A Report on the Project

Investigation into various IoT (Internet of things) Architectures, Standards, Alliances

Submitted by
Navdeep kaur Rai

In partial fulfillment for the award of the degree
Master of Science in Internetworking
(From University of Alberta)

Under the guidance of
Juned Noonari

Sept 2017 – March 2018

ABSTRACT

In IoT (Internet of Things) everything will be connected starting from home to appliances, office buildings, vehicles, health and gadgets. Although, this technology is in its early phase but its demand is rising at a rapid pace. It is estimated that till 2025 there will be billions of devices connected. In my project I am going to do discuss about the evolution of IoT and its applications and usage in various fields such as environment and wildlife monitoring, infrastructure management, industrial applications, Energy Management, Medical and Healthcare systems, Building and Home Automation and Transport systems.

In my project I am going to do research about different trending technologies such as 5G, Machine Learning, Big Data, Cloud computing, Blockchain and the Beacon technology and will be discussing how these technologies are correlated to IoT. There will be discussion on Benefits of IoT in different fields such as Healthcare, Agriculture, Manufacturing, Transportation, Finance, Education and effects on communication after opting to IoT services.

Later, in the project there will be discussion on IoT requirements which will cover everything to device such as specification and requirements and the physical devices such as Sensors, Actuators and Gateway and the wireless connectivity mediums and Security requirements. There will be discussion on various challenges and issues that IoT industry is facing at present and the IoT Alliance with its standards and applications in different industries such as vertical and horizontal. In the last, I am going to cover about the prevailing architectures for IoT and will discuss about them.

ACKNOWLEDGEMENT

Firstly, I would like to express my gratitude towards the Almighty God without whose blessing nothing is possible and I would like to show my gratitude towards my mentor Mr. Juned Noonari without whose valuable contribution such as piece of advice, encouragement and significant reviews had helped me a lot to complete this project. I would also like give thank Mr. Shahnawaz Mir for guiding me in choosing my project and for cooperation which has helped me to successfully complete this project.

I would like to thank my parents for their effort of keeping me motivated which has provided me strength to complete my project on time and would also like to thank my class fellows who have helped me with their skills in completing this project.

Navdeep Kaur Rai

Table of Contents

List of Figures

Chapter – 1

Introduction:

1.1 IOT Emergence:

Although, the term IOT (Internet of things) was first coined in 1999 by Kevin Ashton – executive director of Auto-Id center but the recent trending topic had shown its first glimpse in 1832 when Baron Schilling in Russia created the Electromagnetic telegraph – first form of electrical telecommunications that is how the binary system was put into practice. In June 2009, almost after ten years after using the term "Internet of Things" as a main title in his presentation which he made at Procter and Gamble (P & G), he published an article and said:

"Our environment is physical and the societies in which we live are not based on any ideas- all they are based on is results. In this world, we cannot rely on ideas we believe on outputs. Moreover, our devices rely on practicality and not on ideas". [1]

One more thing he has mentioned is that this will help us to know when our device lifecycle is finished and we need the replacement. Development of Internet was considered as best possible form of communication between humans. However, due to recent developments and inventions, technology has reached to a far level – artificial intelligence is embedded in devices by which machines will take over human work load. These smart devices will have ability to interact with both the humans and machines, this is what we will call internet of things era.

1.2 Internet of Everything:

Internet of Things (IOT) – Internet of things is the network of devices (computing, mechanical, and digital) which are connected together through the unique identifiers and have the ability to communicate with each other without requiring the human-to-human and human-to-computer interaction.

The following diagram will give a brief review about the internet of things:

Figure 1- Things connected around the globe taken from https://en.wikipedia.org/wiki/Internet_of_things#/media/File:Internet_of_Things.jpg

1.3 Industrial IoT or Industry 4.0:

The term industrial internet was coined by GE in the late 2012and it is estimated that industrial internet could be a $225 billion industry by 2020. [2] Industrial IoT is the use of IoT Technologies in the manufacturing industries which will transform the manufacturing industries by availing the acquirement and accessibility of the large amount of data at a faster speed and in a more proficient manner than was available before. Industrial IoT constitutes Machine learning techniques, machine-to-machine (M2M) communications and big data analysis which have been the major building blocks when considering the setting up of industrial IoT. [3]

1.3.1 Industrial IoT Benefits:

These data analysis help the companies to track and resolve the problems at a greater speed and thus help in saving time, safety and cost. System operators are able to use predictive maintenance techniques through accessing the data from sensors and automation equipments. These Industrial IoT networks of intelligent devices help company's business leaders to get a full insight of how their enterprise is doing and can help in good decision making. [4]

1.3.2 Industrial IoT Protocols:

There are a range of protocols which help in sharing of data from an edge to the cloud within an industrial internet system and some of them are: MQ Telemetry Transport was developed by IBM but it has now become an OASIS standard, Data Distribution Service for Real-Time Systems (DDS), MQ Telemetry Transport (MQTT), Constrained Application Protocol (CoAP) which is going to be used in some smooth devices such as WSN which will permit them to communicate. Detailed summary of the protocols will be covered in the upcoming chapters. [6]

1.4 Smartness in IoT:

Smartness itself is an important characteristic of IoT like sensor networks and it can be further categorized into object smartness and network smartness. Network smartness is characterized by the following functionalities:

- Layers interfacing with the physical world (i.e. tags and sensors) should have standardization and openness to the communication standards of the communication layers between nodes and the internet.
- Object addressability (such as providing direct IP address) and multi-functionality (i.e. a network built for one application can be used by other applications as well). [5]

Object smartness is the combination of internet and emerging technologies such as near field communications, real-time localization and embedded sensors that enable daily used objects to be transformed into smart objects which can react according to the real time environment.

Now, let’s describe the smartness in internet of things through suitable examples:

- A living room with interconnected devices:

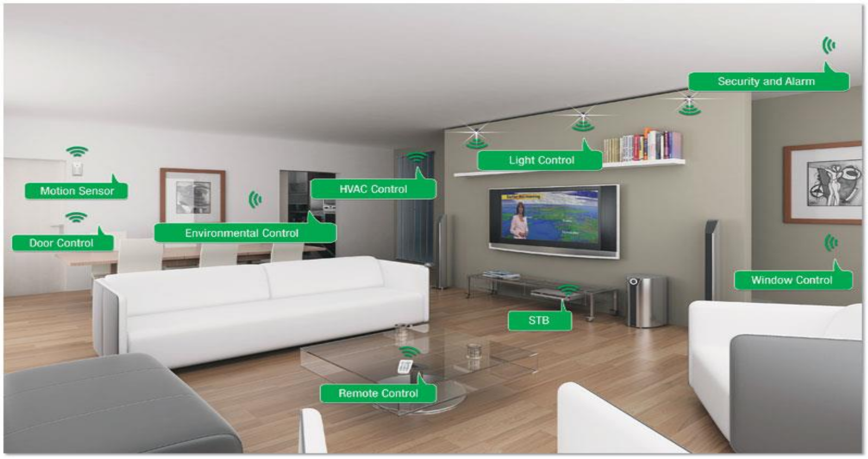


Figure 2 – Room with connected objects taken from http://saphanatutorial.com/introduction-to-internet-of-things-part-1/

Commented [NJ1]: Make sure to provide appropriate references for all the diagrams.

This figure illustrates that when you come in living room to watch TV, light control will automatically switch on lights and TV and remote control will switch to the channels according to your requirement by controlling the STB. Environment control and HVAC control will adjust the temperature according to your body requirement. Window control will always remind you of the necessary items to pick up before you head out from your home. [7]

- Smart car:
  The next picture depicts that a smart car will read the data beforehand and will detect the real-time traffic and will let know the motorist that which route he /she should follow to avoid the traffic congestion. Provide the information related to nearby parking lots, restrooms etc. and will warn of the motorist of the accidental prone areas. It will automatically sense the collision and will apply the emergency brakes if required. [8]

Figure 3 - Connected cars taken from http://saphanatutorial.com/introduction-to-internet-of-things-part-2/

1.5 Market share:

IoT market has started burgeoning from the past decades by having a market value of $44.0 billion in 2011. According to the Forbes, Cisco has predicted its global growth to be 14.4 trillion by 2022 and the 4 industries that will cover more than half of the predicted growth will be manufacturing (27%), retail trade (11%), information services (9%) and finance and insurance (9%). [9] According to the geographic analysis, North America represents the largest market share of the internet of things in 2014. Growths of industrial, automotive and healthcare sectors are the major sources for the growth of IoT in North America. Major participants in the growth sector are Google Inc. , Cisco Systems Inc. , Apple Inc. , Microsoft Corp. , Intel Corp. , IBM Corp. is all from United States. [10]

Figure 1.4 illustrates the IoT growth rate with estimated number of active devices until 2018. Investors from developed and developing countries come forward to invest in this new wave of technology i.e. IoT which indicate the strategic planning of governments to keep them update with latest trends in technology and its future impacts on industry. For example, the IoT European Research Cluster (IERC) has conducted and supported several IoT projects by considering their special requirements such as end-user and applications requirements.

Different countries are stating their different IoT milestones to be achieved in the near future such as Singapore government has announced itself to be a first smart nation by investing in smart transport systems, developing the e-government structures, using the surveillance cameras and other sensory devices to obtain data and extract information from them so as to act smartly to deal with every sort of problem. Indian government has planned to create $15 billion IoT industry and has also planned to develop over 100 smart cities that would require an investment of over USD 150 Billion. [5]

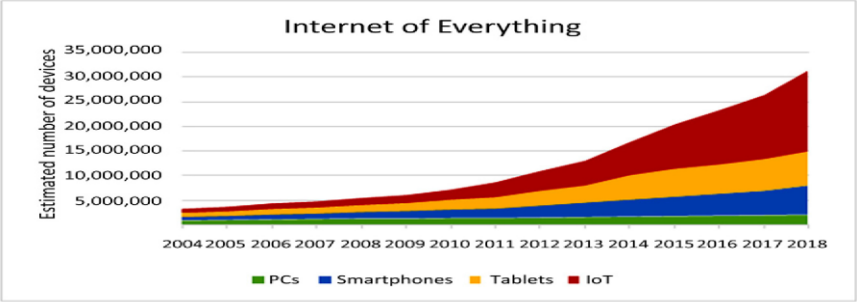


Figure 4 - Graph depicting connected devices per year taken from Internet of things: Principles and Paradigms(BOOK)

Chapter -2

Why we need IoT:

With connected devices life would be easier. There are certain areas which need IoT monitoring and controlling so as to lower costs, time saving and quality purposes. While surfing internet like opening Gmail or Facebook we come across certain ads or articles which are related to our interest or favorites this is because of IoT and machine learning. As devices try to learn our area of interest and will open or provide recommendations of the similar content in the right section. Same happens in case of YouTube, it learns what your music preference is and recommend according to that. IoT can be a boom in the following mentioned sectors: [27]

2.1 Environmental monitoring:

2.1.1 Ways IoT revolutionize farming:

IoT can help in measuring the water or air requirement for the growth of plants. It can help to tell what kind of soil is required for vegetation. The devices used for agriculture purpose will keep a track of what kind of fertilizers is required and what has been already added to the soil so as to maintain fertility in soil.

Let us consider the ways IoT can transform agriculture sector:

- **Livestock monitoring:**

  IoT devices constantly monitor the livestock and if there is any change in the preset parameters then user is sent an alert through text or email. A company called Moocall has developed a battery-powered sensor that continuously monitors the pregnant cows to send the notification related to labor to the farmer. Battery of sensor lasts for 2 months and alerts the farmer by sending text if the battery level drops to 15%.

  Second application of livestock monitoring is Cattle watch which is used to provide real-time insight of animal behavior like if there is any change in eating or drinking habit, body temperature and its location. It even alerts about the presence of any predatory animal over the location.

- **Precision farming:**

  IoT sensors can help farmers to make smart decisions on the amount of air quality, water supply, weather suitable for crop and fertilizers required for crop growth. There are different researchers and experiments going around the world to shift the farming to precision farming. One such example is providing information regarding accurate water supply for each crop by a company called Cropx. Different algorithms and patterns are used to differentiate between hilly and flat areas. Another example which can be taken into consideration is by Analog Devices Inc. which are working on a project called Internet of Tomatoes involving Microelectromechanical systems and sensors. ADI is planning to integrate hardware devices with software applications so as to provide complete solutions to farmers related to farming.

- **Autonomous tractors:**

These self driving tractors came to the market before the self-driving cars. These tractors help in saving time and money by performing several tasks such as spraying insecticides. [30]

2.1.2 Required for natural disasters:

IoT is required in tsunami or earthquake prone areas where the residents will be alerted before the tragedy so they can escape to safe areas or they can avoid building their homes or offices in such areas. This will reduce the number of loss of lives and less damage to property. These natural disasters come without warning so there is a need for early detection.

Most of the severe earthquakes are experienced by Japan, which caused a extensive loss of property and lives. In 1995, Kyoto earthquake of magnitude 7.3 caused a death toll of 6,434 which forced Japan’s government to build a seismic warning system cost of 1 billion dollars. It is effective but is not affordable by the developing countries. So there are some startups which are planning to build at a warning system at a lower cost like zizmos.

This warning system will work by connecting multiple sensors to a central server. These multiple sensors will detect the motion of earthquake epicenter and will transmit warning to the nearby residents. Earlier the cost of sensors was significantly high but it has reduced over a last decade because of the advancement in smart phones and wearable technology. [28]

Here is the list of some smart and hand-held IoT solutions which can make the life of people safe and less vulnerable to such disasters:

- **Brinco:**

This is the first IoT driven device that warns its user about the upcoming tsunami or earthquake personally. If accelerometer of the device senses any vibration it sends the information immediately to a private cloud service of Brinco which further absorb this information with other seismic networks to obtain the result. If the output obtained is positive, then it sends the alarming notification to its users. This information can be further shared by the use of social networking sites.

- **Brck:**

This device is used in poor infrastructure areas where 2G communication still persists. This device is compatible to work with solar energy and hence proves to be a significant advantage to the disastrous prone areas where continuous power flow is still a dream. Smart phone users can easily connect with this device and share the available information with the other wi-fi connected devices.

- **Grillo:**

  Grillo is another revolutionized device in the race of IoT driven products. It is invented in Mexico and is a App supported product. This app has to be installed in user's living or working area which is further connected with Grillo's sensor networks. Whenever there is abnormal vibration in the ground it is automatically sensed by the Grillo which further connects with its network and verify it. When it receives a positive result it sends a push notification to its user as a warning.

- **Citizen flood detection network:**

  It is an open source IoT-driven infrastructure that is connected with flood sensing nodes. Node is usually located under the bridge of river which senses the level of water regularly after 5 minutes and if it senses that water level has exceeded the pre-defined safety standards then mapper-service will change the color of map to yellow or red and sends the notification to its users about the upcoming disaster.

- **Flood beacon:**

  Flood beacons are designed in such a way that they continuously monitors the water level by floating over the water surface and whenever it senses any change in the water level it sends a push notification to its user. Xively is used to store all the information of water body for further analysis.

- **Floating sensor networks:**

  This floating product has its own Accelerator sensor and Global Positioning System. If there is any sudden change in the level of water it sends alert notification to the nearby residents through web.

- **Lightning detection:**

  Heavy lightning takes many lives around 24,000 per year. To overcome this problem, new light detectors are developed that can sense a small change in gamma blast far from 40 kms. It senses data after every 15 mins. It can filter the information so as to send accurate and instant information to the local people for their safety through internet.

- **Alarms:**

Alarms (Assessment of Landslides using Acoustic Real-time Monitoring Systems) are an application which is used to provide warning for landslide to be occurred. Accelerator sensor is deployed over the areas where landslides occur most frequently. Sensing any change in movement and density of ground, warning is sent to locality.

- **Myshake:**

  This is an app based service provided to its users for the detection of earthquake. Whenever it senses any vibration in the ground it sends the information to Berkeley Seismological Laboratory and its location via GPS for the verification. If the verifies information is positive, alert is sent back to user. [29]

2.1.3 Required for wildlife Monitoring:

As the humans are becoming more money minded, so it is difficult to preserve the wildlife. For some people, money has only become the motivation for their survival. They are selling animal body parts to fill their coffers such as selling elephant teeth, rhino horns, tiger bones and skin for leather and medicinal purposes. Even some people experiment medicines on animals so as to see their effect on animal body which has raised the concern for protecting these animals from such humans.

Conservative agencies of Tanzania have developed a LoRa sensor which is used to keep track on endangering species such as black rhinos. These sensors keep the track of animals within sanctuary and providing minute-to-minute details to security personnel so as to safeguard animals from poachers.

2.2 Managing infrastructure:

IoT can help in finding defects or faults in infrastructure such as in bridges, machines, roads and railway tracks so to avoid the loss of lives. Some of the IT organizations have started embedding these networked sensors like energy companies use to measure vibrations in turbines. These sensors are programmed in such a way that they could tell when the machine needs maintenance so as to avoid the productivity loss.

Jet engines have embedded sensors to measure the physical parameters such as temperature, pressure and quality to increase the efficiency of product. Change in these parameters can inhibit the manufacturing process.

2.3 Industrial applications:

Industrial applications can play a significant role in increasing the marketing of the product and improving its quality. These applications can help as if what minor changes can enhance the potential market.

There are some of the companies which have already started using sensors to depict maintenance beforehand:

- **ABB firm:**

  ABB is a robotics firm which uses sensors to continuously monitor these programmable machines so as to alert about their maintenance before the breakage of their parts.

- **Airbus:**

  Commercial jetliners have millions of components and assembling these components costs billions of dollars. If any of the components is embedded wrong it will be an enormous loss to the company. So as to avoid such losses, Airbus has launched a new manufacturing process called Factory of future to boost productivity. Company has provided workers wearable technology such as smart glasses and equipped tools with sensors to eliminate errors

- **Amazon:**

  Company is experimenting on how much humans and machines can collaborate. Amazon is planning to bring drones (which can carry information related to the sensors and machines to visualize if the work is being done as scheduled) in the picture for delivery purposes and using the kiva robots (which were acquired for $775 million in 2012) for finding the shelves of products and reducing human workload. These kiva robots have reduced the operational cost by 20%.

- **Boeing:**

  Boeing is using IoT technology to improve the efficiency of its products and is deploying more and more connected sensors in its planes to fetch real-time data.

- **Bosch:**

  Employees used to spend quality amount of time in finding appropriate tools for the given project which somehow affects the productivity. So as to avoid such treasure hunt, company planned to embed sensors on the tools which made tracking more precise.

- **Caterpillar:**

  Caterpillar, now known as Cat is helping the marine sector by the use of IoT and AR (Augmented Reality). It sends notification about the fuel level and if filter needs replacement through AR app. It can also provide basic instructions for changing the filter through this app.

- **Fanuc:**

Fanuc, a robotics based firm has been known for zero downtime. Company is using sensors along with cloud-based analytics to predict the failure of a component or robotic part before it can inhibit the production.

- **Gehring:**

  Gehring uses IoT to provide visualization to its customer about the company operations so as to make its customer satisfied before they place orders which has come as a boon for company in efficiency and production matters.

- **Hitachi:**

  Hitachi is a Japanese based company with 16,000 employees. It mainly focuses on developing connected products such as connected trains which will be its new service and it has its own IoT based platform called Lumada which has enhanced production of infrastructure in the sectors of steel manufacturing, electricity and many other industries.

- **Komatsu:**

  It is also a Japanese based mining company which is about to bring self-driving trucks in this smart world. This company has linked all of its national and international firms with robots so as to keep track of operations in real-time.

- **Kuka:**

  It is a German based company which has linked its hundreds of robot to a private cloud so as to produce 800 vehicles each day.

- **Maersk:**

  Danish shipping company has welcomed IoT to keep the tracks of any spills from containers, routes of ships and fuel consumption. Spilling occurs mainly if the temperature is out of control so to avoid such circumstances and losses, Maersk has provided sensors and data analytics to guide the company how to store and locate these empty containers.

- **North star BlueScope steel:**

  Company uses wearable technology to track the health status and safety of employees. These wearable help to track the pulse rate, blood pressure, body temperature and the functioning of body so that project managers could acknowledge when the employee need break and also to avoid the dangerous events such as environmental temperature and radiations persisting in the workplace which could cause suffocation and may further lead to loss of life.

- **Rio Tinto:**

  An Australian mining company which is using driverless trucks for transportation and an innovative drill technology for helping the worker to locate the drilling area for ores. They are planning to introduce the driverless ships as well. All the mining operations are conducted efficiently with the help of programmers and technicians.

- **Stanley Black and Decker:**

  Company has deployed the smart factory program in its construction sites so as to enable workers to locate tools and to track the ongoing progress using radio signals. Company has recently launched a connected battery that only monitors the battery percentage but it also turn off the tools if any offender tries to misuse them. [31]

2.4 Energy Management:

As the population is araising so is the energy consumption. So here comes the need of IoT to utilize the energy more efficiently with the use of some sensors. Most of the companies are focusing on this area as some of the revenue of the company is used in unnecessary utilization of power and other resources. So as to avoid such over consumption of power, companies have started deploying the remote controlled sensors which will turn on the lights of conference room only if someone is present else it will automatically turn off, same is the case for air conditioners like if someone has turned on the AC but has forgot to turn it off, the automated sensors deployed over there will take care of such negligence by turning it off after the room temperature has reached the desired temperature level. So such technological innovations save a lot for company.

In 2015, GE has launched two energy related initiatives – Predix and current. Predix will take care of the massive amount of data generated by IoT devices and make the significant use of it. Current will look after the unique requirements of customers and will control the power required for energy driven areas. [32]

There are certain initiatives which can help countries to deal with energy management issues:

- **Smart grid:**

  Smart grid technology is one among the upcoming innovations that would enhance the power efficiency and quality by using renewable energy resources such as solar power and wind energy which have lower operational and maintenance costs. This initiative will further help to deal with climate change as well.

- **Smart garbage collector:**

Waste collection is of high priority as the current systems used for garbage collection are inadequate. So there is need for implementing smart bins. As in previous systems, trucks are scheduled to collect the garbage from the city but sometimes the collection is too high that the street needs more trucks for collecting their garbage. So there is a need to embed sensors in the bins which will provide real-time data to the garbage collecting companies so that required action can be taken. This will help in challenging the persisting environmental challenges and to cope up with them.

Different companies are investing in smart bin and market is expected to grow from 57.6 million dollars to 223.6 million dollars in 2025. In 2016, Cisco along with TDC has agreed to deploy this waste monitoring system in Denmark. Even the traffic lights are equipped with sensors that send information to the town committees.

Another solution in this arena is solar-powered Bin operating on the Wi-Fi. This is little expensive project as for this city has to be provided with Wi-Fi connectivity. Although, in June 2016, UAE has deployed this Bin in one of its city but to achieve sustainability goals there is need to deploy these Bins all around. [33]

- **Smart meters:**

Smart meters have already been the talk of industry from the last 3-4 years. According to Business Intelligence report, it is expected that smart meters market will exponentially rise from 450 million devices to 930 million devices in 2020 which is almost double in 5 years. These meters help to track and control the energy consumption and reducing carbon emissions in air thus taking care of environment as well. Aidon, the most advanced company in the use of smart meters has now turned to smart SIMs for better connectivity. Smart SIMs provides better connectivity as they are programmed in such a way that they choose the best available connection.

