systems that can function with significantly less energy. Energy saving is a factor not only in hardware and system architecture, but also in software, for example the implementation of protocol stacks, where every single transmission byte will have to justify its existence

G. Wireless Communication

From an energy point of view, established wireless technologies such as GSM, UMTS, Wi - Fi and Bluetooth are far less suitable; more recent WPAN standards such as ZigBee and others still under development may have a narrower bandwidth, but they do use significantly less power.

H. Maneuverability

In this context, IoT devices need to move freely and transformation their IP address and networks based on their location. Thus, the routing protocol, like as RPL, has to reconstruct the DODAG each time a node goes off the network or joins the network which adds a large amount overhead. Besides, mobility might outcome in a transformation of service providers which can add another layer of complexity due to service interruption and alter gateway.

I. Trustworthiness

The system should be completely working and delivering all of its specifications properly. It is a very critical need in applications that requires emergency reaction. In IoT applications, the system should be highly trustworthy and fast in collecting data, communicating them, and making judgment and eventually the wrong judgment can lead to calamitous scenarios.

J. Handle

To handle all these devices and keeping track of the lack of success, configurations, and performance of such huge number of devices is definitely a trouble in IoT. Providers should handle imperfection, configuration, and performance of their interconnected devices.

K. Accessibility

The accessibility of IoT includes software and hardware levels being endowed at any time and anywhere for service subscribers. Software accessibility means that the service is endowing to anyone who is authorized to have it. Hardware accessibility means that the live devices are convenient to access and are favorable with IoT functionality and protocols.

6. Conclusion

The Internet of Things (IoT) is still in its infancy as an incidence. IoT has components that range in complexity, from simple recognition tags to complex machine - to - machine communication. Internet of things is a new technology which provides many applications to connect the things to things and human to things through the internet. Each objects in the world can be identified, connected to each other through internet taking decisions independently. All networks and technologies of communication are used in building the concept of the internet of things such technologies are mobile computing, RFID, wireless sensors networks, and embedded systems, in addition to many algorithms and methodologies to get management processes, storing data, and security issues. IoT requires standardized approach for architectures, identification schemes, protocols and frequencies will happen parallels, each one targeted for a particular and specific use. by the internet of things many smart applications becomes real in our life, which enable us to reach and contact with every things in addition to facilities many important aspects for human life such as smart healthcare, smart homes, smart energy, smart cities and smart environments. In the near future, old style factories will be disappeared and smart factories will take place of them. Smart factory has a conscious and intelligent structure so that enables information exchange. Smart products are able to connect the whole factory through intelligent actors such as sensors, robots, conveyors, actuators. Developing countries have to eliminate challenges and adopt new technologies in this new era. IoT practices are crucial to provide automation and competitive advantage. The internet of things promises future new technologies when related to cloud, fog and distributed computing, big data, and security issues. By integrating all these issues with the internet of things, smarter applications will be developed as soon. This paper surveyed some of the most important applications of IoT with particular focus on what is being actually done in addition to the challenges that facing the implementation the internet of things concept, and the other future technologies make the concept of IoT feasible.

References

[1] https: //www.tu - chemnitz. de
[2] https: //0keanis. lib. teipir. grxmlui. bitstream. handle pdf
[3] http: //www.gkmit. com
[4] http: //www.researchgate. com
[5] http: //www.guru99. com
[6] http: //data - flair. traning
[7] http: //www.appinventiv. com
[8] http: //www.internetofthingsagenda. techtarget. com.
[9] Mohammed ZKA, Elmustafa SAA. Internet of Things Applications, Challenges and Related Future Technologies. World Scientific News.2017; 67 (2): 126–48.
[10] Farheen Fatima, at el., Internet of things: A Survey on Architecture, Applications, Security, Enabling Technologies, Advantages & Disadvantages. International Journal of Advanced Research in Computer and Communication Engineering Vol.4, Issue 12, December 2015.
[11] http: //energy. gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_ Pages (1). pdf
[12] http: //ieeexplore. ieee. org/document
[13] Smart Grid enabling energy efficiency and low - carbon transition, https: //www.gov. uk/government/uploads/system/uploads/attachment_data/file/321852/Policy_Factsheet_ - _Smart_Grid_Final__BCG_. pdf.
[14] http: //www.ipscoop. eu/internrtofthingsguide/internetthingshealthcare.
[15] http: // www.science direct. com.
[16] http: //gemalto. com
[17] http: //manufacturing. com
[18] Arko Djajadi, Member. Ambient Environment quality monitoring Using IoTSensor Network. Interworking Indonesia Journal Vol.8, No.1 (2016).
[19] D. Bhattacharjee and R. Bera. Development of smart detachable wireless sensing system for environmental monitoring. International journal on smart sensing and intelligent systems Vol. .7, No.3, September 2014.
[20] http: //losant. com
[21] http: //thesai. org
[22] https: //www.researchgate. net/publication/313651150_Internet_of_Things_Applications_Challenges_and_Related_Future_Technologies.
[23] https: //www.researchgate. net/publication/332060553_The_Future_of_Internet_of_Things_IoT_and_Its_Empowering_TechnologypublicationCoverPdf