MODULE 1

CHAPTER 1

Introduction to Internet of Things (IoT)

Syllabus

What is IoT? - IoT and Digitization. IoT Impact - Connected Roadways, Connected Factory, Smart Connected Buildings, Smart Creatures, Convergence of IT and OT, IoT Challenges, The oneM2M IoT Standardized Architecture, The IoT World Forum (IoTWF) Standardized Architecture, IoT Data Management and Compute Stack - Design considerations and Data related problems, Fog Computing, Edge Computing, The Hierarchy of Edge, Fog and Cloud.

1.1 IOT AND DIGITIZATION

What is IOT?

GQ. What is IOT Digitization ? **(4 Marks)**

- The **Internet of Things** (IoT) describes the network of physical objects "things" that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.
- *IoT* and *digitization* are terms that are often used interchangeably. In most contexts, this duality is fine, but there are key differences to be aware of.
- At a high level, IoT focuses on connecting "things," such as objects and machines, to a computer network, such as the Internet. IoT is a well-understood term used across the industry as a whole. On the other hand, digitization can mean different things to different people but generally encompasses the connection of "things" with the data they generate and the business insights that result.
- For example, in a shopping mall where Wi-Fi location tracking has been deployed, the "things" are the Wi-Fi devices. Wi-Fi location tracking is simply the capability of knowing where a consumer is in a retail environment through his or her smart phone's connection to the retailer's Wi-Fi network.
- While the value of connecting Wi-Fi devices or "things" to the Internet is obvious and appreciated by shoppers, tracking real-time location of Wi-Fi clients provides a specific business benefit to the mall and shop owners. In this case, it helps the business understand where shoppers tend to congregate and how much time they spend in different parts of a mall or store.
- Analysis of this data can lead to significant changes to the locations of product displays and advertising, where to place certain types of shops, how much rent to charge, and even where to station security guards.

Note

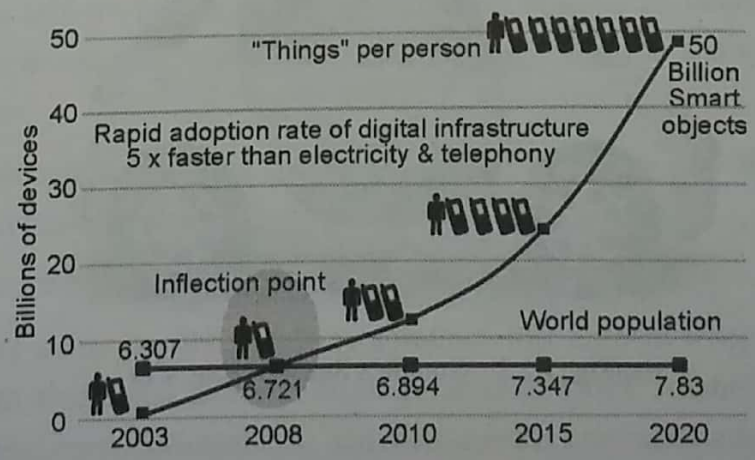
- For several years the term *Internet of Everything*, or *IoE*, was used extensively. Over time, the term IoE has been replaced by the term *digitization*.
- Although technical terms tend to evolve over time, the words *IoE* and *digitization* have roughly the same definition. IoT has always been a part of both, but it is important to note that IoT is a subset of both IoE and digitization.

- Digitization, as defined in its simplest form, is the conversion of information into a digital format. Digitization has been happening in one form or another for several decades.
- For example, the whole photography industry has been digitized. Pretty much everyone has digital cameras these days, either standalone devices or built into their mobile phones. Almost no one buys film and takes it to a retailer to get it developed. The digitization of photography has completely changed our experience when it comes to capturing images.
- In the context of IoT, digitization brings together things, data, and business process to make networked connections more relevant and valuable. A good example of this that many people can relate to is in the area of home automation with popular products, such as Nest.
- With Nest, sensors determine your desired climate settings and also tie in other smart objects, such as smoke alarms, video cameras, and various third-party devices.

1.2 IOT IMPACT

G.Q. Explain IOT Impact ? **(4 Marks)**

- Projections on the potential impact of IoT are impressive. About 14 billion, or just 0.06%, of "things" are connected to the Internet today. Cisco Systems predicts that by 2020, this number will reach 50 billion.
- A UK government report speculates that this number could be even higher, in the range of 100 billion objects connected. Cisco further estimates that these new connections will lead to $19 trillion in profits and cost savings.
- Fig. 1.2.1 provides a graphical look at the growth in the number of devices being connected.



(1A1) **Fig. 1.2.1 : The Rapid Growth in the Number of Devices Connected to the Internet**

- What these numbers mean is that IoT will fundamentally shift the way people and businesses interact with their surroundings. Managing and monitoring smart objects using real-time connectivity enables a whole new level of data-driven decision making. This in turn results in the optimization of systems and processes and delivers new services that save time for both people and businesses while improving the overall quality of life.

1.2.1 Connected Roadways

GQ. Write a short note on Connected Roadways.