2.5 Medical and Healthcare systems:

IoT devices can help in monitoring the health of a person such as pulse rate, body temperature and blood pressure so to avoid any major health issues. IoT has become the need which need to be adopted looking at the different perspectives.

- **To monitor patient health:**

Most of the patients are more comfortable and easily recover in home atmosphere rather than on hospital beds. So with the help of wearable technology, doctors can track the health of patient and can respond to the events to be occurred beforehand or we can say prepare himself for the upcoming risks and taking care of them.

- **To monitor medical assets:**

IoT technology can help in finding the medical equipments to the staff so that they can provide more attention to patients rather than tracking the supplies and medicines. There should be sensors connected to tools to track them and should provide the required information.

- **To maintain vital equipments:**

  Maintenance plays a significant role as all the critical medical equipment should be taken care beforehand, before the patient needs it. Sensor technology should look after if there is any crack or update required for the equipment's software. Everything should be pre-planned.

- **Track equipment usage:**

  Equipments should be tracked with the help of sensors as if how they were used on patients. Proper tracking should be done from hospital bed to washing stations so as to figure out that the equipment was used in right order and in right direction. [34]

2.6 Building and Home Automation:

As people are already stressed with lot of other things, they don't have time to think about switching on or off devices connected at home or buildings. So there comes a need to connect the devices to internet and make them automated. This automation can save time and energy thus people have to pay low electricity bills.

Let's discuss an example where IoT becomes necessity- suppose you are going to work from home and in hurry you forgot to shut down air conditioner and light. In the midway you remember that you forgot to shut off. So here comes a point either you will travel all the way long back to home or remain the lights and air conditioner on for the entire day which in one or other way will lead to more energy consumption such as paying more electricity bill or wasting fuel if coming back and getting late to work. So as to avoid such problems proper sensors should be embedded in home to control each and every device of home such as TV control, lightning, security system, thermostat, air conditioning and street lights which work according to the human need.

There are certain devices in the market such as eccobee3 and Philips Hue. Eccobee3 controls the temperature of room and Philips Hue to control lightning. August smart lock is used to provide home security which works through Apple's Homekit.

2.7 Transport systems:

As there is lot of traffic on roads, so there is a need to manage it through a systematic approach or a technology. IoT an emerging technology which has expanded its wings in every sector needs to be deployed in transport sector as well. Finding parking spaces is a difficult task nowadays.

According to the data calculated by a research it is estimated that around 30% of traffic is caused by the motorists who are looking for parking space in the city. Not only the traffic, cars are consuming thousands gallon of gas and producing hundreds of tons of carbon dioxide in the atmosphere just because they are not able to find the parking space spontaneously. So to encounter such things IoT can come as a savior for both the environment as well as people. Sensors should be embedded in the parking lots which gather the real time data such as if the spot is occupied or empty. This will minimize traffic congestion and environmental deterioration.

More traffic on cities can prone to accidents. Bringing autonomous vehicles can help to overcome these accidents as vehicles are trained or sensors are embedded in them in such a way that they work efficiently. These driverless vehicles will decrease the need of parking lots and traffic lights. If an accident occurs, sensors on these driverless vehicles will send an alert to nearby vehicles to take a different route so as to reach their destination safely and on time. If these vehicles find any emergency vehicles near to them they send an automatic alert to the nearby vehicles thus providing a way beforehand so as to avoid any casualty. According to the research conducted by Morgan Stanley, IoT could avoid the accidental deaths by 30,000 and injuries by 2.12 million per year. [36]

Another example of time saving and finding best route is by Google maps. Let us consider one more example where IoT can make a difference.

Amsterdam Airport - fifth among the top 10 largest airports of the world is so busy that it is difficult to maintain minute-to-minute coordination with aircraft, crew and ground staff. To load the baggage in the plane or off the plane there is a need of Carts which should be at right place at the required time unless the next flight will delay or will reach late at next destination causing trouble to both the arriving and departing passengers. Ground crew members need to be aware of the location of carts whether it is in maintenance site or some other location. So as to track the real-time data of these carts we need sensors. [35]

Chapter-3

Enablers:

IoT is a system of connected things and devices which can transmit, store and receive data. IoT is itself an enabler that can make the devices to talk to each other such as street lighting system which can dim or switch on/off lights based on the outside environment and the information embedded in them. A number of technological advancements have led to the rise of IoT. Now let us discuss some of the key features that have enabled the growth of IoT:

- **Cheap sensors:**

  Earlier, sensor prices were quite high around $1.30 in the past decades making difficult for companies to embed a large number of sensors for a particular purpose. But now the prices have significantly dropped to 60 cents which is almost half of the previous price thus making the way for connected devices to work efficiently by providing regular monitoring and sensing.

- **Cheap bandwidth:**

  Considering the data of previous 20-30 years, it has been noted that cost of bandwidth has declined abruptly thus making 40 times cheaper than the previous years.

- **Cheap processing:**

  In the early 2000's processing cost was too high which was one of the inhibiting factor in growth of technology. As the processing costs declined precipitously by a factor of 60X it became easier to connect the devices and make them smart enough so that they can know what to do with the coming data.

- **Smart phones:**

  Smart phones have also been the reason behind the growth of IoT as they serve as remote controller for connected devices such as home, cars and health.

- **Wi-Fi availability:**

The unlicensed spectrum available everywhere has also been the driver behind the growth of IoT. Now the user does not have to pay much high fees to the carrier as this wireless connectivity (Wi-Fi) is available for free or at a minimal price.

- **IPv6:**

IPv6 can support multiple connected devices at a given time as it has bundle of addresses available around 3.4*10^38 addresses. [41]

Now, let us discuss some of the key technologies which have enabled the growth of IoT in the market. Without the help of these technologies, it was a difficult affair to conduct IoT to that level where devices are connected, talking to each other and enacting to the requests as they come.

3.1 5G:

3.1.1 Definition of 5G:

5G is defined by a new radio access technology in concurrently used with the multi-layered networks that can handle high throughputs up to 10 Gbps and increased data volumes at a very low latency as low as 1 ms. 5G is term which is used to describe the mobile networks which are beyond the 4G LTE mobile networks and it is further assumed that these 5G networks will not be available until 2020. [11]

3.1.2 How 5G differs from previous mobile networks:

While looking back it can be concluded that every G runs for a full cycle of 10 years before the next G supersedes it. 2G networks were designed for voice; 3G for voice and data; 4G for broadband experiences and 5G will provide a high data rates and low latency which will enhance the IoT connectivity. [12] The next generation wireless network will mark its growth beyond mobile internet to massive IoT by the next 3-4 years. The main advancement in the upcoming generation is not only data speed improvements but will also improve the performance of critical communication use cases as compared to today's 4G and 4.5G.
4G is good till now but it won't be able to support the future IoT based applications which require low latency. For example, emerging autonomous cars and intelligent transport both require low latency.

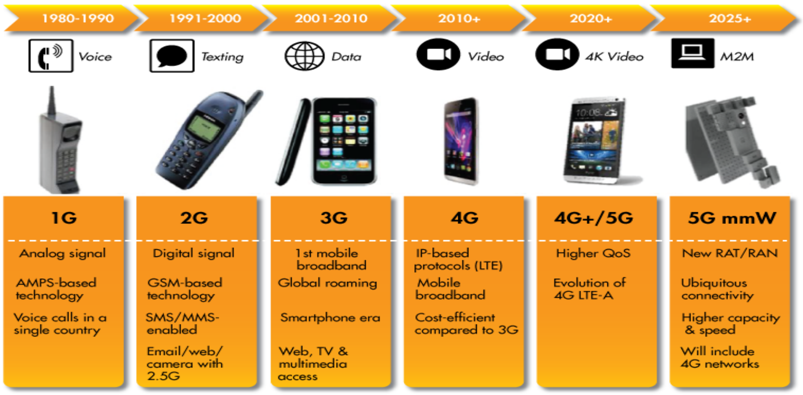


Figure 5 – Evolution of Mobile networks taken from http://www.mwrf.com/systems/top-5-rf-technologies-5g-IoT

3.1.3 Present spectrum:

The previous generations use the so called orthogonal multiple access. As 2G networks are based on Time Division Multiple Access (TDMA) in which each second is further subdivided into lot of short time slots and each user has its own time slot and within that mean time other users cannot interfere or connect. So such techniques cannot support the IoT applications as in IoT we will have lot of devices connected to each other and we will have to allocate time slots to each of them which is difficult according to the present spectrum as of limited bandwidth and time slots which inhibits 5G to rely on Orthogonal multiple access technique. [13]

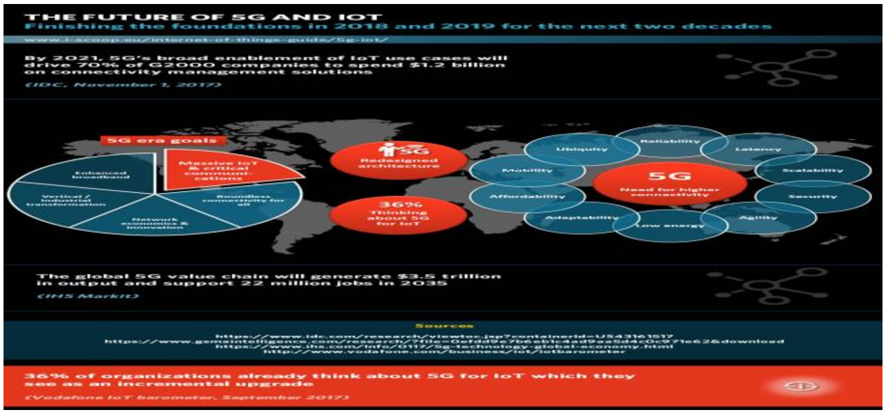
3.1.4 New Spectrum requirements:

Lot of research is going on how to develop non-orthogonal multiple access technique which will have number of users using the limited bandwidth channel as this technique will provide better trade-off between system throughput and user fairness. Another way to overcome this problem is using cognitive radio technologies. By using the radio technologies we can allow multiple users to use one particular channel at a given time. If this connection of multiple users remains good with base station, also called as Node B in UMTS (Universal Mobile Telecommunications System), then we can achieve a large data rate. Initially the users might experience the performance deterioration but it can be handled significantly if power control mechanism is carried out. Massive MIMO and full duplexing can also prove significant for dealing with such spectrum crunch.
Moreover, 5G will support both uplink and downlink transmissions. 5G will support the downlink transmissions whenever the device is underground or deep inside water and

will support uplink transmission by the use of non-orthogonal multiple access techniques. [13]

3.1.5 Future of 5G and IoT:

5G will bring the authenticity, latency, affordability, mobility and agility that would be required in various IoT applications and services. Figure 1.5 illustrates that IoT will bring numerous jobs up to 22 million by 2035.



THE FUTURE OF 5G AND IOT

Finishing the foundations in 2018 and 2019 for the next two decades

www.i-scoop.eu/internet-of-things-guide/5g-iot/

By 2021, 5G's broad enablement of IoT use cases will drive 70% of G2000 companies to spend $1.2 billion on connectivity management solutions

(IDC, November 1, 2017)

The global 5G value chain will generate $3.5 trillion in output and support 22 million jobs in 2035

(IHS Markit)

Sources

https://www.idc.com/research/viewtoc.jsp?containerId=US43161517
https://www.gsmaintelligence.com/research/?file=0efdd9e7b6eb1c4ad9aa5d4c0c971e62&download
https://www.ihs.com/info/0117/5g-technology-global-economy.html
http://www.vodafone.com/business/iot/iotbarometer

36% of organizations already think about 5G for IoT which they see as an incremental upgrade

(Vodafone IoT barometer, September 2017)

5G era goals
Enhanced broadband
Massive IoT & critical communi-cations
Vertical / industrial transformation
Boundless connectivity for all
Network economics & innovation
5G
Redesigned architecture
36%
Thinking about 5G for IoT
Ubiquity
Reliability
Latency
Mobility
Scalability
5G
Need for higher connectivity
Affordability
Security
Adaptability
Low energy
Agility

Figure 6 – Future of 5G and IOT taken from https://www.i-scoop.eu/internet-of-things-guide/5g -IoT/#The_future_of_5G_and_IoT_8211_and_the_future_impact_of_5G_beyond_IoT/

The following Figure 6 describes about the adoption of 5G by the population; as we can see that initially in 2020 only 8% of population is excited about 5G but as the time passes it follows an increasing upward trend. We can visualize that by 2025 this value will enlarge up to 34% (1.1 billion connections). [14]

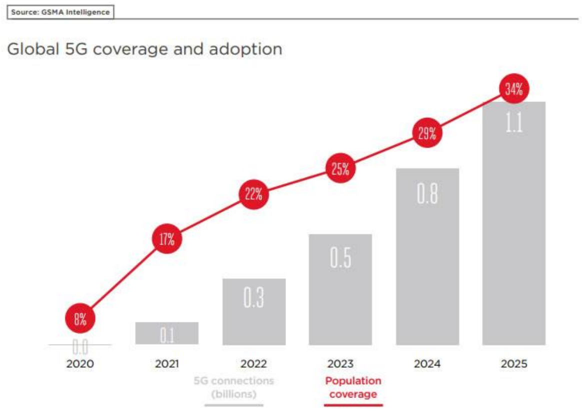


Figure 7 – Global 5G coverage and adoption taken from from https://www.i-scoop.eu/internet-of-things-guide/5g -IoT/#The_future_of_5G_and_IoT_8211_and_the_future_impact_of_5G_beyond_IoT/

3.2 Machine learning:

3.2.1 Machine learning:

Machine learning was defined in the early 1959 by Arthur Samuel. Machine learning is the subset of Artificial Intelligence which provides machines the ability to learn different algorithms and improve its functionality via learning from the past experiences without being specifically programmed.

3.2.2 Machine learning revolutionized IoT:

Machine learning has revolutionized IoT in three different ways:

- **Making data useful:**

The gigantic amount of data generated by IoT has been combed by the machine learning algorithms so that no human could have easily got through over it in a year or spending a lifetime at work. Machine learning not only sort companies through preexisting data but also do predictive analysis to predict the future market trends and meet the customer requirements successfully.

- **Making IoT more secure:**

Machine learning algorithms are helping to scour the challenges faced by the IT officials such as cybersecurity analytics. These analyses help the industry to solve any problem which may be a labor problem – unable to attract the enough human resources so as to meet the requirements of their wealthy clients or by finding IoT vulnerabilities. Machine learning is used to monitor and analyze the data exchange and foresee the threats and crimes before they could happen.

- **Expanding the scope of IoT:**

Machine learning is concurrent with developing and programming the mobile world. Not only the IoT is interested in connecting the devices, machine learning has benefitted the autonomous vehicles, smart cities and factories. It has easily integrated into IoT's platform. [15]

3.2.3 Machine learning applications in IoT:

- **Cost saving in industrial applications:**

  This application can be further described by taking an example from mining company, Goldcorp that uses very large vehicles to pull away materials but when these vehicles malfunction it costs company loss of $2 million per day. Company is now using machine learning so as to predict when the machine needs maintenance before it collapses and to avoid the productivity loss.

- **Shaping experiences to individuals:**

  We are all familiar with machine learning applications in everyday life like Amazon and Netflix both uses machine learning to the preferences of their customers and provide better services to them through product suggestions and recommending movies and shows. Nest thermostat uses machine learning to learn about the preference for warm or cold temperatures and it automatically adjusts the temperature when a person reaches his home or wake up in the morning. [16]

3.2.4 Contribution of machine learning in industrial Internet of things:

Industrial internet of things has already restructured many fields of industry such as manufacturing, automobiles and healthcare. But the real value cannot be achieved until machine learning is connected to sensors.

According to Forbes report, Cloud computing* has been considered the biggest enabler of connected devices and enterprise IoT. The key driver behind the increasing growth of IIoT is the availability of cheaper storage and the computing power.

Cloud computing: storage of information over internet instead of hard drive is what we call as cloud computing. Some of the common examples of cloud computing are Google Drive, Apple iCloud and Amazon Cloud drive. [17]

Earlier, for industries it was easier to capture data from sensors and devices but considering the customer's point of view it was found to be cost consuming for storing such massive datasets. Although, after providing the reliable storage facilities, computing horsepower required for processing these datasets were found to be missing which were critical according to business requirements. Hence, cloud storage was accepted by many industries and providing them the benefit of big data and big compute capabilities offered by large public providers which became an important factor in adopting IIoT in big enterprises.

One of the important features of machine learning is that it groups the similar data points from existing datasets so as to predict the value of future data points by using the advanced algorithms. These algorithms can predict the future values of sensors connected with IoT devices from the historical information stored in cloud. [18]

3.3 Cloud computing:

Cloud is also a key enabler and it is found that nearly 55% of developers find the connectivity to devices through cloud. Nearly 26% of the IoT developers rely on cloud computing according to the recent survey report. At present, only 37% of IoT applications are built using cloud and this number will escalate to 50% in the next couple of years. [37]

3.3.1 Role of Cloud computing in IoT:

Cloud computing and IoT both have a dependency relationship with each other as IoT is used to connect devices and cloud computing is used to store the huge amount of data generated by these connected devices. Amazon web services, one of the most frequently used IoT cloud has pointed out the following benefits of using cloud computing:

- Resource availability is quick.
- Cost-effective as it saves money on operating data centers.
- Provides the infrastructure capacity needs.
- Can make the applications developed in minutes.

3.3.2 Fog computing:

Fog computing is the upcoming version of cloud computing as it will provide a way by which we can directly store or process data on local computing device rather than on cloud or data center. According to the business insider’s report currently only 570 million devices are using fog computing which will show a tremendous growth to 5.8 billion in 2020. Fog computing is a power source for those IoT devices which don’t have their own computing power. So, such devices can rely on fog computing to process and collect information rather than relying on cloud. Under this model, interconnected devices send data to a nearby edge computing device such as gateway, industrial PC or micro data center which processes and analyzes this data. [19]

3.4 Big data:

Internet of things is going to generate a massive amount of data which will impact the big data universe in such a way that it will force the companies to reform their current systems via upgrading their tools and technology so as to store such ample amount of data. One way is to move to platform-as-a-service model which provides more flexibility, scalability, compliance and a sophisticated architecture to store all the precious IoT data.

There are different models available to store data – private, public and hybrid. If the data is sensitive then private cloud is the best option for storing such data otherwise public or hybrid any can be used. Amazon web service cloud is an example of public storage of data.

The most important step in storing the IoT data is being able to receive events from IoT-linked devices which can be achieved through connectivity. Devices will be connected by Bluetooth or Wi-Fi which will need to send messages to brokers about the available data by using different protocols such as MQTT, HTTP. One of the popular open-source brokers available is Mosquito. When data has been received, next step is to store it by finding the suitable technology. Most of the companies use Hive and Hadoop for storing data but NoSQL databases are better as they offer low delay, high throughput, more flexible and gives user the option to add new events easily.

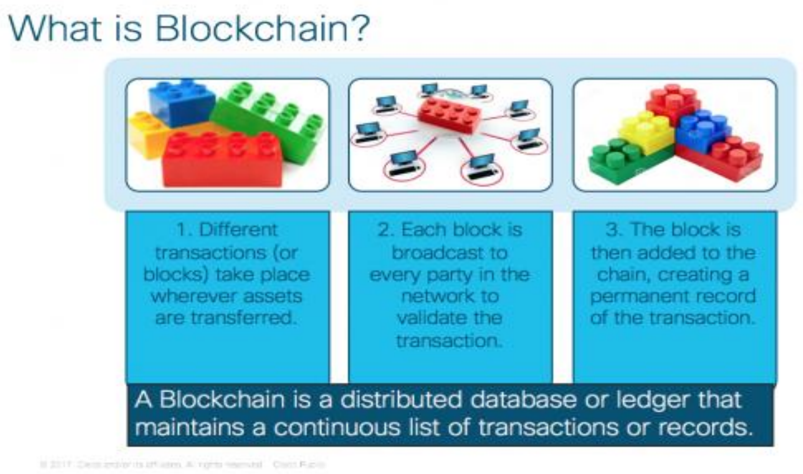
Data generated by IoT devices will be of different forms such as raw data, processed data and communication protocols which will carry different security risks along with them. Multi-layered security and proper segmentation of network will enhance the security of the network. Properly configured will follow a policy to check which of the devices are permitted to connect. Network segmentation can be done by software-defined networking technologies and the networks segmented by these technologies can be used for point-to-point or point-to-multipoint encryption.

Extracting and managing such big amount of data is a challenge in itself. Analyzing of data should be done on the basis of three parameters – infrastructure, performance and future development. Future development and right–size infrastructure can be achieved by following a hybrid approach and the performance can be maximized by connecting a single-tenant physical server should be connected to single customer. [20]

3.5 Blockchain:

3.5.1 Definition of blockchain:

Blockchain is an online database that maintains the records of transactions or growing set of data. It is a public ledger: distributed system that is no single person holds the authority on blockchain technology. Transactions done by this system are immutable and meddle-proof that is they cannot be deleted or copied. All the participating nodes have a copy of chain not transactions and previous data cannot be altered, if someone wants to alter the block it requires collusion of network majority.



What is Blockchain?

1. Different transactions (or blocks) take place wherever assets are transferred.

2. Each block is broadcast to every party in the network to validate the transaction.

3. The block is then added to the chain, creating a permanent record of the transaction.

A Blockchain is a distributed database or ledger that maintains a continuous list of transactions or records.

Figure 8 – Blockchain transaction process taken from https://blogs.cisco.com/sp/could-blockchain-technology-become-the-mainstream-platform-for-digital-transactions/

3.5.2 Blockchain existence or history:

Blockchain concept was brought into existence by a person or group known as Satoshi Nakamoto who published a research paper regarding electronic cash payments that will be sent directly to receiver without going through a financial institution. In 2009, an open source program was implemented with 50 blocks of coins. Anyone can install that open source program and become a part of this Bit Coin peer-to-peer network. Bit Coin is also known as cryptocurrency. [21]

3.5.3 Types of Blockchain:

There are two main types of Blockchain:

- **Public Blockchain:**

  Data is available to read or write. Some Blockchains give the limited access either to read or write like Bit Coin offers access only for write.

- **Private Blockchain:**

  This Blockchain consists of known and trusted participants which can do both the tasks – writing and reading. [22]

3.5.4 Blockchain revolution over last decade:

Blockchain has innovated a lot over the last 10 years.

- First innovation in the Blockchain was Bit Coin which is now used by millions of people for doing the payments digitally and is currently hovering in the market with a value of 10-20 billion dollars.

- Second innovation was called Blockchain which was to make clear that the technology on which Bit Coin relies could be separated from currency and can be used for other organizations. Most of the financial institutions are busy in doing research on Blockchain and is expected that 15% of banks will start using Blockchain in near future.

- Third innovation was Smart contract, constituent of second generation Blockchain called Ethereum, which built small computer programs related to financial functionalities such as providing loans or signing bonds in spite of cash-like tokens of the Bit Coin.

- Fourth innovation is proof of stake. These Blockchains are more authentic by proof of work. In this group with highest computing power is the decision taker. These groups are called miners which provide security in the exchange of cryptocurrency payments.

- Fifth major innovation is called as Blockchain scaling. Presently, each and every computer is busy in processing the each transaction in Blockchain which makes the processes to work slowly but by scaled Blockchain these processes will speed up by figuring out how many computers are required for each transaction so as to avoid the traffic jam while processing each transaction. These scaled Blockchains will be a tough competition for the payment middlemen companies of the banking world such as visa and swift. [23]

3.5.5 Key areas where Blockchain can transform IoT:

- **Improving workflow and providing spontaneous reviews:**

  Blockchain technology is highly significant in shipping industry. It helps to control the documentation at each step of protocol as supply chain is highly complex and inter-communication hinders it. Calculations proved that out of all the transportation costs one-fifth is associated with processing of documents and administering them. It provides a source of authentication that no document can be deleted or altered without the consent from network or company.

  Some of the companies like IBM and Maersk have started to implement Blockchain so as to make systems more transparent and to improve inventory management by saving millions of dollars.

- **Managing life cycle of resource via Blockchain:**

  Blockchain can be used to maintain different sets of records such as history, maintenance, breakdown and ownership of resources. The above mentioned parameters are often left unmeasured and lead to critical failures. So, as to avoid such damaging events these parameters can be put into practice via IoT tracking and can be recorded by Blockchain which can provide more reliable functionality to all stakeholders. [24]

Filament is also investing in IoT and Blockchain covering the major sectors such as agriculture, manufacturing and oil firms. It uses a wireless technology, called Taps for data collection and resource monitoring without the use of any central network authority or cloud. [25]

- **In managing up infrastructure:**

  Blockchain technology can help in tracking the several suppliers and vendors via restructuring FCAPS (fault, configuration, accounting, performance, and security) model across multiple domains.

- **Promising the safe and reliable food supply chain:**

  Blockchain technology can help in tracking and tracing the ingredients by simplifying the complex and multifaceted processes from multiple sources on a single distributed system which gives an instant review of each step on a chain. In this way, quality issues will be addressed more precisely and accurately. [24]

3.5.6 Blockchain and IoT future:

As the devices are becoming smarter with the help of IoT, so is the need of adopting new technologies to make the IoT devices more secure which can be done by Blockchain. Blockchain could make the data more autonomous. Blockchain relies on peer-to-peer network model which help in availing the streamed data accessible for users who can tokenize the value of this real-time data. This Blockchain streaming platform “Streamr” provides mechanism so that anyone can buy and sell data. For instance, self-driving cars need to upgrade their data constantly related to traffic congestion, changing electricity prices and weather forecasts. Streamr provides single interface for delivery and payment of data to people and machines. This data can be traded using cryptographic token called DATA coin which relies on Blockchain. In this way, car can get the real-time information it requires by paying for it and later can sell the data it generates so as to provide the updated data related to road conditions, locations, and traffic congestion and battery levels to other cars. That is how data stream economy will be born. [26]

3.6 Beacon technology:

Beacons are cheaper and smaller devices which can track the very precise location than GPS but within a range of 50 meters. These are typically used for indoor location technology but can be used for outside locations as well. Beacon communication basically is done through apps. Apple uses iBeacons and the facebook has offered the new app to the New York users which rely on beacons. These beacons help to improve the productivity and efficiency in the workplace so enterprises have started using beacons. [38]

3.6.1 History of connecting with people:

- **The wheel:**

  It was the first and foremost invention which enables people to relocate to far-off place thus helping people to move the goods and materials with the help of wheel. It came in 3500 BC.

- **Printing press:**

  By coming in 15th century, it transformed the education and communication areas and information was widely spread across regions and countries.

- **Radio:**

  Radio was invented in 1895 which enhanced the globalization and gave an idea for bringing mobile communication.

- **GPS:**
  GPS came in early 1970's which made the transportation much easier and convenient. This location based tracking help entrepreneurs to grow more in the market.

- **Beacons:**

  Beacons, the small devices which came in 2013, mixed the outside world with inside world or vice versa and enhanced the productivity of enterprises. Beacons are becoming the key enabler of IoT. These are Low energy Bluetooth transmitter or receiver which makes it efficient to work with smaller batteries but for longer period of time. [39]

  It is cheaper than Bluetooth and even consumes less power than a normal Bluetooth device. Now let us discuss some of the top companies which are manufacturing beacons:

  - **Estimote:**

This company has more than 10,000 SDK’s for making beacons which is already dominating the other beacon manufacturers.

- **Sensorberg:**

  This company manufactures tiny beacons with the range of 30 meters especially for marketing shops.

- **BlueSense:**

  This is a new entry in the beacons manufacturing competition which promises to meet the growing needs of community and these mini beacons can be used for inventory purposes.

- **RadBeacon:**

  The manufactured beacons of this company are stored in USB which can be put in use by plugging the USB with the laptop and beacons are available for service. [40]

Chapter - 4

Benefits of IoT and its effects on communication

A. Benefits:

There is no doubt that IoT will revolutionize each sector starting from agriculture, health, manufacturing, homes and transportation. Let us consider each sector one by one to get a better insight and review the benefits provided by IoT to it.

4.1 Healthcare:

IoT is constantly upgrading the tools and systems to take of the patients in a better way and in a reduced cost which the patients family can bear so as to decrease the number of deaths every year. This continuous monitoring of the patients through the deployed sensors helps the doctors to figure out which patient needs more attention and care. Now, let's list some of the advantages of healthcare system:

- **Decreased costs:**

  With the help of IoT, there will be certain deductions in the costs as there will be no hospital admissions and discharging fees. Doctor need not to have regular visits instead the embedded sensors at home will give the real-time update to doctor about the health of the patient.

- **Improved outcomes of treatment:**

  These connected solutions give the doctor or caretaker the real-time update about the health of a patient which assists them in making more informed decisions rather than vague decisions about the medications and treatment required.

- **Improved disease management:**

  As the caregivers are continuously monitoring the patient, when they found any changes in the health which may be symptoms of any deadly disease they abruptly starts the medication to have a control on disease before it gets out of control.

- **Reduced errors:**

This real-time monitoring and collection of data will reduce errors in patients health reporting and giving medications so help in avoiding wrong decisions which could have proved to be deadly for a patient.

- **Enhanced patient experience:**

  IoT will enhance the patient experience as he will be monitored continuously and whenever there will be need physician will come and do the required analysis which help in building trust of patients.

- **Enhancement management of drugs:**

  In healthcare industry it is difficult to manage drugs and tools. So these sensors embedded on the tools can help to track them on time and if they require any kind of maintenance it will be taken care beforehand. This will help in providing medical aid to the patient on an appropriate time. [42]

Wearable technology, smart pills and delivery robots have enhanced the quality of healthcare system.

4.2 Agriculture:

Adopting IoT will help to monitor and collect data for enhancing the productivity of crop and reducing the expenditure for its growth. IoT help in sensing the soil, air and temperature required for increasing the crop yield. Following are some of the benefits if we start relying on IoT:

- **Increased production:**

  Crop production will be increased by implementing IoT in farming as it will provide the proper list of requirements such as water, air and pesticides.

- **Water conservation:**

  Sensors deployed over there will identify how much moisture is required for a particular crop and will check the soil conditions and in this way only the desired amount of water will be provided so as to conserve water.

- **Real-time data and production insight:**

This real-time monitoring will help the farmers to take more precise and accurate decisions related to the crops growth. This visualization provides them a insight of how the production level goes, whether it is going as per planned or some changes are required to enhance it.

- **Lowered operation costs:**

  This automation in farming will reduce the operational costs as there will be less resource consumption, low chances of human error and overall cost required for farming.

- **Increased quality of production:**

  This will enhance the quality of product by providing a time to analyze how the growth continues and if there is any change required in the ongoing process.

- **Accurate farm and field evaluation:**

  Continuous monitoring the growth of a crop gives an idea about the next crop growth and what changes should be implemented to increase the productivity of future crop.

- **Improved livestock farming:**

  In livestock, wearable technology such as sensors and machines deployed in animals provides the health status and reproduction information directly to the farmers so that they can enact according to the requirement.

- **Reduced environmental footprint:**

  Implementing IoT in farming will affect the environment in a positive way such as resources will be utilized in a efficient manner. Water will be utilized as per requirement and same will be air, light and temperature required to maintain the soil fertile.

- **Remote monitoring:**

This will help the farmers to continuously monitor their farm even if they are far-off from the agricultural land. Thus, enabling farmers to take real-time decisions and that too quickly and apt from an internet connection.

- **Equipment monitoring:**

  Equipments are continuously monitored and tracked so that if they require any maintenance it can be done beforehand so as to fulfill the emergency needs. [43]

IoT will let the farmers to know about their farmlands better and providing real-time monitoring and weather conditions will help them to avoid crop damage. Earlier, farmers used to contract labor for spraying pesticides over a large farmland which was cost-consuming and time consuming both. Now the labor has been replaced by drones which not only help in spraying insecticides but also monitor the crop growth and health on timely basis.

4.3 Manufacturing:

According to Tata Consultancy services report, it is calculated that manufacturers who have started using IoT in their corporate have experienced 28.5% increased revenue than those who have not deployed it. Following are some of the key benefits of deploying IoT in manufacturing industry:

- **Greater energy efficiency:**
  In large firms, energy consumption bills are quite high and these bills don't provide the smaller details on bill instead bill tells the entire consumption and how much will be the entire amount needed to pay. So here comes a gap which needed to be filled through IoT. This real-time monitoring will provide insights as if how to turn off the device or machine if it is not in running stage, how to optimize the production schedules and other saving opportunities. It can even help to determine which machines are performing better and provide solutions for the underperforming ones.
- **Predictive maintenance:**
  Earlier maintenance schedules were based on historical data collected for a device but it's not always fundamentally true. Sometimes the device does not even require maintenance but its schedule is put into practice which causes money loss and time wastage. Here, IoT is fruitful by embedding sensors that will tell when and which device requires maintenance so as to avoid the productivity loss. Sensors provide the real-time evaluation of devices and if there is no need of replacement or repair of any particular device then those resources, money and time can be saved.

  For instance, IoT sensors are deployed to measure the temperature of a device and if it senses that there is any sudden change in temperature that is more than threshold or less, the staff will be automatically alerted to take care of the situation before it goes out of control. Some of the companies such as French rail company SNCF, is already using these IoT related services to detect the early warning signs of potential failure and resolve issues before they affect productivity.

- **Higher product quality:**

Keeping the product quality high plays a major role in maintaining the business at a forefront. By keeping the quality high, there are certain other benefits such as low wastage, high sales and customer satisfaction is achieved. Product quality cannot be achieved until and unless it is properly set, calibrated and maintained. In cases, it may happen that manufacturers don’t even know that equipment has any problem. As a result, quality may get worse and manufacturer only get to know when the situation has got out of control.

To illustrate this point more deeply, let’s say an auto manufacturing company is providing the painted metal products. Company is highly reputed for its deliverables to the customers but only a single wrong step has proven to be a worst for company’s sale and market value. As there was no technology embedded to take care of the temperature of paint stations, as the temperature got slightly change which affected the quality of paint. In the first look there was no change viewed in the metal products. Products seem to be perfectly fine and even passed the quality test. The effects came into lime-light almost after a year when customers start complaining about the issues. This has resulted in loss of trust, damage to the reputation and customer dissatisfaction. The situation would have been avoided if the real-time monitoring was put into practice with the help of IoT sensors. Whenever there was a sudden change figured out by the sensor, it would have alerted the staff and this situation would not have progressed to that level.

- **Reduced downtime:**

If the product is delivered accurately at an appropriate time it serves a profit maker to the company. If a machine stops working in the middle of making product, the outcome will be a damaged product which will raise the downtime expenses. To make this point more clear, let us understand it through a suitable example – suppose an oven breaks down while processing a bun in a firm which will result in not only the loss of ingredients and production time but will also enhance the downtime expenses for a firm. IoT comes as a safeguarding tool in such cases. The real-time monitoring of IoT sensors will analyze any such problem at the initial stage as if when the performance has began to deter and will alert staff of the upcoming problem and will reduce downtime expenses.

- **Faster and more informed decisions:**

The real-time monitoring will enhance the performance and production of a plant. Managers and staff will not be concerned about the maintenance of equipments or tools as they will be provided relevant information by those deployed IoT sensors. So there won't be any need to maintaining the historic data about the maintenance or replacement of equipments. Management will be less stressed about the performance deteriorating because of failed equipments and will be more concerned about increasing the production of firm. [44]

4.4 Transportation:

IoT will transform the every sector of industry and will reduce the cost in significant ways. Parking, airports, railways, buses and cars are areas of transport where connected devices can provide financial benefits and reliable services. Let us discuss the advantages of smart transport system:

- **Improved safety:**

The connected transport system will reduce the number of causalities as these autonomous vehicles will be properly programmed about the traffic areas; maintain speed at highway, urban and rural areas; will get the real-time updates from other connected devices through the sensors; avoid the dangerous routes and regularly check the maintenance of vehicle. It will enhance the customer and driver safety using video surveillance.

- **Higher efficiency:**

These IoT sensors improve the efficiency of vehicles by providing the real-time update about the maintenance of vehicles to the drivers and operational personnel so as to avoid any heavy breakdown of vehicles which would have cause heavy loss to the company which totally relies on transportation sector like the shipping companies, delivery vehicles and public transport. So to make this point more clear in terms of efficient management – if a truck which is taking the delivery of a store and in midway it stops immediately because of some problem in vehicle's engine. Now, the store has to manage with the products which are short and would have to request their customers who are in need of those short products and even the truck company has to do the double task like firstly they need to find the truck which would replace the broken truck and deliver the products to store or need to find the mechanic immediately to cover the losses. So in this situation, if the sensors would have been deployed then the problem would not have reached that level.

- **Enhanced customer experience:**

This wireless connectivity can make the life of customers easier and reliable. It provides the information related to bus schedules so that customers don't have to wait long time at the bus stop waiting for bus. Instead the Google maps provide the real-time updates which has attracted many customers and it has even launched a new feature asking the passengers to give the reviews about the congestion in the bus which they have taken.

Autonomous vehicles will help each other to find the empty parking spots which will save lot of energy in the form of gas and will save time as well which can further be utilized in some constructive work. These vehicles with the help of sensors will communicate to each other and will store the data if they find any parking spot free and then the same data will be sent to every vehicle so as to help the one who is looking for parking.

- **New revenue streams:**

It can become as a source of income by making the customers satisfied by providing them new facilities throughout their journey like playing their on-demand videos. [45]

4.5 Financial services:

IoT has transformed the way banks were working. Now it is easy and convenient to transform such a huge amount of data reliably. Now let's discuss how the IoT has benefitted the different financial services:

- **Insurance industry:**

These companies are collecting data through telematics systems which can be further used for different kinds of insurance such as health, vehicle and accidental. These telematics systems enable the companies to capture data more conveniently and evaluate their client's risks and increase their company's revenue. Now some of the companies have started offering user based insurance which works by tracking the driving habits of their client through the sensors deployed in their car which captures the real-time data and on the basis of which company offers discounts to the customers for their safety and betterment.

- **Banking industry:**

As we know that bank employees have to deal with so many transactions on daily basis and they have to keep a track so as to avoid any fraudulent transactions thereby keeping their customer's trust and faith in their bank. IoT helps in availing the entire customer's info available to him through different banking apps. Customer can do online transactions which enable them to save their time and transportation charges. Banks now completely rely on IoT technology like they install sensors in their customer's home who apply for home loan from them. These sensors let the bank know that this much amount of money is required for particular damage or a repair which benefit both the borrower and bank.

- **Credit card company:**

Credit card companies have started using low energy Bluetooth devices to send notification to their customer about the credit information by tracking their location. Customers can now track the amount of credit they have used and the remaining credit left which gives them more personalized experience. Company is focusing more on IoT so as to fulfill their customer needs.

- **Customer relationship management:**

Financial services are putting more effort to make their customer experience best and satisfied. This reliable connectivity can be achieved by managing their customers' data through the cloud based applications. Customer relationship management software can be used to organize the documents in the cloud with more security. This will enhance the business performance and customer satisfaction.

- **Maintain data privacy and security:**

As in today's world lot of data transfer takes place so there are quite reasonable chances when data may get interpreted. There are lots of scammers which can trace your personal financial account information. So as to avoid such circumstances IoT paved the way for security and privacy of customer data. To make the point more clear, let us emphasise on following example- as we know IoT is pacing at such a high speed that in next 3-4 years everything will be connected. Let's say we have connected refrigerator which senses the items which are running low and automatically orders the product from nearby grocery store. While making payment through IoT app customer is provided with credentials so as to avoid any fraudulent transactions which in the other way help to gain the customer satisfaction and trust. [46]

4.6 Education:

IoT will benefit the education sector in the following areas of interest. Let’s discuss the benefits in detail:

- **Increased efficiency:**

The use of smart technology in education helps the students to develop different kinds of skills such as critical thinking, proficient in different languages and building confidence level to deal with difficult situations. It is found by study of University of California that use of smart gadgets has helped the medical students to score 23% more in exams. There are different apps available to provide real-time experience to students. One such app is Anatomy app which helps in visualizing the inner human body and other one is Revision app which helps the students to test their knowledge before they appear for real exams.

- **Student-centered approach:**

Wearable technology can change the overall development of students such as check their heart rate, calorie consumption, brain signals so as to check if they are concentrated towards study or there are some thoughts which are distracting them from their path. These technologies help to improve the student’s nutritional diet and eliminate the stress causing agents by sending an alert notification to parents as well as teachers to take care of the pupil.

- **Improved school and campus security:**

As we know that after 2013 there has been many cases of school shooting which has mercilessly killed many students. Such incidents can only be avoided through enhanced security systems like badge recognition software which will allow only nice people to enter the premises or sensors should be deployed at the gate of school which detects the heavy metals and alerts the police and school management through the push notification. [47]

B. Effects on Communication:

Wireless communication came into existence in the early 21st century which makes the whole world connected to each other, making the people around the world to send and receive messages to each other. Invention of smart phones is considered as world is carried out in pocket. After that social networking sites came into existence which enabled the individuals to get insight of what is going on around the world and to the people they are connected on sites. There is more flow of knowledge and ideas as compared to earlier. Apps such as LinkedIn have made the business networking more reliable and convenient. With the advancement of technology now things have started communicating too which is called as Internet of things. It is expected that there will be more communication with machine and human rather than human to human which means machines will replace humans. Internet of things will make humans more independent like if you have to buy a grocery for a family then you are not concerned about grocery and neither is the family, machines will do it for you. So the machines will cut that part of interaction among family. Personal interactions will be reduced to a very minute level. People will become more machine oriented and will have less time to communicate among each other to share problems and feelings which will rise the depression patients because of isolation. The effects may be seen on business as well as more of the communication will be through internet which will enhance the lack of motivation among employees as in team meetings there is always a chance of more communication rather than point to point communication.

Chapter – 5

IoT requirements:

As we already know that system is made up of three components: Device, Gateway and Cloud.

Device:

A device consists of hardware and software components and can interact with the world through internet and by connecting with the other networks. Each device consumes different type of information and this information can be best handled by the backend systems. Let’s discuss the types of information found in IoT scenarios:

- **Device metadata:**

  Metadata contains info about the device and metadata components are almost same for each device as they are hardly changed. Examples of metadata field are identifiers, which class model, revision number, when was it manufactured and the serial number of hardware being used.

- **State information:**

  State information help to determine what is the current status of device and this information can be read/ write.

- **Telemetry:**

  Data collected by the device is called telemetry and this data is eyes and ears that are provided by the devices to the applications. This data is collected through sensors and every source of telemetry turns to be channel for the telemetry.

- **Commands:**

  Commands are the actions performed by device on the collected data. Commands usually don’t represent the state data and they have temporal relevance that is why they include time-to-live value or other expiration values in their traits. Some of the examples of commands are self cleaning cycle and increase the rate by 10 or 20 percent.

When we think about IoT, what we understand is that everything needs to be connected sensors, actuators and network connection which will enable the devices to be connected and the regular flow of data.

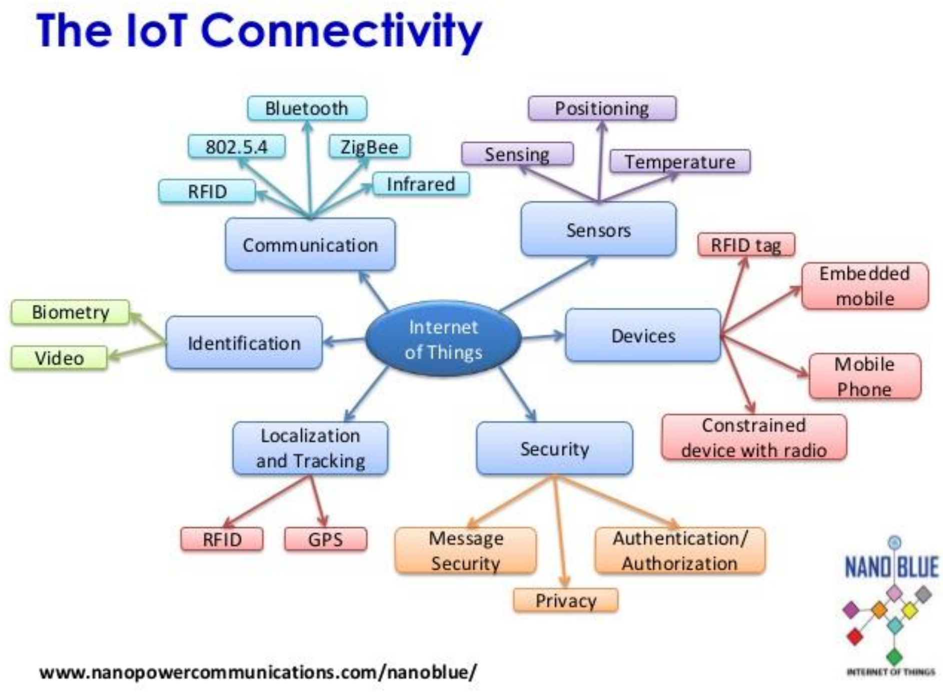


Figure 9 – IoT Connectivity taken from https://www.pinterest.ca/pin/633178028831909036/

5.1 Sensors -

Sensors are often called as key ingredients for devices to be connected. They are used to do the real-time monitoring and storing the data to take the action according to the requirement. They are used to convert the physical phenomenon to electrical impulse and also referred as transducers. There are different kinds of sensors used for different applications such as –

- **Temperature sensors:**

  These types of sensors are required to measure the temperature of a device or a thing so as to ensure that it remains in the equivalent to the pre-set value. These can be used for measuring the temperature of soil, water, inside and outside temperature of room or a plant.

- **Proximity sensors:**

  These sensors are mostly used to detect the motion and are often used by retailers to send deals or coupons of product to their customers through smart phone. These can be helpful in the crowded places where it is difficult to find a parking lot.

- **Pressure sensors:**

  Pressure sensors are used to gauge the pressure in pipelines. These can be helpful in agricultural sector where most of the water leakage occurs or can be used in the buildings to notify the management if any such condition prevails. They can also be used in smart vehicles to gauge the tire pressure and in aircrafts to measure the force and altitude in the atmosphere.

- **Water quality sensors:**
  These are used to monitor the quality of water. These can be useful in rain water harvesting techniques as to sense if filters are working effectively.

- **Chemical/ smoke or gas sensors:**

  These can be used to detect the level of air pollution in the city, smoke in the building or room to alert the fire controllers and can also be used to alert the management if there is any chemical spill on the ground to avoid hazardous accidents.

- **Level sensors:**

  These sensors are used to detect the level of liquid in tanks such as gas tanks, diesel tanks and water level in the natural reservoirs such as dams and lakes.

- **IR sensors:**

  These are used by doctors to monitor the blood flow in patients and heat leakage in buildings. These can also be used to detect the infrared radiations. [48]

We have learned that sensors collect the information. Now we need to discuss what is done with that collected data. Collected data is processed and analyzed further with the help of actuators. What is the purpose and definition of actuator is, let us discussed in brief:

5.2 Actuators-

These kind of transducers work opposite to sensors as it converts the electrical signal back into physical action. These are also used whenever there is a requirement to turn on\ off device by applying certain amount of force. Actuators can create all types of motion such as linear, oscillatory or rotational it's just the matter how they are designed and asked to operate. Few examples of actuators are Lully, sentry, hue and nest. Lully is used to enhance sleep and to sense the quality of sleep, sentry serves as a home security guard and alerts the residents about the quality of air and if there is any kind of security threat. Hue is a bulb or lightning and is a product of Philips Company which is used to control the lightning at office or home with the help of Hue app. It can also be used to change the color of light according to your requirement. Nest introduces different kinds of actuators such smoke detectors and security cameras.

Sensors and actuators both serve as backbone of Internet of Things as without them there will be no real-time monitoring of things and people. Smart phones also consist of both the transducers-sensors and actuators. Camera and microphone are sensors whereas speaker and screen are actuators. As we have already discussed about sensors and actuators now let us discuss about the wireless connectivity required to take these collected and analyzed data to next step.

5.3 Computational requirements of IoT:

Hardware processing units such as microcontrollers, microprocessors, System on chips and field programmable gate arrays and software applications are included in computational requirements. Hardware platforms such as Arduino Uno and Raspberry Pi are used.

- **Device hardware:**

  While choosing hardware for devices there are certain factors which needed to be kept in mind before putting them into practice:

  - **Cost:** Before selecting hardware it should be noted that company or firm can support the cost and customers can also support that price during sales.

  - **I/O roles:** Device can primarily act as sensor or actuator or can be a combination of both the roles.

  - **Power budget:** It should be noted down that device can connect to electricity or it is a battery oriented or solar power device.

- **Networking environment:** consider whether the device can connect to the internet through wired or wireless channels. If it is wireless then up to which range transmission power is achieved and how much energy costs are added. If it is wired then is it possible that it can wire directly to the internet as TCP/IP routable.

Device platforms:

There are multiple options available for selecting hardware platforms for IoT applications. Some of the examples of platforms are single-board-computers and microcontrollers. Common instances of single-board-computers are Beaglebone and raspberry Pi and of microcontroller platforms are Arduino series and Adafruit feather. These platforms help you to connect to multiple numbers of sensors and actuators through hardware interfaces.

Hardware interfaces:

Most of the hardware interfaces are serial interfaces. These interfaces control the flow and timing of binary information using multiple wires along with the use of primary data wire and method of communication between peripheral and central processor is defined by hardware interfaces. Following are some of the interfaces which are commonly being used:

- **USB:**
  Universal Serial Bus is commonly used for plug and play array devices.

- **GPIO:**

  GPIO is General Purpose Input Output pins. These pins are connected directly to the processor. These pins can be designed in such a way to carry both the digital and analog signals and digital pins only have High and Low state. Digital GPIO supports Pulse Width Modulation which switches quickly between on and off. PMW can be used to modify the brightness of LED. The wider the width of on pulse, brighter is the glow of LED.
  Analog pins might have access to analog-to-digital conversion (ADC) circuit. It continuously samples analog waveform such as analog audio signal. Analog pin can have any value not only high and low like digital pin. Let's elaborate it further like an 8-bit ADC has a range of 0 to 255 while the 10-bit ADC has a range of 0 to 1024 for digital values.

- **I2C:**

  Inter-Integrated Serial Bus enables multiple modules to be assigned a discrete address on the bus.

- **SPI:**

  Serial Peripheral Interface devices follow the master-slave architecture. There is one master and the mode of communication is full-duplex. Following are the SPI logic signals:
  SCLK: This is the output from the master.
  MOSI: Master Output Slave Input and this is also output from the master.
  MISO: Master Input Slave Output and this is output from the slave.
  SS: Slave Select is an active-low signal and this is output from the master.

- **UART:**
  UART is Universal Asynchronous Receiver/Transmitter. It is used to translate the data between serial and parallel forms.

- **Hardware abstraction in software:**

  While building the IoT solutions, most of the sensors and actuators that we come across are not supported by the OS for abstraction so abstraction of such devices can be done with the libraries that abstract across platforms. These Libraries such as Johnny – Five, JavaScript framework, MRAA and Firmata represents peripherals in the form of lightweight drivers on the top of hardware interfaces.

- **Computing environment:**

  Capabilities of processor totally rely on hardware constraints of power and cost. Some computing environments are microcontroller device based systems which are more constrained and directly run your application on processor while the others are system on a chip (SOC) based which support the Linux operating system. These computing environments serve as a bridge connecting the application code and the hardware. Computing environment executes the software which might be completely loaded during the boot up from read-only memory (ROM). [68]

- **Microcontroller development boards:**

Microcontroller is a SOC based that provides data storage and processing capabilities. Microcontroller contains processor core and memory like RAM and Erasable Programmable Read-Only Memory (EPROM) for storing the custom programs that run on the microcontroller. Sensors and Actuators connect to the microcontroller through digital or analog GPIO pins or hardware bus. Commonly used interfaces such as SPI and I2C are used for intra-device communication.
Arduino is an open-source device platform which is used for creating compatible development boards and tooling. Standard approach to develop and run software on Arduino is to use C or C++ and the arduino IDE. Arduino boards are too compatible that they can be used for third-party shields such as adding an Ethernet port or Bluetooth to arduino Uno.

- **Single Board computers:**

  Single board computers are next step to the microcontrollers as they allow attaching peripheral devices such as Keyboards, Mice and Screens as well as offering adequate memory and processing power. SBC's can be expanded to hats on Raspberry Pi and capes on BeagleBone Black and some of the additional modules such as motor controllers or analog-to-digital converters. [69]

Cloud platform:

Cloud platform is the important computational part of processing in IoT. Cloud is a platform where data is sent from the devices. Cloud solutions help to complete the complex processes to be completed and transmit the collected data to a service which is cloud-based. This service is used to mix the data of other cloud-based services to the information in IoT device which will help the end user.

5.4 Gateway:

IoT gateway is a hardware component that acts as a collaboration point to connect these sensors and actuators to each other or to any external network available. It deals with reliability and latency issues among the incompatible devices. Key features a good IoT gateway must have:

- Mostly operates efficiently on Linux environment.
- It must have support for programming languages such as Java, Python or Node.js.
- It should support different communication protocols such as Bluetooth, Wi-Fi, Zigbee and Z-Wave.
- It should be able to connect to different types of networks such as Ethernet, Cellular, Wi-Fi and satellite and should ensure that communication done over such networks is reliable, secure and confidential.

- It should support the network latency, offline mode and real-time analyzing at the edge and should have the data forwarding ability.
- It should have the remote access to start\stop and configure the other gateways and applications. [49]

Connectivity comes in two types – wireless and wired. Let us in detail wireless connectivity first:

5.5 Wireless connectivity:

Connectivity is required to make the connection of real-time monitoring and analyzing of sensors and actuators through a network which can be either wired or wireless. Wired connections are not preferred for IoT applications although they provide more security and privacy than wireless. Wired connections are more expensive so that's why IoT opts for wireless connectivity. With the advent of technology there is more focus on eliminating limitations such as making the connections are more reliable and secure channels. Now let us discuss the popular wireless communications available for IoT devices:

5.5.1 Wi-Fi:

Wi-Fi is the most commonly used wireless connection to make a link between the gateway and the router. It is basically used in the links which require high speed and medium range such as video monitoring at home or office for security purposes. Most recent version of Wi-Fi which is 802.11ac only operates in 5 GHz ISM band and with a high speed up to 1.3 Gb /s while the rest of versions operate in the unlicensed band of 2.4 GHz and in a limited range of 100 meters. All the shortcomings of the Wi-Fi will be addressed by the upcoming versions – Wi-Fi HaLow (802.11ah) and HEW (802.11ax).

- **802.11ah:**

  This version was introduced to rectify the problem of limited range and power as it uses the 900 MHz license band which provides an extended range along with low power consumption capabilities. It provides a range of up to a kilometer more the earlier versions which were only up to 100 meters. Implementation is taking a little while because it requires a specialized access points and hardware.

- **802.11ax:**
  IoT devices demand more efficiency so as to meet such requirements there was a need of this new version of Wi-Fi. It maintains the learned targeted wake time and station grouping feature from the Wi-Fi HaLow and make the clients to be more power savers and avoid conflicts. It can allow 18 clients to send data simultaneously on a 40 MHz channel as it uses uplink multi-user MIMO capabilities. The adoption of this version totally relies on the clients as how much they are willing to spend on access points. [50]

One more Wi-Fi standard is on the way which is designed to use the white spaces in TV and the unused TV channels as these channels are suitable for providing long range and no light-of-sight transmissions. Base station checks if the channels are available.

5.5.2 Bluetooth:

Bluetooth is widely used for short-range communication. It operates in the unlicensed band and is following the principle of Frequency-Hopping Spread Spectrum (FHSS). Gaussian Frequency Shift Keying (GFSK) is the modulation method preferred and offers a 1-Mb/s. New version of Bluetooth is called as version 4.1 or Bluetooth Low Energy (BLE) or BT smart.

- **Bluetooth Low Energy:**
  BLE is a low power consumption device which comes as a significant advantage for IoT based applications. Nokia introduced BLE in 2006. Most popular applications of BLE are smart watches, car key fobs and heart rate monitoring. Upcoming applications in this domain are from smart home, smart city and internet of things. The first product to come up with BLE technology was iPhone 4s. [51]

5.5.3 Zigbee:

Zigbee comes as a ray of hope for controlling and sensing the applications at isolated locations. It is built on IEEE standard 802.15.4. This standard is also used to deal with low-rate wireless personal area networks. It is used to define the specifications required for security layer so as to make the exchange between two different products from different manufactures more compatible. It uses low power frequency which enables the devices to have long battery life. Zigbee can communicate only over a small range of 76 meters lower than Wi-Fi.

There are three kinds of specifications zigbee offer:

- **Zigbee Pro:**

  It provides the features which are required by IoT devices such as low cost, networks for reliable D2D communication. It also offers a feature which supports self-powered devices through the green power. It was released in 2007.
- **Zigbee RF4CE:**

  It is designed specifically for simple applications such as device-to-device control and does not require full mesh networking functionalities. It was released in 2009.

- **Zigbee IP:**

  It is specifically designed for low-powered and low-costs devices that fully rely on IPv6 full mesh networking technologies.

Zigbee consist of different topologies- star, mesh and cluster tree.

Star network: It is used where simple designs are required. In this different nodes communicate with central node of star.

Mesh network: It is a network (Local Area Network, Wireless LAN or Virtual LAN) that uses one of the mesh topology may be a full mesh or partial mesh topology. This network provides more reliability. It consists of nodes and the nodes within the range are able to communicate to form mesh. There are different routes available in a mesh network and messages are transmitted with the help of relays. This kind of network is more robust and if there is no chance of collisions as multiple paths are available to reach destination.

Cluster tree network: It is also known as hybrid network as it is a combination of mesh and star network. [52]

Zigbee Alliance:

Zigbee alliance assists the product manufacturers to introduce the energy efficient wireless control into their products more quickly and cost-effectively. Companies which come under this alliance are NXP, Philips, HUAWEI, Silicon labs, Smart things and Schneider electric. There are three kinds of membership available under this alliance:

Adopter:

It offers access to all the interoperability events and all the documents and activities.

Participant:

It has all the voting rights and has access to all the documents and specifications while developing.

Promoter:

It offers automatic voting rights to all work groups and after final approval offers a seat on alliance's board of directors. [53]

Zigbee announced a universal language called dotdot for Internet of Things.

5.5.4 Thread:

Thread was specifically used for home appliances and it is a reliable, cost-effective and low power open standard communication protocol. It came into existence in 2014. Three main types of devices in thread are:

- **Border routers:**

Border routers are used to provide connectivity from 802.15.4 network to the adjacent networks on different layers. If one border router fails, then another router takes the responsibility of border router hence makes the network to be more robust.

- **Routers:**

  These routers are usually degraded to make them REEDs (Router-Eligible End Devices). These devices are neither used in routing nor in data transfer but are taken as end point that can be called when needed.

- **Sleepy End Devices:**

  These devices are known as host devices or sleepy child or sleepy node. When sleepy devices wake up they transmit data and the rest of time they sleep. Parent is that router which is directly paired to the sleepy device. Communication is only possible through parent device. The cycle of transmission goes as – firstly wake and perform the initializations required and then go to receive mode to check if path is clear to transmit and then move back to transmit mode to transmit data. After the data has been transmitted, wait for acknowledgment and on receiving acknowledgment go back to sleep mode.

  Threads mostly use ad-hoc mode of networking. Threads support full mesh topology. It operates in the unlicensed band spectrum. Thread appears to be a future solution for IP over low-rate wireless personal area networks as compared to zigbee IP. [54]

5.5.5 Wi-Max:

It came into existence in early 2000's for short range wireless communication and the rate at which data is transmitted is 30-40 megabits per second. It is also known by the name of 802.16 in IEEE standards. WiMax's original target was the rural areas where there was not good internet connection available not the cable TV and DSL. This technology was once used by lot of mobile carriers in US specifically sprint which later on shifted to the new LTE networks which were more faster as compared to WiMax. WiMax usually produces better signal when near window or outside. Link labs are developing new technology known as Symphony link which will eliminate all the problems. [55]

5.5.6 LPWAN:

LPWAN is Low Power Wide Area Networks. As the name suggests it consumes low power and work efficiently in a wide area of networks. Most of the LPWAN's follow a star topology. LPWAN's come in both types – Cellular and Wireless. Cellular networks come under licensed spectrum while the wireless networks use unlicensed spectrum. We are going to discuss in detail about the wireless LPWAN's upcoming technologies which are about to be deployed or under development: [58][59]

- **Sigfox:**

  Sigfox is a proprietary which was founded in 2009 by French based company. It uses low modulation rate to achieve longer range. It is used in applications such as parking sensors, water meters or smart garbage cans where a system needs to send small but infrequent bursts of data. Data sending back is very limited and signals could interfere which can become an issue. There is only one operator per country and messages can be transmitted over a distance of 30-55 km in rural areas, 3-10 km in urban area and 1,000 km in line-of-sight of applications.

- **LORA:**

  LORA is an open standard and has about member companies throughout several countries and the founding members are IBM, Microchip, Cisco, Semtech, KPN and many more. Functionality is similar to Sigfox as it can also only do uplink transmissions. Unlike Sigfox where signals might get interfere because of narrowband transmission; there is no chance of interference as the information is spread on different frequency channels and data rates using coded messages. Although it is open source but transceiver chip which is required to implement LORA is only available from the company Semtech which has brought LORA into existence. It operates on unlicensed spectrum.

  - ➢ **Symphony Labs:**

    Link labs are a member of LORA alliance. Link labs were found in 2013 by the members of laboratory who worked in John's Hopkins University in Maryland. These labs added some important features such as receipt of message received or transmitted and repeater capability and variable range.

- **Ingenu:**

  It belongs to the unlicensed spectrum and is also called as on-ramp wireless. Ingenu also has a proprietary model. Ingenu designed the new technology known as RPMA (Random Phase Multiple Access). Now let us discuss about RPMA in detail:

  - ➢ **RPMA:**

    This company was founded in 2008 in California by the former employees of Qualcomm Company. RPMA has a significant advantage over LORA and Sigfox as both can do only uplink transmissions but RPMA supports both uplink and downlink transmissions. System is more robust and has a better coverage as compared to Sigfox and LORA.

- **Weightless (SIG):**

  It was founded in 2008 and has 5 promoter group members. Weightless operates on unlicensed spectrum. Weightless comes in three different versions:

  - **Weightless-N:**

    Communicate in single direction and operational cost is low. It is founded from NWave’s technology. Functionality is almost alike Sigfox but possess better implementation at MAC layer. It uses advanced modulation techniques to allow better connectivity with other radio technologies without adding to the noise factor. It is best for sensing applications such as monitoring level of tank, reading temperature and smart metering.

  - **Weightless-P:**

    Can communicate in both directions but for shorter range and has low operational cost. It can operate in both the spectrums- licensed and unlicensed. It is founded from M2COMM’s Platanus technology. It uses the combination of frequency division multiple access and time division multiple access modulation techniques in 12.5 KHz band which is greater than Sigfox but is lower than LoRa. Data rate is adaptive and sensitivity rate is quite high. It supports PSK and GMSK modulation as well. It supports both uplink and downlink transmissions and development kits for weightless-P have almost merged in the market.

  - **Weightless-W:**

    It operates mainly in the local spectrum of licensed TV band. Communication is bidirectional and operates in a wide range of 5 Km but operational cost is little expensive. It has a shorter battery-life. [56]

Now, let’s discuss briefly the wired LPWAN’s technologies:

- **Cellular LPWAN:**

  Cellular technologies basically operate on licensed band spectrum. Cellular technologies constitute of GSM, WCDMA, LTE and 5G. Narrowband IoT (NB-IoT) is considered as the most attractive solution for the LPWA technologies. Cellular connectivity has already reached the 95% population. These wired networks are governed by 3GPP standards. Cellular networks can address the issues from Massive to critical IoT use cases. QoS mechanisms are specifically taken care by cellular networks. Although, it is assumed that cellular connectivity is not efficient for IoT but the recent innovations in cellular technologies such as NB-IoT and LTE-M are going to make remarkable difference in the thinking of IoT players. Now let us dig deeper in the upcoming technologies. LTE-M further consists of Cat1, Cat0 and Cat M which supports wide range of applications. NB-IoT covers all IoT applications with ultra low ends and EC-GSM covers IoT applications involving GSM markets.

- **EC-GSM:**

  Today, most of the mobile applications use EDGE/GPRS for reliable connectivity. It operates on 900 MHz spectrum. It does not require more carriers as the new software is sufficient to enable 50,000 devices on a single transceiver. Earlier, eDRX was a part of EC-GSM but now it is different entity. It was developed to improve the battery life and power efficiency. Idle mode behavior of eDRX is now shifted to get engaged in some other tasks such as tuning to the network and listening to the downlink pages and traffic over there.

- **LTE-M:**

  Mobile users are experiencing remarkable changes in the performance because of introduction of new features- MIMO, Lean carrier and Carrier Aggregation. LTE-M can be significant as it has power saving mode and eDRX can extend the battery life of these IoT based applications. It is also known as CAT-M1 as it offers highest bandwidth among LPWAN technologies. It has ability to support roaming and voice on 4G spectrum.

- **NB-IoT:**

  It is also known as CAT-NB1 and operates on existing LTE and GSM infrastructure. It offers uplink and downlink transmissions of about 200KBps by using only 200 KHz of frequency. It can support 200,000 subscribers with the same carrier. It has ability to use both 2G and 4G spectrums. [57]

While using LPWA technologies for IoT connectivity there are three principles that needed to be taken into consideration for better security:

- Design should be secure:

Technology to be built should be secure by design from the beginning; it should not be afterthought when the technology has been designed.

- Simple:
  Security should be clear and transparent so that it should be visible how pieces come together for IoT protection.

- It should follow the standards:
  Standards should be followed otherwise they are compliance to pay fine up to million dollars a day. This makes nuclear power plants, oil and energy providers and smart grids to follow the rules and regulations stated by federal government.

LPWA wireless providers should offer these six guarantees to ensure secure connectivity:

- Message confidentiality:
  Messaging should be confidential which can be achieved using encryption techniques. These scrambled messages can only be unscrambled through using right key or password.

- Message integrity and replay protection:
  Message should be kept integrated as if even after encryption someone can spy on your passwords and use them later for same tasks which could create havoc.

- Mutual authentication:
  Mutual authentication enables the devices and individuals to know who else is in data exchange. It forbids the stranger to create an obstacle for the team.

- Device anonymity:
  Every device has unique identity that keeps them distinguishable from other devices so identity should not be disclosed for security purposes.

- Secure Multicasts:
  Secure multicasts use mutual authentication and guarantees that even there is lot of transmission going on between devices but all are protected.

- Authentic firmware upgrades:
  Proper firmware should be installed and should be upgraded on time to address any kind of security vulnerability. This will further enhance performance and efficiency of devices and would urge the customers to invest more in IoT. [64]

5.5.7 RFID:

RFID is the simplest communication method as compared to others and it is used in various day to day applications such as consumer products available throughout the world, hospital staffs to track their patients, tolling services to track the vehicles for tolling purposes and by farmers to track their pets. RFID tags can be read, write, transformed, locked and updated as compared to the traditional tags. RFID consists of readers and tags. Generally, tags are of two types:

- **Active tags:**

  These tags have stronger transmission signals and a wide range as they have their own power source. These tags can transmit periodically without the need of reader.

- **Passive tags:**

  These tags don't have any power source so they need reader to get activated. Bus pass and metro pass are examples of passive readers. These tags rely on the radioactive energy transmitted by reader.

Now let's discuss about reader:

- **Reader:**

Readers resemble RFID tags as both have same physical components such as antenna to receive and transmit signals. They either comes with a equipped battery or are required to plugged-in into wall wallet so as it requires the strong RF signals for tag activation purposes. The reader can manage the information by connecting it to reader controller and reader may also do writing and updating of tag, it all depends on the application. RFID usually have three tags- one of them is antenna which has been already discussed, the other two are Integrated Circuit and power source. IC is used for storing, processing and modulating/demodulating the signals. Power is required if the tag is active one.

5.5.8 Near-Field Communication (NFC):

NFC is efficient for short range communications as it operates in 13.6MHz band. Contact-less payment such as Apple Pay and Google Wallet are only possible because of NFC's. Almost 9 out of 10 smart phones come up with NFC's capabilities as smart phones can do data sharing by tapping each other. It is used to open the doors of cars such as BMW which come up with NFC technology. NFC comes up with two kinds of devices:

- **Initiator:**
  Passive targets are powered through its generated RF field. It initiates the communication.

- **Target:**
  This device receives all the communication from initiator and it can act be either active or passive. [60]

5.5.9 Wireless HART:

It operates in the unlicensed band spectrum and is highly suitable for electromagnetic interference. It can act as a wired protocol as well in case of automation space where it uses a two-way communication between a host and smart field instruments. It permits full wireless connectivity for real-time communications and is based on 802.15.4 IEEE standard. It offers both star and mesh topologies and offers low frequency information updates. Mesh topologies consist of motes and network managers. This technology is based on dust networks. Every device under this technology works as a source and repeater. [61]

The next requirement for IoT devices to work efficiently is security. Devices should be more secure and there should be less chance of interruption while these devices communicate such as hacking.

5.6 Security:

Considering the IoT ecosystem, security is considered as one of the main requirement of IoT connectivity. It is estimated that security market will grow from $7.9 billion to $37 billion by the end of 2021. Gemalto is considered as the head of security in IoT and has even coined the new term Internet of Trusted Things.

Head of M2M Segment Marketing at Gemalto has written in his company blog that infrastructure used in making of smart cities should be secure and diligent. He further elaborated by giving an instance of functioning of street lighting system. He mentioned that if one part of the system is weak, it will lead to security compromise for the whole system and same is for the car parking, traffic and waste management system. An experiment was conducted at MWC to find the vulnerable IoT devices in Spain and Barcelona. It was found that there were 5 million vulnerable smart devices which include 150,000 webcams which can be easily hacked and around 79,000 smart kettles and coffee machines. [63]

Security is the key ingredient of IoT devices to work efficiently and securely. There are certain factors/fundamentals which should be kept in mind while the making of these devices:

- **Ensure continuity and availability:**

There should be no hurdles and interruptions which could have halted the functionality of these devices. There should be continuity and availability for the smooth functioning of these IoT devices. It should also focus on the architectural design model such as centralized and decentralized (these topics to be discussed in upcoming chapters). Let's consider the example of smart grid which is used for provisioning power supply for the household needs but this supply can be interrupted if the smart meter is programmed by the attacker for misuse.

- **Design considerations:**

  All the important parameters such as security, privacy and data protection should be taken care at the design stage because once the design is made it becomes difficult to add these functionalities. As most of the IoT devices does not have high computing power so security must be considered before designing and implementing such devices.

- **Context-aware and situational risks:**

  As the privacy policies are becoming contextual and complex, it is difficult to assess the risks associated with the design of these IoT devices. Let's consider the example of implementing smart energy management such as smart homes and grids applications which have difficulty to consider data minimization and informed consent while considering the privacy and security parameters because of open environment.

- **Traceability:**

  As IoT devices generate large sums of data so managing such data raises concerns for authentication of objects. This authentication will increase the security of IoT devices.

- **Repurposing of data:**

  As we have discussed earlier that large sums of data is generated and this data could be used for other unlawful practices rather than their specified purposes. These malpractices can only be avoided if intelligence agencies are given the access to data.

- **Violation of individual privacy and data protection:**

  There have been many cases of electronic theft. One such case is misuse of contactless credit cards in which name and card number of individual can be read without any identification required which raised the concerns for privacy as this revealed information can be misused by attackers to purchase goods with the identity and bank account information of that card holder.

- **User locked-in:**

  Cloud computing and social networking applications are prevailing in such big numbers that it is difficult for consumer to migrate from one IoT service provider to other because they are locked-in to one provider. This dependency of consumers on the service provider needed to be taken care so as to escape from the security and privacy related issues.

- **Health related implications:**

  As with the advancement of technology in IoT sector, more and more industries are relying on remote monitoring and sensing so is in case of medical. There are chances that identification and information collected from remote monitoring could be interchanged which could lead to loss of life. Information collected from IoT devices could even reveal that person is suffering from certain disease which could lead to physical attacks on that person.

- **Difficult decision making:**

  IoT enables the devices to take decisions on the basis of information they have collected which is quite opposite to human decision making as the devices could not sense the emotions properly while making decisions which is quite different from human decision making process. This could even make some individuals feel the loss of control on their own lives as the decisions taken by the objects might not be as transparent. [65]

Proper security mechanisms should be followed while there is communication between devices and communication between device and human being. There should not be a loss of data due to noise or channel failure and device itself fail. Data should be protected from the attackers or hackers who can misuse this data for filling their own coffers. Security requirements of IoT devices include authenticity, confidentiality, integrity, privacy, availability and regulations to be taken care before handling such sensitive IoT data.

Generally, security has logical and physical issues. Logical issues mainly include malware functioning problems. Deploying IoT in devices raises many issues such as adopting light weight cryptographic algorithms; data exchanged between nodes should be minimized. Security issues in IoT can vary from technological to philosophical ones such as privacy and trust. Devices such as smart phones use number of applications such as WhatsApp, LinkedIn, Phone calls; Instagram uses different methods to exchange data through audio or visual modes which leads to security threats to the data exchanged between devices. Let’s discuss in detail about the different kinds of security required for efficient working of these connected devices:

5.6.1 Physical security:

Physical security plays a significant role in the connectedness of these smart devices. Physical security along with hardware components security also includes backup and supporting services, locations of wired being used in the devices. While installing a network at home or office premises or connecting it to the wide area network or internet, there is a need to develop certain measurements which people should follow as we can see that many times outages occur mainly due to human negligence or awareness. Network devices can be easily disturbed by humans. Sometimes such disturbances occur out of curiosity to use the updated device without any knowledge such as removing the cable connected to I/O port of device or moving the switch to different port can lead to violation of device in terms of physical security. Violating with the features of smart temperature controllers, connected cars and security cameras can lead to large loss of money. Hence, physical security should be taken into consideration while developing IoT devices.

5.6.2 Logical security:

Logical security uses certain technologies to enable the individuals to access the private data on the basis of their authenticity. It defines which individuals are allowed to use particular technology and which are not. Logical security comes in different forms which are defined in detail as follow:

- **Authentication:**

  Authenticity of device or individual is necessary to avoid the chaos. If proper authentication is followed, it tells whether the person or device is allowed to access data or not. In the most developed countries such as Canada and America proper health card number is provided to the people residing in those countries so that data of patients does not collaborate with each other and making difficult for doctors to take decisions on their patient’s health. Medical data of the patients accessed by the different users such as nurses, doctors, medical researchers and insurers should be handled with the proper authentication key. Any alteration in the data by criminal mind can lead to loss of life. There should be proper CCTV installation or physical guards to take care of the sensitive data. This authentication can be achieved by different means such as MAC address, QR codes, RFID and IPv4 OR IPv6.

- **Medium Access Control (MAC):**

  One of the finest features in authentication is to have a unique identifier such as Medium Access Control. It is a 6 byte number which is assigned by the manufacturer to its device to make it unique from other devices. Access points have separate table which tells them which MAC addresses are allowed to fetch certain information from which devices and which not. IEEE 802.15.4 offers upper layers to achieve good security facilities. It has been observed that some companies have started taking advantage of real-time monitoring or authentication such as if there is water in the basement, alarm will trigger automatically to make management aware of water loss and controlling sensitive systems such as lights, thermostats and appliances remotely.

- **Radio – Frequency Identification (RFID):**

  RFID plays a significant role in augmenting conventional positioning systems along with automated inspection or identification of products. Tags attached to the objects could leak the sensitive information which could later on lead to losses. These tags can locate the user's private locations. Overall it can be said that cryptographic mechanisms should be followed to ensure the secured IoT devices.

- **Quick Response (QR) Code:**

  QR codes are two-dimensional codes in which objects, things or events can be distinguished from the real-world. These are one of the latest authentication techniques in which black square dots are placed on white grid which allows the protocols to protect data stored in codes by encryption technique. This enables the receiver to verify that message did not collide with the previous one. These codes were initially used by Japan and china and later on by rest of the world.

- **IPv4/IPv6:**

  It is said that IPv6 is more secure than IPv4 but that it also not true as IPv6 uses host-to-host communications which provide confidentiality and integrity between the hosts but could not address the vulnerable attacks and most of the Denial-of-Service attacks. These attacks make the system to stop providing services to the other devices of network for some time.

5.6.3 Security Tools and Software:

There are certain kinds of software which are available for securing the devices as well. There is lot of traffic flow on the internet which has lead to increase in demands of network security professionals and with the upcoming IoT devices there will be huge amount of data flow because of the connected devices. These securing software check the file if it is acceptable or has some viruses before being opened. Security plays an important role in each stage of designing smart device such as from initial design to operations and maintenance environment. Security professionals should ensure that the critical network connection has sufficient bandwidth and redundancy to prevent DoS attacks. In addition to the bandwidth and redundancy there should be installation of detection systems to foresee the upcoming attacks. Smart home security system constitute of different kinds of codes, detectors and cameras to provide security. Detectors trigger an alert to let know the artificial intelligence that there is something to be evaluated and the facial recognition system help to recognize if the visitor is good person or the intruder. Malfunctioning software's are of two forms:

- **Mobile viruses:**

  These viruses can serve as a main threat to the devices which have significant computational capabilities. Viruses can take advantage of the loopholes in a smart system and can cause significant damage. Proper care should be taken while downloading the applications even on the mobile as well as desktop. Sometimes, malfunctioning SMS can also crash the Operating System.

- **Bluejacking:**

  This refers to sending messages to other users with Bluetooth-enabled mobile phones and laptops so as to exploit them by various means such as sending threatening messages or advertising. These messages can only be sent via Bluetooth so as to avoid these messages only a person can do is put Bluetooth on undiscoverable mode.

Apart from supplying electrical power to device, authenticity and integrity must be verified using cryptographically generated digital signatures. The person who has signed a legal certificate should only be authorized to run software while the device is booting. Infineon Pvt. Ltd. Along with many other companies has developed a range of technologies to deal with runtime threats and malicious intents.

System level security:

System level security is also significant for smart devices and the firewall of these devices should always be enabled in the operating to ensure the proper security. The device protocols in which the object or electronic device should be defined in their designated networks such as Home Area Network (HAN), Local Area Network (LAN) and Wide Area Network (WAN). Although, connected devices come with login names and passwords but to ensure more security one can keep double-level entry password such as in banking security system it serves as a fruitful. System level security is totally in user's hand as one should make aware children about the threats and damages of sharing their passwords of smart door key, smart connections and distributor meters. Along with that, software's should be updated on time to keep track of everything and make to it simple.

Antiviruses:

Antiviruses are need of every individual who are using smart devices so as to protect their devices from viruses, Trojan horse, worms and spyware. This malware software steals the vital information and takes advantage of it. Antivirus constitutes of programs which help to identify these viruses and try to eliminate their affects. Antivirus uses two techniques to figure out these viruses and to resolve them:

i) Examining files completely so as to cross check if it matches with any of the virus in virus dictionary.

ii) Tracking the behavior of computer programs as if it is found suspicious relevant action is taken.

To avoid viruses to enter desktop or laptop following modes are taken care:

i) Static scanning is done to check if any of the file is being infected by the malware.

ii) Dynamic scanning which is real-time scanning to prevent being infected at first place.

Fully licensed software should be used with the latest updates.

Firewalls:

Firewall acts as a barrier to prevent authorized access to a networked computer system as well as IoT devices. Networked firewall is used to isolate one network from the other. Packet filtering technique in firewalls is used to prevent unwanted packets entering the networked area by accepting and denying packets. Security level in IoT devices depend on the settings of firewall software.

Monitoring:

Monitoring is an important task when we consider the security of home, building or company. Monitoring can either be done by CCTV Cameras or Internet Protocol (IP) Camera or human physical security.

CCTV/IP Camera:

IP camera is simple video camera which can be connected directly to internet without the need of separate computer. CCTV cameras are used to monitor the process/event in parts from a central room. CCTV is a part of the security process and is not a complete solution. Deployment of IP cameras have become necessity in Network Address Translation (NAT) environments along with dynamic locations. In manufacturing and mining industries, IP cameras and RFID’s are used to provide security to the workers.

Wireless Sensor Network (WSN):

WSN is deployed in smart home or smart office to enable remote intruder detection and image streaming on cell phone. Research is conducted on WSN because the nodes are exposed to attacks in ruthless environment and it is being used in military applications such as ocean surveillance system for the detection of submarines and battle field surveillance. Security can be enhanced by protecting the nodes scattered in unsupervised environment. [62]

We have already discussed about the encryption and fundamentals of security. Now let's discuss how security can be enhanced at three layers of IoT framework:

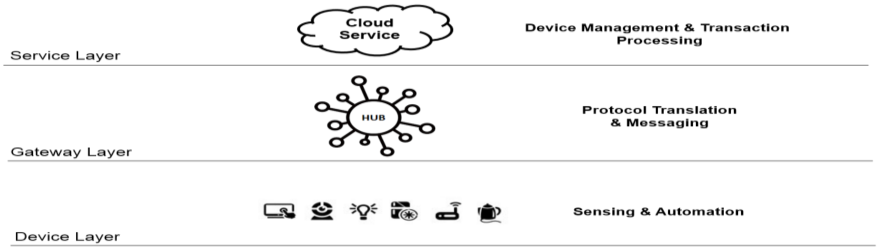

Cloud Service
Device Management & Transaction Processing
Service Layer
HUB
Protocol Translation & Messaging
Gateway Layer
Sensing & Automation
Device Layer

Figure 10 – Three layers of IoT framework taken from https://www.citrix.com/blogs/2015/04/09/whats-required-to-secure-the-IoT/simpleIoTframework/

Securing the device layer:

This layer serves as a junction of people, places and things which can be simple as well as complex. Simple things include connected thermometers and lightbulbs whereas complex things include medical instruments and manufacturing equipments. Security should be built in the design of device itself so that devices can maintain their authenticity, privacy and integrity. Security should be tight enough to avoid any misuse or unauthorized use and should be flexible enough that it could allow secure connections even for temporary basis. Design should be secure enough that no one is allowed to fetch sensitive data from devices such as personal information, credentials or cryptographic keys. One more important thing to notice is that IoT devices should have a long life as if we come across any kind of exploitation, it can be readily addressed with the software update.

Securing the gateway layer:

This layer is used for ensuring the secure communication between the things and cloud services and this communication can be done over public and private networks. Encryption techniques are ideally suitable for technologies such as TLS/SSL but are not suitable with microcontrollers which have limited RAM. To elaborate this point further let's takes an example of Arduino Uno which takes 3 minutes for encrypting a payload while Elliptical Curve Digital Signature Algorithm (ECDSA) takes only 0.3 seconds for encrypting the same payload. This makes the point clear that product manufacturers cannot take an excuse of resource constraints for the lack of security in their product. Another point to be considered while talking about the security at gateway layer is the communication over different protocols rather than Wi-Fi. It means that all the security fundamentals should be taken care while communicating over protocols such as Zigbee and Z-Wave.

Securing the service layer:

This layer is used for representing the management system and is used for classifying the applied policies and rules. To avoid the misuse of data being generated it is important to maintain an audit trail which will enlist all the changes made by the users and devices. Monitoring data could also be able to view the compromised devices which show abnormal behavior. Maintaining consumer privacy is the top requirement of government agencies so as to meet these requirements agencies have created a set of rules which every connected device must follow: it says that customers should have fine control over the data being generated so that they can visualize the data which is sent to cloud if want to, data of each customer should be segregated and they should have their own encryption key and when analyzing the data it should be anonymized. [66]

5.7 Power management:

Power management is also imperative feature in the wearable and portable devices that rely totally on batteries or other non-wired sources. Power consumption of each device is different as each device has different attached sensors, actuators, integrated circuits, storage and processing capabilities. To extend the battery life of a device, sometimes it needs to be put into sleep mode or low power mode. If the data transmission is over Wi-Fi network or there is lot of processing going on device then power consumption would be high and would eventually fall when the device is set to idle. It is vital to optimize the dynamic and static power of battery operated devices. This power optimization can be addressed in three different ways:

- **Power management control:**

  It should address how much frequency and voltage is required for each IoT device. System designer should identify all the power states such as on, idle, sleep and off to maintain the power management control. In the on state nominal voltage should be applied and the frequency cycle should be at full speed. In idle state voltage to be applied should be reduced but the frequency cycle should be again at full speed. In the sleep state voltage applied should be to that minimum level as it can be only used for memory and f/f retention and frequency cycle is gated off. In off state no voltage is applied and frequency cycle is too gated off.

- **IP implemented for low power:**

System designer should include the IP blocks to include the power control wrappers and frequency scaling which will enable a valid power state within a device. The main objectives which system designer must understand for implementing IP for low power are: first one is that leakage power will dominate the power consumption if device is turned off for a majority of time and second one is that dynamic power will dominate power consumption in the vice versa state. If the communication systems work inefficiently then lot of saved dynamic power is lost. So if the data rates are low and communication is point-to-point then BLE (Bluetooth Smart) should be used and for higher data rates Wi-Fi is the best solution. [67]

- **Power aware software**

5.8 Memory:

Antifuse OTP (One Time Programmable) memory is the best fit for meeting the requirements of these IoT based devices. This One T- Fuse memory cut down any further steps by decreasing the bit-cell area. Programming of bit-cell is done for higher reliability through transistor's channel and also through a pump called as integrated charge pump. 1T- OTP is more secure than floating-gate MTP architectures. It can operate over wide temperature range such as above 150 degree Celsius. [70]

Chapter – 6

Major challenges for IoT industry:

Internet of Things is growing like a snow-storm. According to the report of cyber Security Company, by 2022 every household will be connected with 500 devices which used to be 9 devices. This connected technology where everything from retail shops to hotels and from cars to airplanes is linked also comes with its own caveats and requirements which needed to be fulfilled with proper approaches and solutions. Major challenges to be expected in this growing industry are:

6.1 Security Challenges:

As more and more devices are connected so is the concern for security as more data sharing increases the vulnerabilities for customer data theft which could reveal the data from customer health to financial information through internet-enabled medical gadgets and electronic gadgets. Internet of Things is mixture of digital world with the physical world which requires more and more secure infrastructure to avoid the terrible accidents such as data breaching and hacking of gadgets. There have been many cases of data breaches but the recent one is from Germany where almost 16 million citizens were affected by the accident. Basic networking devices such as routers, satellite receivers, network storage and smart gadgets such as TV's and car are easily to hack. There have been several incidents to prove that cracking the entire network is no more catch-22. Recent example of this is given by Matthew Garrett when he was able to connect his computer to a tablet which is used for controlling lights in the entire London hotel.

There are many factors contributing to the rise of insecurity in these connected devices. One factor out of all these is to remain ahead among the competitors. Every vendor is in Bear Flag state to bring out the next innovative device before the other competitors do. Following these criteria illustrates that vendors are more interested in fulfilling their own coffers rather than considering the impact of threat because of their insecure gadgets.

Another factor can be following traditional method of coding as most of the IoT programmers often come from embedded system programming background and are unaware of the threats of threats of IoT programming. They usually don't have the proper knowledge to program for a hostile connected environment of the internet and end up making a code which is easier to exploit.

Other factors such as scalability and laziness of customers have also contributed to the rise of insecure IoT devices. Most of the security solutions today are created considering the general computing devices in mind. Most of the IoT devices are unable to deploy such security solutions because of lack of computational power and proper operating systems. Most of the consumers are too lethargic to keep the track of updates such as performing the basic steps while updating their systems. They don't see the broader view while purchasing a new device despite the cheaper price and attractive features which make them prey to the security threats.

6.2 Privacy challenges:

Some of the IoT devices collect sensitive data which is protected by the legislation and vendors and manufacturers don't take required precaution measures while storing this data. It should be the responsibility of the vendors or manufacturers to discard or remove this personally identifiable information so that consumers aren't exploited if there is any data breaching.

There is one more thing which needs consideration is that when data is generated by a single device it does not seem to be that harmful but when combined with other devices it could turn out to be terrific as it could reveal the life pattern of an individual if it is reached by the bad people.

Now, let us discuss some of the major threats or challenges to the privacy of consumers because of the evolution of IoT:

6.2.1 Identification:

Threat of identification is dominating every other threat because of the following technologies: firstly, Surveillance Camera technology which is integrating at a larger scale and is being used for analytics and marketing purposes as well. Facial database is easily available from the Facebook which could be used for unlawful practices. Secondly, fingerprints database will also easily accessible because of the interconnection and vertical communication of daily things will open up the identification of devices. Thirdly, speech recognition is being widely used in mobile applications because of which speech database is already built and can be amplifies for attack vectors.

6.2.2 Localization and tracking:

Tracking can be easily done through different means such as GPS, internet traffic or cell phone location. Consumers will be exploited through the GPS stalking as their location will be stalked by someone who they don't want to. These Location-Based Services will be in most use by the evolution of IoT and which will make the data collection more persuasive and users will be less aware as if when they are being monitored by someone and are involved in the risks involved.

6.2.3 Profiling:

Profiling means compiling the data of individuals and then inferring the data for their greed or interests. It is commonly used in e-commerce businesses. The impact of this feature in the terms of IoT evolution is twofold- firstly, this evolution will bring the explosion of data as more and more devices will be connected. Secondly, data collection which was done quantitatively will be more qualitative as it will dig deeper into lives of people.

6.2.4 Privacy-violating interaction and presentation:

It means conveying the private information to the unwanted audience through the use of public medium. The upcoming IoT applications such as smart retail, transportation and healthcare will require heavy communication with the user. So it can be imagined that how this information will spread quickly because most of the interaction of people with things will be in public. Such conversations should not be done in public such as queries related to health or any precarious topics.

6.2.5 Lifecycle transitions:

Privacy is disclosed when smart things change their spheres during transitions such as photos and videos remain in used phone. Sometimes, such data is really disturbing. Data aggregated in the smart things will reveal most of the lifestyle of an individual. [71]

6.3 Connectivity challenges:

Connecting so many devices will be the biggest challenge that IoT industry will face. For now we highly rely on centralized, server/client paradigm to connect and authenticate different nodes in a network which is okay but what about the time when hundreds or thousands of devices will be involved. So at that time such networks will require huge investments and expenditure in terms of maintaining cloud servers that handle large amount of information exchange and if this server goes down entire system will be disrupted.

Future IoT will have to rely very much on decentralized network architectures. This will come into existence by pushing the functionality to the edge by using fog computing models which will take the charge of time critical operations and cloud servers will take the responsibility of data gatherings.

Some of the other approaches on which we can rely are peer-to-peer communication models where there will be direct exchange of information between the devices after they identify and authenticate each other and will not need any broker to complete their communication. Challenges involved in this kind of architecture can be overcome by the use of phantom protocol.

6.4 Compatibility and longevity challenges:

As IoT is going through its growing stage so many technologies are trying to be become the standard technology which can be used for everything related to IoT. At present we have competing technologies such as Zigbee, Z-wave, Wi-Fi, Bluetooth and Bluetooth Low Energy (BTLE) and these all trying to be a standard technology for providing the transport mechanism between the devices and hubs which will further require extra hardware and software while deploying these devices.

Some of the other compatibility issues that come into limelight are through the non-unified cloud services and lack of usage of M2M protocols. Some of the technologies which are in high use will become obsolete in the next few years and will make the devices useless which rely on those technologies. Some of the appliance such as smart TVs and fridge will be in use for much longer and will be able to serve people even if their manufacturers goes out of service. To make the work of developers easier some of the platforms such as Afero and Apple's Homekit will enable developers to focus more on functionality rather than other issues as these platforms will take care of other challenges by themselves. [72]

6.5 Interoperability challenges:

Interoperability is also a big issue in adapting these IoT devices because most of them are proprietary and incompatible to each other. Fragmentation has raised the cost incurred for suppliers, developers and users. According to the research it was that interoperability issues are raised when adapting the newly IoT based solutions in the US. The only solution for balancing the effects of fragmentation of devices is to purchase the high quality software and then collect and spread this information.

Most of the developers want their IoT solution to operate on multiple sensors; all they need is to modify their service according to the sensor type or manufacturer. Fragmentation comes along with integration costs and maintenance costs for the developers. We already discussed that usage of proprietary solution/ non-standardized solution creates hurdles such as incompatibility between the devices.

6.6 Device management:

Device management is another important challenge that needs to be addressed while deploying the IoT solutions. Maintenance costs, deployment costs and incremental improvements all will be added to the comprehensive device management capabilities. According to the research report it was found that in 2014 US government asked Tesla and General Motors to take back some of their cars due to potential fire risk coming from defective electrical component they have used while manufacturing these cars. Tesla Company has updated their vehicles just by installing a software patch but on the other side General Motors didn't have any remote services so they have to manually update their 3,80,000 cars. So this example completely tells us that technology choice has made a significant difference in terms of maintenance costs and user experience for both the companies. [73]

6.7 Standards:

If proper standards are not followed the devices will behave inappropriately and developers will design products without considering their impact which may be positive and negative both. If these devices are configured and designed poorly they will give the negative picture to the networking resource they are connected to. Most of these cost constraints are there because everyone is rush-gold state to implement their IoT based solutions before their competitors could do. As structured data are stored in relational databases and are queried through the SQL while unstructured data are stored in NoSQL databases without a standard queried approach. Companies are more interested in implementing big-data tools which leads them to lack of human talent and execution systems.

6.8 Regulations:

There are certain legal and regulatory questions that need to be addressed just like the privacy. Despite the legal issues there are other issues which need to be addressed such as cross-border data flow, privacy lapses and security breaches. The main concern is that technology is advancing at a much faster pace than the regulatory policies.

6.9 Intelligent analysis and actions:

Challenges while adopting the intelligent analytics and actions are because of the following factors: firstly, sometimes, analysis is done inaccurately due to the flaws in model/data being collected. There are several algorithmic limitations which are exposed through the false positives or negatives. Secondly, legacy systems are structured in a way to handle the structured data but most of IoT businesses generate unstructured data. Thirdly, older analytics software works mainly on batch-oriented processing but for now all the data is first loaded in a batch and then analyzed. Fourthly, slow adoption of new technologies and greedy human behaviors don’t allow the adoption of analytic actions. [74]

Chapter – 7

IoT Alliance:

The IoT alliance sought to motivate and build the local IoTA networks throughout the world. Alliance particularly means to share the resources freely with any group or organization with similar objectives and motives. This sharing of material encourages the remote attendance at the events and helping each other to find the presenters for events. There are several consortiums in the industry; some of them are listed below:

7.1 RFID Consortium:

Main purpose of this consortium is to promote the adoption of UHF RFID technology and by providing the access to all the patents required for practicing the UHF RFID standards to all the industry participants so as to follow the standards announced by EPC global and ISO.

Applications:

This licensing program helps to improve the shipping, inventory management and other service benefits to the consumers, retailers and manufacturers.

Members:

It is open to new participants but the existing members are listed below:

- 3M Innovative Properties Company
- Convergence Systems Limited
- ETRI
- LG Electronics, Inc.
- Zebra Technologies Corporation

This logo illustrates that product is covered under RFID Consortium and should abide by the rules and regulations of this consortium.

Figure 11 – RFID Logo taken from http://www.rfidlicensing.com/

Countries which have registered patents under this consortium are mostly Australia, Belgium, China, EU, France, Germany, Great Britain, Italy, Japan, Korea, Netherlands, Singapore, Spain, South Africa, Sweden and US. [75]

7.2 NFC Forum:

NFC Forum has brought back the NFC technologies to provide the users reliable experience and to deliver secure and tap-based interactions for organizations across the world-wide. The main goals of NFC forum are develop certain mechanisms and test according to those so as to ensure that transactions are consistent and reliable across all the three modes of NFC. It's another main purpose is to be a leader in this industry competition so as to provide positive experience to the user by educating enterprises, service providers and developers.

NFC Forum provides a secure framework for application development, interoperable solutions and NFC- enabled transactions. It has helped the dozens of organizations by creating them committees and working groups. NFC Forum was found in December 2004 and in June 2006 they have outlined their own architecture and to the till date it has created 16 specifications. These specifications provide a road map to all the members and parties those who are interested in creating consumer products as if how their products should be. So we can say serves as a guideline.

Standards:

It has its own specifications such as Contactless Card Technology (ISO/IEC 14443 A & B, ISO/IEC 15693 and JIS-X 63 19-4)

Members:

- Apple Inc.
- Dai Nippon Printing Co., Ltd.
- Google Inc.
- Infineon Technologies
- Intel Corporation.
- Master card Worldwide
- NXP Semiconductors
- QUALCOMM Inc.
- Samsung Electronics Co., Ltd.
- Sony Corporation
- STMicroelectronics N.V.
- Visa Inc.

Application:

It is mainly used in Horizontal/Telecommunication. [78]

7.3 Wi-Fi Alliance:

Wi-Fi Alliance provides standardized Wi-Fi technologies and programs which assist in meeting the quality, performance, capability and security standards of the new products. It is observed that now there are more Wi-Fi devices than the humans on the earth. Main goals of Wi-Fi alliance are welcoming technology and inspiring innovation. Its mission is to encourage the acceptance of new technologies worldwide and recommending the fair worldwide spectrum rules.

This logo reveals that these products have passed all the validation tests, obey all the new security mechanisms and back all the advanced features.

Figure 12 – Wi-Fi Logo taken from https://www.wi-fi.org/who-we-are/our-brands/

Members:

Main sponsors of the Wi-Fi Alliance are Apple, Cisco Systems, Dell Technologies, Microsoft and many more. Contributor’s list is as Accton, Acer Inc., BlackBerry Ltd., Canon Inc. and many others.

Applications:

It is used in 802.11ax, Automotive, Coexistence, Dedicated Short Range Communications, Healthcare and Internet of Things. [76]

7.4 Zigbee Alliance:

Zigbee 3.0 is entire solution for making the smart devices to work together from the meshed networks to the open networks. It was found in 2002.

Standards:

There is no requirement to be fulfilled before becoming member in the alliance. Everything is clearly listed in alliance documentation from voting rights to rules for members those who want to participate in development of standards. There are certain requirements for standard development as members have to market needs. Before developing standard members have to go through MRD, TRD, 0.7, 0.9 and 1.0 . One more thing that no standard is confirmed until standard testing is done by implementing three standards which will enhance the quality control check of the standard.

Members:

Zigbee Alliance has three kinds of membership: Promoters, Participants and Adopters. Promoter members are Comcast, Huawei, Itron, NXP, Philips, Silicon Labs and others. Participants are Alibaba Group, ARM, CEL, ESI, GE and others. Adopters are A&D Co Ltd., Accenture Global Solution, Delta Controls Inc. and others.

Applications:

It is used in Smart Homes, Connected Lightning, Utility Industry and Retail Services. [77]

7.5 3GPP (3rd Generation Partnership Project):

It covers all the telecommunication technologies along with radio access technologies, core transport, security and quality of service.
Technical specification groups in 3GPP are:

- Radio Access Networks (RAN)
- Service and System Aspects (SA)
- Core Network and Terminals (CT)
- GSM EDGE Radio Access Networks (GERAN)

The main goal of 3GPP systems is to make the systems compatible from backward and forward so that user gets an uninterrupted experience. Latest example of this technology is Compatibility of LTE and LTE-Advanced. It has open membership.

Standards:

Main focus of 3GPP specifications are on IoT needs such as CIoT (Cellular IoT) and Vehicular Communications (LTE-Vx). Supporting organizations are from Europe, China, India, Japan, Korea and US (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA and TTC).

Applications:

It is not specific to any particular industry as it provides technologies which are relevant to many industrial domains. [78]

7.6 AVNU Alliance:

It was found specifically for the applications which have precise timing and low latency. It is open for formal membership not for public and confirmation of standards are done by members only but is open for consultation from external parties.

Standards:

It is based on open standards (IEEE 802.1 TSN, 802.1 Series, IEEE 1588, IETF DetNet and many others.). Supporting organizations are from Automotive, Industrial Automation and Audio/Video.

Applications:

It is mostly used by smart manufacturing, automotive and audio/video. [78]

7.7 BBF (Broadband Forum):

Broadband User Service (BUS) work area is a new area was created in 2015 so as to focus more on IoT related specifications. Earlier workgroup which used to take care all of these specifications was Broadband Home WG. TR-069 was provided by Broadband Home WG which is designed to provide communication between CPE and Auto-Configuration Server (ACS). It provides the broadband industry with reference implementations, test plans and technical specifications required for the assistance of broadband end user and for the service providers and application developers. It is open for both formal membership and for public.

Standards:

This BBF BUS WF will further develop TR-069 which was developed by Broadband Home WG and will also develop Universal Service Platform (USP) to take care of the existing use cases, machine-to-machine/IoT use cases. They have produced documents related to the developed TR-069 protocol. Some of them are listed below:

- TR-069: Amendment 1: CPE WAN Management Protocol (December 2006).
- TR-069: Amendment 2: CPE WAN Management Protocol v1.1 (December 2007).
- TR-069: Amendment 3: CPE WAN Management Protocol (November 2010).
- TR-069: Amendment 4: CPE WAN Management Protocol (July 2011).
- TR-069: Amendment 5: CPE WAN Management Protocol (November 2013).
- TR-330: TR-069 UPnP DM Proxy Management Guidelines.
- TR-181: Device Data Model for TR-069 (February 2010).
- TR-181 Device Data Model for TR-069 Issue 2, (May 2010).

- TR-181 Device Data Model for TR-069 Issue 2, Amendment 2 (February 2011).
- TR-181 Device Data Model for TR-069, Issue 2, Amendment 5 (May 2012).
- TR-181 Device Data Model for TR-069 Issue 2 Amendment 6 (November 2012).
- TR-181 Device Data Model for TR-069 Issue 2 Amendment 7 (November 2013).
- TR-181 Device Data Model for TR-069 Issue 2 Amendment 8 (september 2014).

Application:

BUS mainly focuses on the horizontal industries and the protocol specified (TR-069) mainly focuses on the Home/Buildings. [78]

7.8 ESMIG:

ESMIG is formed by the European countries whose main agenda is to provide services such as products, multi-commodity metering, displaying and managing at consumer premises. It is open only for formal membership and believes in open ratification processes.

Standards:

ESMIG does not believe in developing specifications so urges only for open standard use. Standards which ESMIG support are CEN/CENELEC/ETSI TR 50572 and these are updated on yearly basis. The specifications which are covered under these standards are mainly related to smart energy distribution systems. Supporting organizations are Apator, Chameleon, Ericsson, Gemalto, Luna, Vodafone etc.

Applications:

Its main focus is on vertical energy industries. [78]

7.9 ETSI (European Telecommunications Standards Institute):

ETSI is used to produce standards specifically for fixed, mobile, radio, converged, broadcast and internet technologies. The standards produced by ETSI mainly focus on enabling those technologies on which business and society depends. It is a non-profit organization whose member organizations are from 64 countries and are more than 800. Its primary agenda is to improve the life of coming generations and to resolve the technical issues. It is open to public and ratification of processes is done by the members only and is open for any external consulting.

Standards:

Totally rely on specifications.

Applications:

It also depends on the type of specification used and with which standard. [78]

7.9.1 ETSI TC ATTM:

TC ATTM closely works with Technical Bodies which are liable mainly to communicate networks and services so as to maintain the exact border line for taking care of member’s needs. Some of the protocols are excluded from the ATTM such as signaling but some of its services are still provided such as seizing, releasing the line, dialing and calling. Its primary goal is to engage and increase the expertise which can develop and maintain ETSI outputs on every facet of infrastructure and transmission. TC ATTM also focuses on providing support to customer application by working on end-to-end transmissions over networks. It is open to general public and ratification is done by members only.

Standards and applications:

Both depend on the specifications required and usage.

7.9.2 ETSI TC CYBER:

Its main responsibility is to act as savvy in the areas of cybersecurity and to build standards and maintain them so as to provide helping hand in the implementation of cybersecurity standardization in ETSI. Some of the other purpose is to fill the gaps where standards do not fit and to answer the policy requests related to the ICT sector. It is coordinated to the organizations such as European, National, International standards, ENISA, 3GPP, OneM2M and Professional. It is open to public and standard’s confirmation is done by members only.

Standards and Applications:

Both are specification dependent.

7.9.3 ETSI TC DECT:

This technology is particularly designed for machine-to-machine communications such as home and industrial automation. Attributes of this technology are ultra low energy consumption and secondly to cover wide regions. It is apt with all kinds of sensors, alarms and utility meters, devices which are used for automation. It is open to general public but ratification is only done by members.

Standards:

ETSI TS 102 939-1 and ETSI TS 102 939-2 are the main specifications. In ETSI EN 300 175 parts 1-8 are the specifications where technical details are found which are organized by layers and EN 300 175-8 is the specification of security model. Specifications of repeaters are under construction.

Applications:

- Home/building (Smart living)
- Smart cities
- Energy
- Healthcare
- Wearable
- Smart manufacturing/industry automation

7.9.4 ETSI TC ERM:

The horizontal TC has the following responsibilities: firstly, to deal with ETSI deliverables in whole or partially. Secondly, to deal with inter-system characteristics such as ETSI deliverables including radio spectrum parameters as well. Thirdly, to co-ordinate ETSI positions for the productive usage of radio spectrum. It is also open to public and confirmation and validation of standards is done by members only.

Standards and Applications:

Both of them are specification dependent.

7.9.5 ETSI TC HF (Human Factors):

It takes the responsibility of all the areas under information and communication technology (ICT). It is used to develop standards and produce reports that will set the criteria to build usability in digital network economy. It is designed to address the needs of everyone from young to old and disabled ones as well. It is open to public and validation is done by members only.

Standards and Applications:

Both of them are specification dependent.

7.9.6 ETSI TC ITS (Intelligent Transport System):

Its primary responsibility is to build standards and specifications which will further help to implement ITS provision services across the network such as for transport networks and multiple modes of transport without including the ITS application standards and EMC. It is open to public but some of the groups are only open to members. Ratification process is done by members and consultation can be done by external parties as well. ECC and CENELEC are the supporting organizations.

Standards and Applications:

Both of them are specification dependent.

7.9.7 ETSI TC Smart BAN (Smart Body Area Network):

This is a vertical technical committee which has the duty for development and maintenance of ETSI standards and implementing those Smart Body Area Network Technologies such as wireless and personal body area networks.

Activities part mainly includes the close communication with ETSI TC ERM, TC M2M and 3GPP. Some of the other activities are organizing regular meetings/workshops with appropriate bodies for personal welfare stakeholders and to establish relationships with external parties such as CONTINUA Alliance, Bluetooth SIG, CEN, ISO and HL7. It is only open for formal membership and ratification is done by members only and it is open for consultation from external parties. Supporting organizations are Toshiba, CSEM, Oulu, Telecom SudParis, Florence and the Hermes Partnership.

Standards:

It is dependent on Specification.

Applications:

It includes sectors of Health, Wellness, Sports and Medical as well as Retail sales.

7.9.8 ETSI TC Smart M2M:

It will provide specifications for M2M services and applications. Activities of TC Smart M2M will include the following: firstly, to be expert in M2M and internet of things areas. Secondly, to maintain the published specifications and develop the specifications as required for regulatory purpose. Thirdly, transfer the results of OneM2M to ETSI TC Smart M2M. Most of the groups are open to public but some are open to members only. Ratification process is handled by the members only and in consulting external parties can also participate. Supporting organization is OneM2M.

Standards and Applications:

Both are dependent on specifications only.

7.9.9 ETSI ISG CIM (Context Information Management):

The main goal of this alliance is to develop specifications and interoperable software implementation of CIM layer. This layer permits applications to update, manage and access contextual information as well as publishing that information through publication platforms.

Standards:

After careful analysis it will figure out in what way existing protocols need to be transformed to gain the access of flexible information. Whole sums of SDO documents are being examined.

Applications:

- Horizontal Frameworks
- Smart city vertical
- Smart agriculture
- Smart Factory

7.9.10 ETSI ISG IP6 (Internet Protocol6):

It produces information technology standards for fixed, remote, radio and other communications. It has the desire to create awareness about IPv6 when used in critical infrastructure and about other topics as well such as 5G, SDN, Cloud Computing and IoT. Its main objective is to reap backing from all the stakeholders to accompany them on pre-standardization logistics along with taking care of IPR issues and work procedures. It is open to public and ratification process is done by members only but is open consulting from external parties.

Standards:

Standards and protocols developed by other SDO's can be used.

Applications:

Cover multiple domains.

7.9.11 ETSI ISG MEC (Mobile Edge Computing):

MEC is used to provide the real-time information such as subscriber location and cell load so as to provide the services which are contextual based or application based. It provides an environment which has ultralow latency and high-bandwidth. To make customer experience best they have a regular check on their radio and network conditions. It is open to public and ratification is done by members only and consulting can be done by external parties.

Standards:

These are dependent on specification.

Applications:

Different industrial sectors are covered by different specifications. Smart City is mainly the focus in some specifications.

7.9.12 ETSI ISG NFV (Network Functions Virtualization):

The main goal of NFV was to clearly understand the pre-standards before implementing and considering the expansive standards so as to clearly understand them, define and to agree on the goals of this virtualization network functions. This consideration took place between 2013-2014 time of the year and the publication of standards that is the release of first specification took after that consideration.
The goal remains same in 2015 and 2016 which was to produce the technical specification by conveying the informational documents and normal documents whose aim was to probe for interoperability. Informational documents consist of analysis, use cases, detailed descriptions and studies, reports etc. while the normal documents consist of requirements, architectures and interface specifications.

With the help of these documents NFV will address the challenges such as making the virtualized platforms easier to operate than what are they today. Next, is to attain the virtualized network appliance which have high performance and to maintain stability of the network and service levels without the degradation of appliance load and relocation. This will make sure that level of resilience does not get affected on any hardware or software failures. This will also help to create virtual network appliance which will operate without any hypervisor or hardware configuration and to integrate the EMS, NMS, OSS, BSS and the other orchestration systems into the network operators. It is open to public and ratification is done by members only but the consultation can be done by external parties as well.

Standards:

It depends on the specifications.

Applications:

It is used in network infrastructure.

7.9.13 ETSI ISG OEU (Operational Energy Efficiency for Users):

The main goal of this ISG OEU is to create efficient indicators for environmental efficient ICT. These ICT systems are of high importance to the customers those who use it for car manufacturing, banking, insurance and airplane companies, governmental ministries and Network Operators.

With the backing ETSI ATTM members are acknowledged in ATTM#9 meeting and European Commission, ETSI members along with users have grouped together for non-for-profit organization (CRIP/CTO Alliance) which is OEU.

This CRIP/CTO alliance is an association of officials those who are investigating to rise towards the environmental efficiency of ICT areas through the short-term and long-term proposals. It is open to public and ratification is done by members only.

Standards:

It is dependent on specification.

Applications:

Energy efficiency

7.10 Fairhair:

This alliance is the combination of most of the leading industries such as Lightning, Building Automation and IT industry that aspire to aid the Internet Of Things. The perception of this alliance is to provide cost-effective, certified and secure IP based infrastructure. This will help to move from proprietary solutions to common building infrastructure which will back the constrained devices such as sensors, thermostats and so on. It is open for formal membership and ratification is done by general assembly in accordance to the voting rules.

Standards:

This alliance will develop specifications based on open IEEE and IETF standards.

Applications:

Smart building

7.11 Global Platform:

It is a non-profit organization which aims to develop specifications for the secure deployment and management of multiple applications on secure chip technology. Its standardized infrastructure allows the service providers to develop digital services and then later on deploy it in different channels and devices. Its security and privacy guidelines empower the combination of secure and non-secure services.

Global Platform has become the standard for trusted end-to-end deployment. This technology is widely adopted across sectors of finance, telecommunication, and government, automotive, healthcare and retail. This organization supports the long-term interoperability and scalability of application deployment. It is earlier open for formal membership and then can be used publicly after being a member. Ratification is done by members only and consulting can be done by external parties.

Standards:

It depends on the specification.

Applications:

- Mobile
- UICC
- Smart card

7.12 GSI:

This is a non-profit organization established in 112 countries with a total of more than one million member companies. It uses a different set of standards such as barcodes and RFID's. Most of the GSI standards are developed or are developing are for IoT. Auto-ID has developed and coined the term Internet of Things which is prevalent today and this can be accessed by using unique EPC on the tag attached to the object. Standards were developed and technology was brought for implementation in the market. EPCIS is a GSI standard that defines data for visibility modifications and for open supply chain. It is open for formal membership and ratification process is done by formal members and consulting can be done by external parties. Supporting organizations are from all the sectors such as retail, healthcare, transport and consumer goods.

Standards:

- ISO
- W3C
- UN/CEFACT

- IETF

Applications:

- Retail
- Healthcare
- Transport/logistics

7.13 GSMA (GSM Association):

The main agenda of GSMA is to build broader mobile ecosystem by connecting mobile operators with the different companies such as manufacturing handset and other devices, software and internet companies and the equipment provider companies. It has almost united 800 operators with 250 companies. This initiative helps the operators to increase their delivery of connected devices in the M2M market. It is open by formal membership and ratification process is a closed process and is done by members only and external parties are not even allowed to do the consultation part as well. Some of the supporting members are 3GPP and there are 800 operators and 250 companies to support this initiative.

Standards:

GSMA was specifically made for the public policy and the spectrum policy. One standard which was developed by GSMA was eSiM.

Applications:

It is mainly used in the different vertical areas of industry such as mobile application, management of mobile services, mobile API and for personal data.

7.14 HyperCat:

It is specifically designed for disclosing the internet of things data hub charts over the standard web technologies so as to enhance the discoverability and interoperability. Hypercat is an open, lightweight JSON-based hypermedia catalogs formats. Supporting members/organizations are IBM, BT, Flexeye, 1248 Ltd. and Thingful.

Standards:

Hypercat 2.0 has developed a new process BSI PAS which was completed in April 2016.

Applications:

- Integrated/complete IoT solutions (i.e. horizontal).

7.15 IEC (International Electro-technical Commission):

IEC covers all the electro-technical aspects that can come under it such as starting from plugs, wires to control and management. IEC supports various protocols such as IEC61850, IEC 61968/61970 (CIM), XMPP, DLMS/COSEM, OPC-UA and various field buses. Some of the group/committee members are listed below:

- SC3D was formed for classifying and identifying the product properties
- TC 8 was formed for maintaining the supply of electrical energy
- TC13 was formed for measurement of electrical energy
- TC 57 was developed for management of power and exchange of information
- TC65 was developed for the control and measurement of industrial processes
- SG8 Industry 4.0 was developed specifically for making manufacturing processes work smartly
- SG 9 was formed for Communication Technologies;
- SG10 Wearable Smart Devices;
- SyC Smart Energy;
- SyC Active Assisted Living;
- SEG1 Smart Cities;

7.15.1 IEC TC57:

Equipments and systems required for the preparation of standards are EMS and SCADA, distribution automation and information required for real-time and non-real time information. Some of the individual pieces of equipment such as telecontrol, systems and databases are out of control of TC57. It is open to public and ratification is done by members only and consulting can be done by external parties. Some of the supporting organizations are Energy, Smart Grid and Smart cities.

Standards:

- IEC/TR 62357.
- IEC 61968
- IEC 61970
- IEC 62325
- IEC 61850
- IEC 62351
- IEC 62346

Applications:

- Smart grid
- Smart city

7.15.2 IEC TC65:

It was established in 1968. The main goal of TC65 was to measure the industrial process, control and management. The scopes of SC65 were as – Goal of SC65A was to prepare the standards regarding the system's aspects such as operational condition and methodologies for the assessment of the systems. One important aspect was to prepare standards for the electrical/electronic/programmable electronic systems. Goal of SC65B was to prepare standards for hardware and software devices such as for measurement devices, analyzing equipment, actuators and for logic controllers.

Goal of SC65C was to prepare standards for wired, optical and wireless networks. The scope of this includes cabling, interoperability and co-existence. Goal of SC65E is to prepare standards that will address the device properties, classification, selection, configuration and monitoring. It is open to public and ratification is done by members only but consulting can be done by outside parties. Supporting organizations are manufacturing and industrial automation.

Standards:

- IEC 60050-351
- IEC 61010
- IEC 62443
- IEC 62708
- IEC 61326
- IEC 61131
- IEC 61499
- IEC 61918
- IEC 62591
- IEC 62657

Applications:

Smart manufacturing

7.16 IEEE Standards Association:

Mission of IEEE standards Association is to provide open, inclusive and transparent environment for market relevant. Framework defined in the IEEE 2413 is to promote cross-domain interaction and functional compatibility across IoT devices. IEEE-SA has developed several standards for different domains such as for communication – IEEE 802 and IEEE 1901 was developed, for Transportation – 802.11p was developed and for eHealth – 11073 was developed.

7.17 IEEE P2413:

This is a standard was developed for defining and describing the common things of IoT devices via the use of architectural framework in various domains. It is open only for formal membership and ratification is done by members only and consulting can be done by outside parties.

Standards:

P2413

Applications:

Horizontal

7.18 IETF (Internet Engineering Task Force):

The goal of the IETF was to ensure that usage of internet in good way by defining the terms and conditions in technical documents which will sure that there is no misuse of internet. Mission statement of the IETF is documented in RFC 3935.

7.18.1 IETF WG 6lo:

The main goal of 6lo is to make easier connectivity of IPv6 over constrained node especially those which have very limited power and processing resources. It will also focus on the optimized usage of network bandwidth. 6lo will work with 6loWPAN technologies which are documented in the RFC’s 4944, 6282 and 6775 for link layer technologies. It will also focus on making MIB modules which will monitor and do troubleshooting. It will mainly focus on the work which is close to constrained nodes such as ROLL and CORE but routing and security will be out of scope. It is open to public and ratification process can also be done by any parties.

Standards:

WG decision for the adoption of the following has been already done:

- draft-hong-6lo-ipv6-over-nfc
- draft-ietf-6lo-btle
- draft-mariager-6lowpan-v6over-dect-ule
- draft-schoenw-6lo-lowpan-mib
- draft-ietf-6man-6lobac
- draft-brandt-6man-lowpanz
- draft-bormann-6lo-ghc

Applications:

Horizontal industry

7.18.2 IETF WG 6TiSCH:

It is used to connect the large number of low-power and lossy networks to the resource-constrained networks. We have already discussed about the ROLL and CORE working groups which have defined protocols at the protocol stack and at the adaptation layer which is used with low power radios (IEEE 802.15.4).

IEEE 802.15.4e is a recent amendment of IEEE 802.15.4 with Medium Access Control. It is an emerging standard for the industrial automation and nodes in this network communicates via Time Division Multiple Access (TDMA) schedule. Communication between the neighboring nodes is done through timeslot which provides a bandwidth. This transmission is programmed in such a way that it avoids idle listening and further extends the battery lifetime.

IEEE 802.15.4e only defines about the link-layer mechanisms and it does not discuss anything about the network communication schedule. Initially working group limits its scope over the routing. In that case, if the node has joined the network its schedule cannot be changed as it should be preconfigured or have learned at the time of joining network. The work items of this group will include the following:

- It will focus on distributed routing not the static routing and will feature the different architectural blocks and signal flows.
- It will produce an information model which will describe how an entity can manage the TSCH schedule and provide a data model mapping for an existing protocol.
- This work will help to generate the best practice configuration for RPL and OF0 operations.

It is open to public and ratification is also done by public only.

Standards:

Working group has already adopted the following: 6TiSCH terminology, data model for CoAP, 6top drafts, minimal configuration and architecture.

Applications:

Horizontal industry

7.18.3 IETF WG ACE:

ACE is Authentication and Authorization for Constrained Environments. Mission of this working group is to enable the authorized permit to resources identified by URI and hosted on resource server. Initially work group will assume as if the resource access will take place using CoAP and is protected by DTLS. The authorization server is build through constrained environments. Working group will prosper from the available security analysis and implementation. It will also benefit through deployment experience. It is open to public and ratification is done by members only consulting can be done by external parties.

Standards:

ACE WG charter was approved on 16 June 2014 but RFC's are not produced yet. It has the following tasks – firstly, to use cases and their requirements are produced and secondly, in constrained environments resource access is identified by authentication and authorization mechanisms.

Applications:

Horizontal industry

7.18.4 IETF WG CORE:

CORE is constrained Restful Environments. It will define a framework that will deal with applications of constrained IP networks. Constrained IP network has small packets because of which there is much loss of packets and devices are powered off at any point of time but wakes up for brief periodic times. Initial work item is to define the specifications which includes following:

- It has the ability to perform certain tasks on device such as create, read, update and delete.
- Ability to notify the changes to other devices which have subscriptions of those publications.
- It has the ability to support the non-reliable multicast message which is used for manipulating resources on all the devices in a group.
- Description includes the device name and a list of resources and an optional name or identifier which is used by CoAP to advertise about the query for a device's description.
- It should have the ability to tell if the device is powered on or off by considering operational and manageability aspects.

It is open to public and ratification is done by members only but it can be done by those parties as well who are interested in doing ratification and consulting can be done by external parties.

Standards:

- RFC 6690 is produced for Constrained Restful Environments.
- RFC 7252 is produced for Constrained Application Protocol.
- RFC 7390 is produced for Group Communication for the Constrained Application Protocol.

Applications:

Horizontal industry

7.18.5 IETF WG COSE:

COSE is CBOR Encoded Message Syntax. CBOR is Concise Binary Object Representation format which is used for serialization of data structured to extend it to a JSON model. COSE explores to make a CBOR based signing object and encryption. One inspiration behind the COSE was to reuse the functionality from the JOSE group. JOSE has completed the JSON representation for cryptographic keys, message authentication, encryption and digital signatures. It is open to public and ratification is done by members only and is open for consultation from external parties.

Standards:

COSE WG charter was approved on June 3, 2015. RFC's related to this WG are not still produced. After the production it has to do the following tasks:

- CBOR specification will cover the same cryptographic formats but with optimization for constrained device processing.
- Algorithms which are appropriate for constrained environments will be registered such as AES-CCM-8.

Applications:

Horizontal Industry

7.18.6 IETF WG Deterministic Networking (DetNet):

This WG group mainly focuses on the layer 2 and layer 3 data paths. These data paths can provide bounds on latency, loss, packet delay jitter and high reliability. WG addresses the layer 3 aspects which are required for supporting the applications with deterministic networking. This DetNet combined with the TSN (Time Sensitive Networking) which was defined for conducting the layer 2 operations. Both WG were combined to form a common architecture for both the layers – 2 and 3. Examples are multimedia in transportation, engine control systems and professional and home audio/video.

Initially, WG will focus on the every network available that is not only the networks within the single administration but will also focus on closed group networks as well such as private WAN's and Campus wide networks. It will not waste energy on large group of domains such as internet. The WG will design an architecture which will include everything from time management to security aspects which are required to enable multi-hop, forwarding and latency. WG is applied to unicast and multicast flows which will allow the network to reserve or release the resources when they are no longer required. Layer 3 technologies which can be used without any modification are IP and MPLS.

It is the responsibility of WG to document which environments and topologies are inside and which are outside of the scope of DetNet architecture. This WG is independent of the path set up protocol and mainly focuses on the data plane aspects. It is chartered to work in the following areas:

- As we have already discussed earlier that it will focus on the overall architecture starting from data plane, OAM to security aspects and will also document the usage of IP and MPLS to support the data plane methods over layer 3.
- It will identify what kind of information is required for flow establishment and what can be used by reservation protocol or YANG models. Information related to control plane will be independent from the protocols which are used for advertisement of this information.
- Deterministic networks will have the vertical requirements such as professional audio, electrical utilities, building automation systems and wireless for industrial applications.

This WG coordinates with the other IETF groups as well such as CCAMP, PCE, TEAS, IS-IS and 6TisSCH. WG deliverables include the following:

- Overall architecture.
- Data plane specification
- Data flow information model
- YANG model augmentations

It is open to public and ratification is also open process. Standards are dependent on the specification.

Applications:

Horizontal industry

7.18.7 IETF WG Dice:

Constrained Application Protocol can be used to manipulate the devices which are secured by Datagram Transport Layer Security in constrained environments. Constrained environments include both the constrained devices and constrained networks.

- First task is to define a DTLS profile which is compatible with these connected applications and can be implemented on constrained devices.
- Second task is to define how DTLS layer can do transmission securely of multicast messages and for this session keys are required and changes may be done to DTLS handshake later.
- Third task is to do the investigation related to issues such as fragmentation, re-transmission and re-ordering of messages around the DTLS handshake in constrained environments.

For initial setup, key management and multi-cast sessions are out of scope of DTLS state machine. This WG will work closely with CORE, TLS and LWIG. It is open to public and ratification is also open to public.

Standards:

- Secure group communication specification
- DTLS for IoT profile specification
- Secure group communication for IoT
- DTLS for constrained environment profile

Applications:

Horizontal industry

7.19 IRTF (Internet Research Task Force): T2T RG (Thing to Thing) proposed RG:

T2T RG will focus on doing open research on turning the Internet of Things into reality and on internet where constrained nodes can communicate with themselves and with wider nodes. Main focus of this RG will be on connecting the devices to IP and making the data and management functions available at the end of application layer. Main purpose of this RG is to understand and manage the single purpose silos and gateways and scaling the applications in one network. Next, is to understand the considerations related to deployment, scaling and cost of ownership. It is open to public and ratification process can be done by members and by other parties. Supporting organization is T2T RG which cooperates with IETF.

Standards:
T2TRG

Applications:
Horizontal industry

7.20 International Telecommunication Union – Telecommunication Standardization Sector (ITU-T):

In this study group experts are gathered from around the world to create and define international standards. This study group was established in June 2015 and the first meeting was October 2015 to have discussions about IoT and smart cities and its requirements for standards and applications. IoT related groups have been published- SG11 will look after the interoperability, protocol and testing aspects, SG13 on networking aspects, SG16 on applications and SG17 on security aspects. Other groups known as ‘Focus groups' were also involved in IoT and smart cities- for M2M service layer, smart water management and smart sustainable cities. Study group 15 includes smart grid and network aspects. It is open by formal membership and ratification is close process and no external parties involved in any consultation as well. Some of the supporting organizations are Telecommunication hardware and software, service providers, network providers, application providers and integrators. Some others were member state entities and national regulatory authorities.

Standards:
Some of the published specifications include SDO's standards and protocols.

Applications:

- Horizontal industry
- Vertical industry – home/building, vehicular/transportation, healthcare, cities and farming/agrifood.

7.21 ISO and IEC have combined to form JTC1/WG10:

JTC1 committee was formed when ISO and IEC merged together. JTC1 consists of 76 members and each from different country. In 2014 report was accepted which was presented by the members of organization. The main goal of this working group was to develop strategic business plan till then one standard was developed “IoT RA” which specifies the IoT conceptual model, conceptual reference model from different IoT domains. Every document has to clear the 6 stages to be an international standard. Documents which are approved are only available through subscription or purchase. Ratification is done by national experts.

Standards:
Every standard will have functionality and opening for both semantic and pragmatic interoperability levels.

Applications:
Horizontal industry

7.22 M2.COM:

M2.COM came into existence to build a platform for sensors which are associated with IoT and to add the computing ability in wireless connectivity of devices. It is open by formal membership. Some of the supporting organizations are Advantech, ARM, Bosch, Texas instruments and Sensirion.

Standards:
M2.COM has adopted 2230M.2 to support different wireless communication standards.

Applications:
Sensor applications

7.23 MIPI Alliance:

It is an organization which is used to define the interface specifications for mobile devices. All mobile companies are motivated to be a member of this organization including the semiconductor companies, software vendors, peripheral manufacturers and test labs. These member companies promote the reuse and compatibility in mobile devices.

- **MIPI Alliance specification scope:**

  This specification impacts both the hardware and software in mobile devices. MIPI alliance is analyzing the scenarios and is planning to continue with the specification in those areas which can benefit the industry. This specification only addresses the signaling and protocol part.

- **MIPI I3C Specification:**

  It is a bus interface which is used to connect sensors to processors. It combines multiple sensors from different vendors to improve the cost efficiencies. It gives developers an opportunity to make innovative designs for any mobile product. This specification integrates mechanical, motion, biometric and environmental sensors. To reduce complexity and increase flexibility it uses two-wire interface. For higher performance it supports data rate of 10Mbps.

- **MIPI Camera Serial Interface Specification (CSI-2):**

  This WG has created a design which can resolve any kind of challenge such as bandwidth, features and functionality. The new PHY and MIPI Alliance were released in 2014. These versions were introduced to improve the skew tolerance. Both of these are serial interface but can also the problem of parallel interface as well.

- **MIPI Display Serial Interface (DSI) Specification:**

  This specification defines the protocol between the host and peripheral devices. It defines protocols doing several functions such as link management, signal timing relationship and error handling while auxiliary buses are out of scope. This specification has defined high-speed serial interface so that developing components provide higher performance, low power and less electromagnetic interference.

- **MIPI RF Front End (RFFE) Specification:**

  This specification was developed to control RF Front-end devices such as Power Amplifiers, Low-Noise Amplifiers, filters, switches, antenna and sensors. To meet the cost and performance targets this specification provides low-complexity solutions.

It is open by formal membership and ratification is done by members only and no consulting from outside parties except at the time when there is agreement.

Standards and Applications:

Both are based on specifications.

7.24 OCF (Open Connectivity Foundation):

The main purpose of this organization is to align all the IoT standards so that such solutions can be developed which can work in same environment. With the help of OCF specification, wide range of consumers can interact and work securely. Its vision is to connect the billion of devices without any hurdle of manufacturer and operating system. It is open by formal membership and ratification process is close process and is done by members only and no consulting from outside parties. Organization which supports this foundation is OneM2M.

Standards:

- IETF
- W3C

Applications:

Smart home

7.25 OneM2M:

The main goal of M2M is to develop specifications which can really embed within various hardware and software devices and to attract the organizations which are related to transportation, healthcare, smart homes and industrial applications. It is open to public and ratification is done by members only and consulting can be done by external parties. Supporting organizations are ATIS, ARIB, CCSA, TIA and TTA.

Standards:

- Transport protocols such as HTTP, CoAP and MQTT
- Device management protocols such as OMA DM, OMA LWM2M and BBF TR-069
- Web socket protocol

Applications:

Horizontal industry
Vertical industry

7.26 OSGI Alliance:

This alliance is proven worldwide consortium which is used to create open specifications. These specifications create end-to-end connectivity and to increase the productivity. Technology provides remote management and interoperability for applications. The significant features of OSGI are to – enable the use of components across different platforms, taking into account dependency management, system components are reconfigured without updating or restarting, supporting native libraries deployment, security model to be defined and involving synchronous or asynchronous models for programming environments. It is open to public with compliance testing and ratification process is not open as it is done by members.

Supporting organizations:

Some of the supporting members are Adobe, Deutsche Telekom, Huawei, IBM, Liferay, NTT, Oracle, Paremus, ProSyst Software, Salesforce.com and Software AG, Orange, Telecom Italia, Sagemcom, Schneider Electric, Hitachi, NEC and Eclipse Foundation.

Standards:

UPnP, TR069, enOcean, OMA DM, HTTP/REST and JSON-RPC

Applications:

- Vertical industry
- Modular web application development

7.27 Open group/ Open platform 3.0:

The main goal of this group is to take the benefit of merging of technologies such as cloud computing, big data analysis, mobile computing and Internet of Things. It is basically designed for digital platforms so that business needs of enterprises are fully fulfilled. Ratification process is done by members and can be done by public as well.

Standards:

- Open messaging interface and open data format
- UDEF standard
- Cloud computing governance framework
- Open business data lake
- IoT open lifecycle management

Applications:

- Retail Smart Store
- Sustainable Shopping and Restaurant Street
- Multi-channel marketing
- Supply chain store brand integration
- Multi-channel customer service
- Open government data interchange
- Incident management
- Safe mobility
- Smart retail distribution

7.28 TM forum:

TM forum is highly recognized for connecting brilliant individuals and companies thus a diverse ecosystem to raise the digital business transformation. It comprises of tens of thousands of professionals that do everything from giving practical guidance to training for IT leaders of market leading organizations. TM forum has observed that there are different set of requirements for IOE services. IOE focuses on vertical smart X ecosystems and end-to-end operational capabilities. IOE standards and books include the following – REST based API's, architecture, dashboard and customer digital experience. It is open by formal membership and the ratification process is closed process and no consulting from outside parties except for the earlier cases when agreement was signed for consultation to be done by external parties. Supporting organizations are both the telecommunication companies – hardware and software companies, network and application providers, government and regional entities.

Standards:

Use standards and protocols developed by other SDO's.

Applications:

- Smart health
- Smart finance
- Smart mobility
- Smart climate
- Smart cities forum

7.29 Weightless:

It is a standard which is used for connecting low-power devices. It is open by formal membership and ratification is done by members only and no consulting from outside parties.

Standards and Applications:

Both are dependent on specification.

7.30 UDG Alliance:

It is an alliance which is used for building multi-protocol framework for IoT integration and interoperability in the both IP and non-IP based communication protocols. It is not open to general public and is specifically reserved for UDG Alliance members. Ratification process is closed process and is done by members only and even consulting is also done by internal parties only. Supporting organizations are University and European SME's.

Standards:

It is exploiting the standards developed by SDO's.

Applications:

- Smart buildings
- Smart cities
- Smart agriculture [78]

7.31 WWRF (Wireless World Research Forum):

WWRF's goal is to address the key challenges for the future use. Wireless world is used to address the innovation and infrastructural challenges and to achieve the technological capabilities from wide-area networks to short-range communications, sensor networks and optical networking. Supporting features of this forum are fulfilling the needs of users, taking care of service architecture and communication architecture. It is open by formal membership and ratification is closed process which is done by members only with no consulting from external parties. Supporting members are Nokia, Huawei and China Mobile, Qualcomm, Fujitsu, Bell Canada, HP, NEC, Ericsson, Intel, LG and DoCoMo.

Standards:

- ITU-R
- ETSI

Applications:

Horizontal/Telecommunication [78]

Chapter -8

Architectures of IoT:

There are different kinds of architectural patterns available for IoT. Now, let us discuss each of them in detail:

8.1 Three-tier architectural pattern:

As the name suggests it basically constitute of three-tiers: edge, platform and enterprise. These three of them play their significant roles in processing of flows such as data and control in different activities.

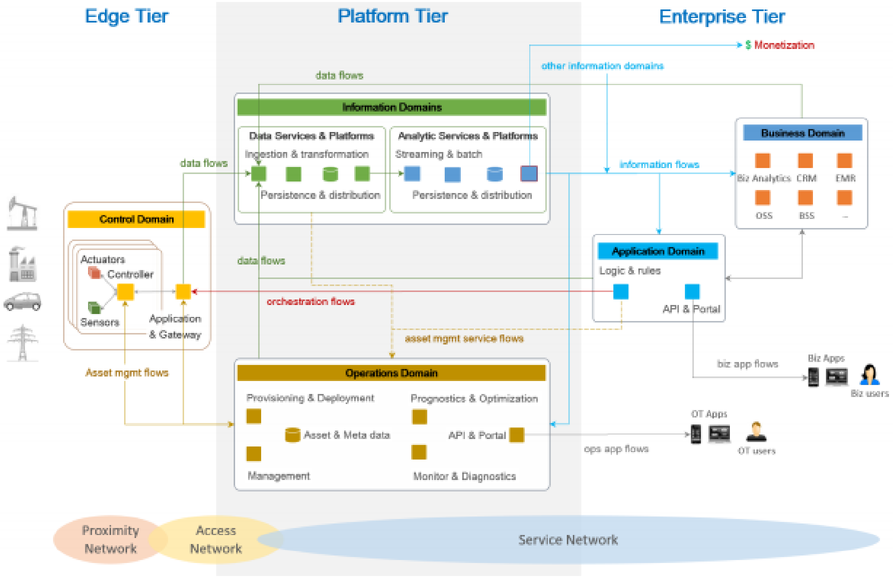


Figure 13 – Three-tier Architecture taken from https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf/

- **Edge tier:**

  Main functionality of this tier is to collect data from the nodes which are at the edge by using the proximity networks (networks which are not boundary specific and can be formed anywhere). Architectural characteristics of tier depend upon the use cases which include different features such as breadth of distribution, location and nature of networks.

- **Platform tier:**

  Main functionality of this tier is to process the information from enterprise tier to edge tier which includes different processes to be completed such as receiving and forwarding the information. It develops the processes and analyzes the flow of information from edge and other related tiers. It provides management functionality and other non-specific services like queries from different data structures.

- **Enterprise tier:**

  Main functionality of this tier is to implement the different applications and support systems which provide end-user services to operation specialists. It receives data stream and also sends the control commands from edge and platform tiers.

  Functional blocks:

  In the above architecture there are several functional blocks and now let us discuss what are they and their purpose. These blocks are part of that tier but are not used for any purpose. Data transform function is a functional block which is found in both the edge and platform tier and both has different functions.

Now let us discuss in detail about the different networks persisting in the three-tier architectural model of IoT:

- **Proximity network:**

  Proximity network is used to connect the edge nodes which mean connecting the different physical components of a device such as sensors, actuators and different control systems. It is used to bridge other networks through the cluster of edge nodes.

- **Access network:**

This network is used to establish a reliable connectivity between the edge and platform tiers for the data and control flow accuracy. It can be any kind of network such as public network, joint network, private network and 4G/5G network.

- **Service network:**

  This network is used to provide reliable connectivity and services between the two-tiers of architecture which are platform tier and enterprise tier. It is used to provide the security between the end-users and different services.

From domain perspective each tier takes care of different domains in the architecture. Edge tier handles control domain functionalities, platform tier takes care of operational domain functionalities and enterprise tier takes care of business domain functionalities. To enable edge computing functionalities in the tier some functionalities of information domain are implemented near to the edge tier. Operation domain is to provide services to other tiers as well. It provides services for the verification of asset credentials.

8.2 Gateway-mediated Edge Connectivity and Management Architecture Pattern:

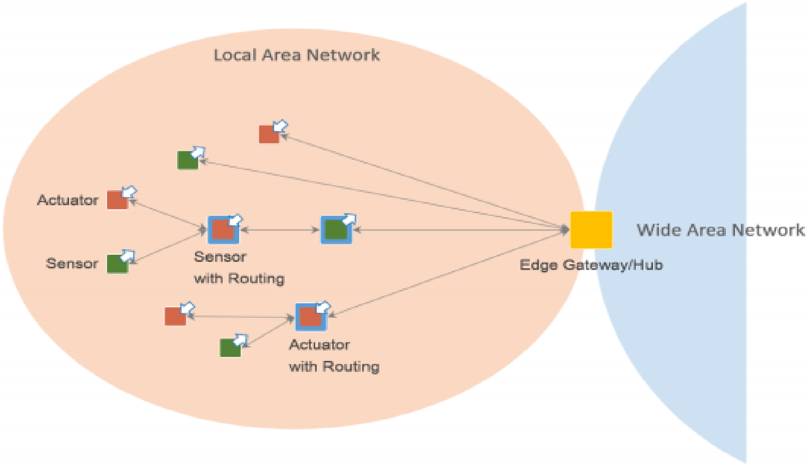


Figure 14 – Gateway- mediated Edge Connectivity Architecture taken from https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf/

As we can visualize from above figure, this pattern is highly used to provide connectivity between the local area network and wide area network. This pattern is used for localizing different operations being performed. Main advantage of this pattern is that it reduces the complexity of IIoT systems and to manage the assets. It is unsuitable to those systems which do not permit the stable clusters to be in localized network such as assets which are mobile in nature.

The edge gateway can be used as both management point and aggregation point whereas management point takes care of devices and assets and aggregation point takes care of information processing and control logic.

Local network uses two types of topologies:

- **Hub and spoke topology:**

  Hub is used to connect different nodes with each other and to other networks as well such as wide area network. Here gateway acts as hub. Main functionality of hub is to allow the in-flow of data and out-flow of control commands.

- **Mesh network topology:**

  This topology is also called as peer-to-peer topology. Purpose is still same like the hub and spoke topology like connecting nodes and network with the help of hub. The only difference over here is that it allows routing capability between the edge nodes. Routing paths vary and modify dynamically from edge node to edge gateway. This topology is best suited for areas which have low-power and low-data applications on geographically distributed devices.

It can be noted that from both topologies wide area network is not able access the edge nodes directly it has to go through the hub or gateway which acts as a single entry point for address translation and routing purposes.

Hub can support the following capabilities:

- Local connectivity is established with the help of serial buses and short-range wireless communication networks.
- It can support the different data transfer modes such as asynchronous, flow, event-based and store-and-forward mode through network and protocol bridging.
- It can support different data processing functions such as aggregation, transformation, consolidation and filtering.
- It can support the management of assets locally and remotely of edge nodes with the help of wide area network.
- Site specific decisions are performed within local scope.

8.3 Layered Data bus Architecture Pattern:

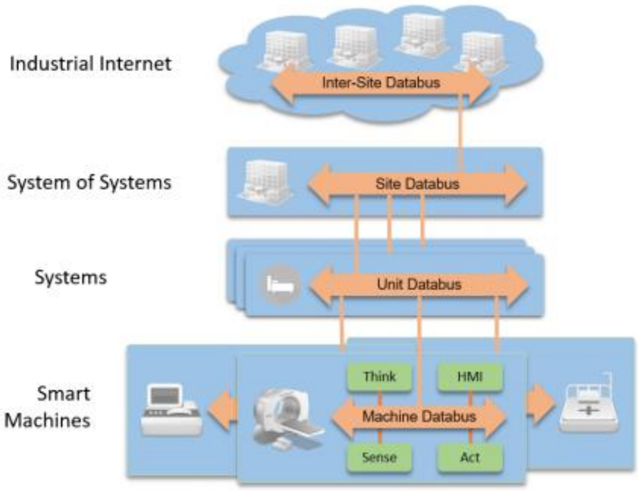


Figure 15- Layered Data bus Architecture taken from https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf/

This architectural pattern is used in many industries so as to deal with low-latency and peer-to-peer communication models. It is basically used in those communication areas where there is direct communications such as local monitoring and edge analytics.

As we can see from the above figure that data buses are used by smart machines for analytics and automation. Systems use buses for supervisory monitoring. System of systems uses data bus for enabling complex and cloud-based solutions.

Data bus:

Data bus is a combination of schemas which helps to communicate between the end points through a connected space. Data bus implements a common model which allows interoperability in communication. Data bus supports communication at all levels from devices to applications. Data bus can be embedded in a smart machine to connect its physical components such as sensors and actuators. At higher level, these data buses are used for communication between the machines. At third level which is system of systems, there data bus is used to coordinate, control and monitor series of systems. Each data bus contains a different data model and each of them functions differently.

Adapters are used to match different data models and also act as interface points for legacy systems. As the transitioning between layers increases so does the filtering decreases, as a result scope of control and analysis increases and data matching reduces. Main example of this kind of architecture is SCADA systems.

Along with the usage in control and enterprise domains it is also handy in provisioning and managing devices within the system. Nearby to data bus there is another communication model which is called as publish-subscribe model. Applications on the data bus take the advantage of this model as they can subscribe the data which they want and publish the information they want to produce. Communication model performs both the tasks – discovery and delivery. Television, radio and magazines define the time-critical systems.

This pattern architecture provides the following benefits:

- Fast delivery which may be in milliseconds or microseconds.
- Automated information and application between buses.
- Integration is scaled at a large extent that comprises of large number of sensors and actuators.
- Availability is infinite.
- Complex system design development. [79]

8.4 Fog computing architectural design:

Fog computing architecture is based on Open Fog consortium which was founded to support the cloud and edge architectures. This consortium defines fog computing as horizontal architecture that allocates resources and services from cloud to things. Fog computing provides different tools such as managing and securing resources that inhabit at the edge. Edge architecture mainly works with servers and applications and excludes cloud while fog architecture works mainly with cloud.

The main objective of the fog computing consortium was to create standards so as to enable IoT systems to operate freely. Considering that, consortium set six working groups which mainly focus on their primary agenda such as architectural, security, software infrastructure and testing. In 2017, new architecture was established called as open fog reference architecture.

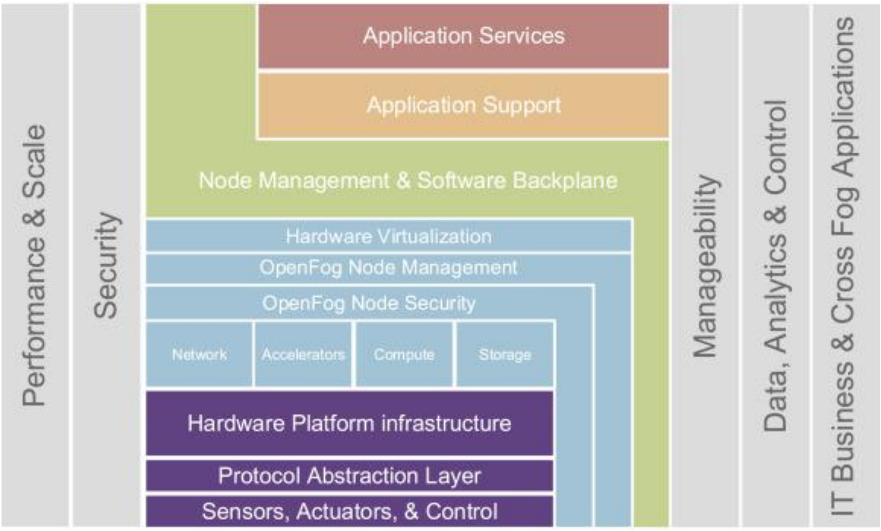

Performance & Scale
Security
Application Services
Application Support
Node Management & Software Backplane
Hardware Virtualization
OpenFog Node Management
OpenFog Node Security
Network
Accelerators
Compute
Storage
Hardware Platform infrastructure
Protocol Abstraction Layer
Sensors, Actuators, & Control
Manageability
Data, Analytics & Control
IT Business & Cross Fog Applications

Figure 16 – Fog computing Architecture taken from https://www.sciencedirect.com/science/article/pii/S2352864817301335/

This architectural pattern consists of system, software and node view. Node view basically accounts for the lower two layers- sensors and abstraction layer. System view is that view which is composed of nodes and components to form a platform. Software view accounts for the three layers above the hardware layer. It is composed of five perspectives which are basically on the left and right side of model such as performance, security, manageability, and control and fog applications.

This fog computing architecture was tested experimentally with smart pipelining monitoring, crowd sensing on the roads, face recognition and emergency services. Communication is possible through fog nodes via wired and wireless transmission and is also used for processing modules such as Graphics Processing Units and Field Programmable Gate Arrays. Fog nodes are connected to sensors and actuators through interfaces. Basically fog computing model work with three tiers in the system but more tiers can be added in the system if there is a demand for special application.

At lower level fog nodes are specifically focused on data collection and normalization of sensors and actuators. At the next tier, they are mainly focused on filtering and compressing data. At the tier which is more close to cloud, fog nodes purpose is aggregate the data and bring out a useful knowledge out of it. It may happen that nodes which are at the edge can do less processing and storing functions than the nodes at the higher levels.

Traditional computing model is still in demand as some functions are more beneficial to be carried out in centralized cloud. 5G Radio Access Network (RAN) is present everywhere and seamlessly supports 100 billion connected devices and high Quality of Service requirements as compared with 4G LTE networks. C- RAN is the combination of wireless network and computing technologies. Original BS is separated into two parts -   baseband resources in BBU's centralized model and the RRH's in BBU's pool via wired/wireless links. CRAN's have several advantages such as high spectral efficiency and energy efficiency. H-CRAN model does not have any front haul requirements with higher nodes.

There are still disadvantages in H-CRAN model such as lacks the processing and storage capabilities at the edge of the network. Taking the advantage of this con, new model was proposed F-RAN which covers all these cons and hence are more reliable and have low latency. [80]

8.5 Multi-tier data storage:

It is an architecture that differentiates the storage of tiers from other tiers so as to increase the performance. Each storage tier can be separated on the basis of their performance, capacity and archiving purposes.

8.6 Distributed Analytics:

It an architecture which combines the proximity analytics with the intensive analytics at the edge of centralized parts of architecture. The architectural pattern comes as beneficial factor when latency or other constraints are fully centralized.

8.7 Lambda Architecture:

This is the one kind of architecture which was not designed specifically for IoT but for data flow and analytics. Lambda architecture is efficient to handle the massive flow of data by separating into two views- batch view and stream view.

Architecture is sub composed of three layers-

- Main functionality of batch layer is to mastering the append-only data.
- Serving layer is used to index the data into batch layer for efficiency.
- Speed layer is used to provide low-latency functionality for the stream view.

Incoming data is first sent to batch layer for higher latency and processing while the speed layer is used to process the data more quickly. [81]

8.8 Asset Integration Architecture:

Asset Integration Architecture involves the combination of assets along with backend services for enterprise applications. Asset can be a vehicle, machine or vehicle which is of interest to the enterprise. Assets usually have in-built board power management and device control for various tasks.

In IoT enterprise the biggest challenge is to manage fixed or mobile assets which can be achieved through a specialized tier which creates a link between them which is known as IoT cloud. Tier usually works with software agent and gateway and this gateway is used to connect different types of assets and enable remote connectivity between the enterprise backend. Software agent is used to encapsulate the different connected devices and providing the homogeneous facilities such as security, local event management and lifecycle management.

Remote assets are managed through database which is implemented by IoT backend. Asset repository is usually combined with event management and remote software distribution. IoT backend uses different kinds of technologies such as ERP (Enterprise Resource Planning) and PLM (Product Lifecycle Management).

Let us discuss about the areas where AIA can be easily mapped:

- **Automotive industry:**

  It is highly in demand in Engine Control Units which are distributed around the power train. Vehicle Control Unit acts as a head of all the systems and serves as a integrator for other systems. Vehicle fleet management is an example of Telemetric Control Unit.

- **Smart Homes:**

  There are several devices available to combine the functionality of gateway with single device connected at home such as Bluetooth, Z-Wave and Wi-Fi.

- **Manufacturing:**

  Microcomputers are available to control and automate the industrial processes. Supervisory Control and Data Acquisition support and mange network of Programmable Logic Controllers.

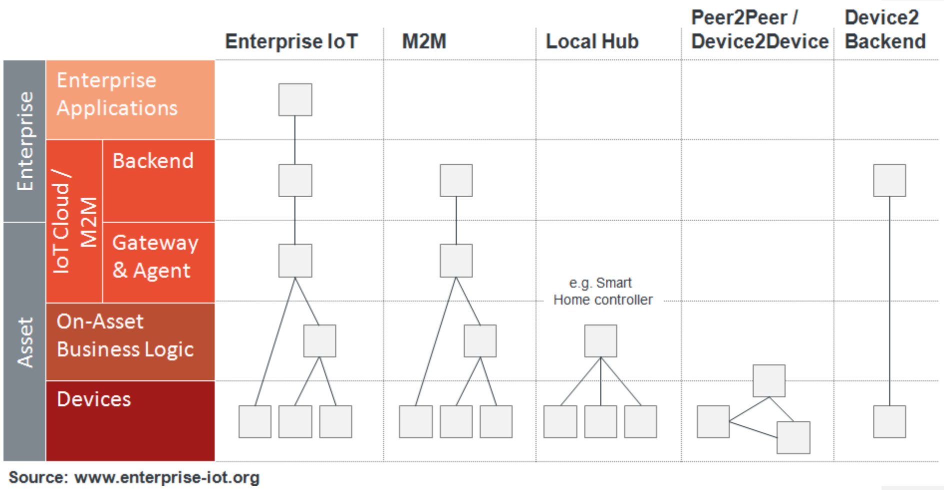


Figure 17 – Asset Integration Architecture taken from http://ignite-IoT.org/wp-content/uploads/2014/12/Ignite-BB-AIA-Patterns.png/

It can be visualized from the above figure that there are several patterns- the one at the right side is Device2 Backend in which the name also suggests that device is directly connected to the Backend. Peer2 Peer or Device2 Device is a pattern in which there is direct interaction between the peers or the devices. Local Hub is a pattern in which multiple devices are connected to each other through a local hub. M2M is a pattern in which multiple assets are connected to a central backend. Advanced services are provided by Enterprise IoT pattern. [82]

Conclusion:

As we have studied different standards which are still developing specifications, so we can say that IoT can get complicated with the new technologies will emerge. As in IoT technology stack some layers are given more preference as their standards are at spar while there are some layers to whom standard is a tough word that is they don't have any standards.

If we consider the case when there is no common communication method between the devices, then devices of different brands won't be able to do the information transfer to each other. Thus, will recluse the idea of connected devices in such case. Let us take an instance of a company which develops smart clothing and a company which develops smart home technology there are significant chances that they won't be able to communicate to each other as they both would be using different types of communication protocols which will lead to rise of interoperability issues and customer dissatisfaction. If their communication protocol or standard is same then the case will be different. So it all depends on standards.

Apart from communication model there are certain other issues or challenges which should be addressed. Internet of Things deals with different technologies like state full and stateless, hard and soft and constrained and unconstrained. If we consider another example of RFID Tag based identification and Sensor-based architecture both have different architecture and communication based protocol and it is not possible to have common architectural model for both of them. As when more and more things will be connected, more and more personal information will be spread.

The main thing that should be considered while developing architectures and standards is that they should be open and customer friendly so that customers can mix applications and services. While designing related to security, risks involved should be carefully evaluated and addressed. Although, decentralized model is accepted as best fit for security related issues but while considering the use cases centralized plays a significant role over there.

If we say that standards should be open that also involves certain risks along with that as there will more risk of data being shared and which leads to potential threats to privacy as more and more personal information will be revealed and there will be wide chances of hacking and theft activities which will lead to monetarily losses. As neutrality in IoT will not bring transparency in operations, it will bring transparency in transactions as well which will not bring happiness overall.

Standardization of IoT is the trending topic. Some committees such as ISO and IEC have joined together and formed JTC1 working group so as to develop an architectural model which take care of interoperability issues. Standard requirement is already fulfilled but their usage and application area is still needed to be addressed. To address this kind of situation ISO has formed an advisory group which will address certain kind of situations and will provide a solution to it.

Some of the issues which still need to be addressed include privacy, security, Trust and faith of customers and when data collection is overstated and one more thing if data collected by devices is unable to handle. Some of the industries are focusing more and more on interfaces but all we need is to avoid this bottleneck of interfaces and could come up with better solutions.

According to the experts, IoT is not only connected devices; IP addresses and Barcodes is also combination of upcoming technology. Consumers should be aware of the policies and procedures so that they should not fall in any trap. IPv6 should be deployed for the full development of IoT and to connect large number of devices. The need of hour is that all the main international standards should be collaborated so as to make the Internet of Things more safe and reliable platform.

References

[1] - http://www.rfidjournal.com/articles/view?4986

[2] - https://www.ge.com/digital/blog/everything-you-need-know-about-industrial-internet-things

[3] - http://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT

[4] - https://inductiveautomation.com/what-is-iIoT

[5] - Internet of things: Principles and Paradigms (BOOK)

[6] - https://www.eetimes.com/author.asp?doc_id=1326169

[7] - http://saphanatutorial.com/introduction-to-internet-of-things-part-1/

[8] - http://saphanatutorial.com/introduction-to-internet-of-things-part-2/

[9] - https://www.forbes.com/sites/louiscolumbus/2015/12/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2015/#777d82f84b93

[10] - https://www.prnewswire.com/news-releases/internet-of-things-market---global-industry-analysis-size-share-growth-trends-and-forecast-2015---2021-300243655.html

[11] - https://www.gemalto.com/brochures-site/download-site/Documents/tel-5G-networks-QandA.pdf

[12] - https://qz.com/179980/the-plans-for-5g-to-power-the-internet-of-things/

[13] - https://spectrum.ieee.org/tech-talk/computing/networks/5g-taking-stock

[14] - https://www.i-scoop.eu/internet-of-things-guide/5g-IoT/#The_future_of_5G_and_IoT_8211_and_the_future_impact_of_5G_beyond_IoT

[15] - https://www.networkworld.com/article/3230969/internet-of-things/3-ways-machine-learning-is-revolutionizing-IoT.html

[16] - https://www.leverege.com/blogpost/machine-learning-applications-in-IoT

[17] - https://www.pcmag.com/article2/0,2817,2372163,00.asp

[18] - https://www.forbes.com/sites/janakirammsv/2017/08/27/how-machine-learning-enhances-the-value-of-industrial-internet-of-things/#617120813f38

[19] - http://www.businessinsider.com/internet-of-things-cloud-computing-2016-10

[20] - https://www.simplilearn.com/how-big-data-powering-internet-of-things-IoT-revolution-article

[21] - http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

[22] - https://datafloq.com/read/securing-internet-of-things-IoT-with-blockchain/2228

[23] - https://hbr.org/2017/02/a-brief-history-of-blockchain

[24] - https://www.networkworld.com/article/3212765/internet-of-things/4-key-areas-where-blockchain-can-transform-IoT.html

[25] - https://techcrunch.com/2016/06/28/decentralizing-IoT-networks-through-blockchain/

[26] - https://www.forbes.com/sites/omribarzilay/2017/11/02/can-blockchain-and-ai-accelerate-the-arrival-of-the-IoT-economy/#277cda3240d8

[27] - https://www.codeproject.com/Articles/833251/What-is-IoT-and-Why-we-need-IoT

[28] - https://www.huffingtonpost.com/robert-armitano/IoT-provides-affordable-e_b_10055446.html

[29] - https://www.researchgate.net/publication/319791590_Internet_of_Things_for_Disaster_Management_State-of-the-Art_and_Prospects

[30] - http://www.electronicdesign.com/analog/3-ways-IoT-revolutionizes-farming

[31] - www.IoTi.com/industrial-IoT-iIoT/top-20-industrial-IoT-applications

[32] - https://www.energymanagertoday.com/energy-management-the-internet-of-things-changes-everything-0120273/

[33] - https://www.greenbiz.com/article/IoT-and-smart-city-trends-boost-smart-waste-collection-market

[34] - https://www.microsoft.com/en-ca/internet-of-things/healthcare

[35] - https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/IoT-in-shipping-industry.html

[36] - https://IoT.do/impact-IoT-transportation-2016-10

[37] - https://techbeacon.com/app-nirvana-when-internet-things-meets-api-economy

[38] - https://www.webopedia.com/TERM/B/beacon.html

[39] - https://passkit.com/buy-ibeacon/

[40] - https://dzone.com/articles/beacon-technology-everything-you-need-to-know-to-s-1

[41] - http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/IoT-report.pdf

[42] - https://www.ibm.com/blogs/internet-of-things/6-benefits-of-IoT-for-healthcare/

[43] - https://www.c2m.net/blog/10-benefits-of-a-smart-agriculture-solution.aspx

[44] - https://fathym.com/2017/05/5-powerful-benefits-IoT-manufacturing-industry/

[45] - https://www.kontron.com/resources/collateral/white_papers/IoT-transportation-kontron-blueprint.pdf

[46] - https://www.xcubelabs.com/our-blog/5-benefits-IoT-financial-services-2/

[47] - http://r-stylelab.com/company/blog/IoT/top-3-reasons-to-use-the-internet-of-things-in-education

[48] - https://www.rcrwireless.com/20161206/internet-of-things/sensor-IoT-tag31-tag99

[49] - https://www.linkedin.com/pulse/three-software-stacks-required-internet-things-IoT-ian-skerrett

[50] - https://www.networkworld.com/article/3196191/lan-wan/wifi-s-evolving-role-in-IoT.html

[51] - https://www.linkedin.com/pulse/what-bluetooth-low-energy-means-internet-things-premaratne

[52] - http://www.radio-electronics.com/info/wireless/zigbee/zigbee.php

[53] - http://internetofthingsagenda.techtarget.com/definition/ZigBee

[54] - https://learn.sparkfun.com/tutorials/connectivity-of-the-internet-of-things

[55] - http://www.mwrf.com/blog/whatever-happened-wimax

[56] - https://medium.com/IoTforall/so-you-want-to-use-lpwan-for-your-IoT-application-now-what-846cd9d14b30

[57] - https://www.ericsson.com/assets/local/publications/white-papers/wp_IoT.pdf

[58] - https://www.i-scoop.eu/internet-of-things-guide/lpwan/

[59] - http://internetofthingsagenda.techtarget.com/definition/LPWAN-low-power-wide-area-network

[60] - https://learn.sparkfun.com/tutorials/connectivity-of-the-internet-of-things

[61] - http://www.ti.com/lit/wp/swry010a/swry010a.pdf

[62] - file:///C:/Users/hp/Downloads/9783319331225-c2.pdf

[63]- https://www.link-labs.com/blog/IoT-and-security-mobile-world-congress-2017

[64] - https://medium.com/IoTforall/securing-your-connectivity-5304c192bea3

[65] - file:///C:/Users/hp/Downloads/7InternetofThingsFactsheetPrivacyandSecurity%20(1).pdf

[66] - https://www.citrix.com/blogs/2015/04/09/whats-required-to-secure-the-IoT/

[67] - https://www.imgtec.com/markets/internet-of-things/

[68] - https://cloud.google.com/solutions/IoT-overview

[69] - https://www.ibm.com/developerworks/library/IoT-lp101-best-hardware-devices-IoT-project/index.html

[70] - https://www.design-reuse.com/articles/32614/nvm-memory-IoT-applications.html

[71] - https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf

[72] - https://www.sitepoint.com/4-major-technical-challenges-facing-IoT-developers/

[73] - http://openmobilealliance.org/blog/the-top-3-challenges-IoT-developers-face

[74] - https://IoT.ieee.org/newsletter/march-2017/three-major-challenges-facing-IoT.html

[75] - http://www.rfidlicensing.com/

[76] - https://www.wi-fi.org/who-we-are\

[77] - http://www.zigbee.org/

[78] - https://aIoTi-space.org/wp-content/uploads/2017/06/AIoTI-WG3_sdos_alliances_landscape_-_IoT_lsp_standard_framework_concepts_-_release_2_v8.pdf

[79] - https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf

[80] - https://www.sciencedirect.com/science/article/pii/S2352864817301335

[81] - http://www.iec.ch/whitepaper/pdf/iecWP-loT2020-LR.pdf

[82] - http://enterprise-IoT.org/book/enterprise-IoT/part-ii-igniteIoT-methodology/igniteIoT-solution-delivery/building-blocks/IoT-architecture-blueprints/