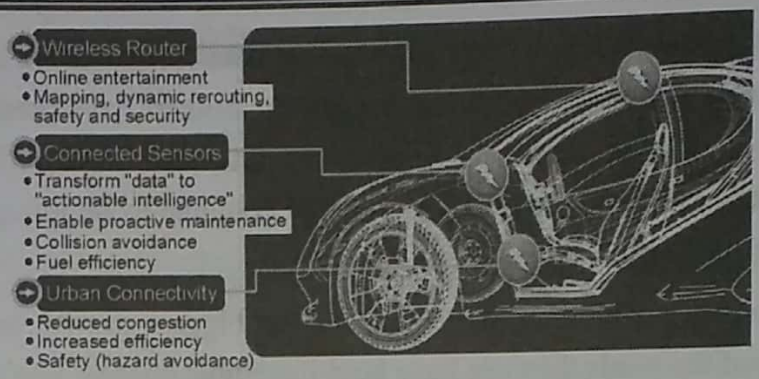
- People have been fantasizing about the self-driving car, or autonomous vehicle, in literature and film for decades. While this fantasy is now becoming a reality with well-known projects like Google's self-driving car, IoT is also a necessary component for implementing a fully connected transportation infrastructure.
- IoT is going to allow self-driving vehicles to better interact with the transportation system around them through bidirectional data exchanges while also providing important data to the riders.
- Self-driving vehicles need always-on, reliable communications and data from other transportation-related sensors to reach their full potential. Connected roadways is the term associated with both the driver and driverless cars fully integrating with the surrounding transportation infrastructure.
- Fig. 1.2.2 shows a self-driving car designed by Google.

(1A2)**Fig. 1.2.2 : Google's Self-Driving Car**

- Basic sensors reside in cars already. They monitor oil pressure, tire pressure, temperature, and other operating conditions, and provide data around the core car functions.
- From behind the steering wheel, the driver can access this data while also controlling the car using equipment such as a steering wheel, pedals, and so on. The need for all this sensory information and control is obvious.
- The driver must be able to understand, handle, and make critical decisions while concentrating on driving safely. The Internet of Things is replicating this concept on a much larger scale.
- Today, we are seeing automobiles produced with thousands of sensors, to measure everything from fuel consumption to location to the entertainment your family is watching during the ride.
- As automobile manufacturers strive to reinvent the driving experience, these sensors are becoming IP-enabled to allow easy communication with other systems both inside and outside the car.
- In addition, new sensors and communication technologies are being developed to allow vehicles to "talk" to other vehicles, traffic signals, school zones, and other elements of the transportation infrastructure. We are now starting to realize a truly connected transportation solution.
- Connected roadways will bring many benefits to society. These benefits include reduced traffic jams and urban congestion, decreased casualties and fatalities, increased response time for emergency vehicles, and reduced vehicle emissions.
- For example, with IoT-connected roadways, a concept known as Intersection Movement Assist (IMA) is possible. This application warns a driver (or triggers the appropriate response in a self-driving car) when it is not safe to enter an intersection due to a high probability of a collision perhaps because another car has run a stop sign or strayed into the wrong lane.
- Thanks to the communications system between the vehicles and the infrastructure, this sort of scenario can be handled quickly and safely.
- See Fig. 1.2.3 for a graphical representation of IMA.
- IMA is one of many possible roadway solutions that emerge when we start to integrate IoT with both traditional and self-driving vehicles. Other solutions include automated vehicle tracking, cargo management, and road weather communications.

(1A3)**Fig. 1.2.3 : Application of Intersection Movement Assist**

- With automated vehicle tracking, a vehicle's location is used for notification of arrival times, theft prevention, or highway assistance. Cargo management provides precise positioning of cargo as it is enroute so that notification alerts can be sent to a dispatcher and routes can be optimized for congestion and weather. Road weather communications use sensors and data from satellites, roads, and bridges to warn vehicles of dangerous conditions or inclement weather on the current route.
- Today's typical road car utilizes more than a million lines of code and this only scratches the surface of the data potential. As cars continue to become more connected and capable of generating continuous data streams related to location, performance, driver behavior, and much more, the data generation potential of a single car is staggering. It is estimated that a fully connected car will generate more than 25 gigabytes of data per hour, much of which will be sent to the cloud.
- To put this in perspective, that's equivalent to a dozen HD movies sent to the cloud every hour by your car! Multiply that by the number of hours a car is driven per year and again by the number of cars on the road, and you see that the amount of connected car data generated, transmitted, and stored in the cloud will be in the zettabytes range per year (more than a billion petabytes per year).
- Fig. 1.2.4 provides an overview of the sort of sensors and connectivity that you will find in a connected car.
- Another area where connected roadways are undergoing massive disruption is in how the data generated by a car will be used by third parties.
- Clearly, the data generated by your car needs to be handled in a secure and reliable way, which means the network needs to be secure, it must provide authentication and verification of the driver and car, and it needs to be highly available. But who will use all this data?



(1A4)**Fig. 1.2.4 : The Connected Car**

- Automobile data is extremely useful to a wide range of interested parties. For example, tire companies can collect data related to use and durability of their products in a range of environments in real time.
- Automobile manufacturers can collect information from sensors to better understand how the cars are being driven, when parts are starting to fail, or whether the car has broken down details that will help them build better cars in the future. This becomes especially true as autonomous vehicles are introduced, which are sure to be driven in a completely different way than the traditional family car.
- In the future, car sensors will be able to interact with third-party applications, such as GPS/maps, to enable dynamic rerouting to avoid traffic, accidents, and other hazards. Similarly, Internet-based entertainment, including music, movies, and other streaming or downloads, can be personalized and customized to optimize a road trip.
- This data will also be used for targeted advertising. As GPS navigation systems become more integrated with sensors and wayfinding applications, it will become possible for personalized routing suggestions to be made.
- For example, if it is known that you prefer a certain coffee shop, through the use of a cloud-based data connector, the navigation system will be able to provide routing suggestions that have you drive your car past the right coffee shop.
- All these data opportunities bring into play a new technology: the IoT data broker. Imagine the many different types of data generated by an automobile and the plethora of different parties interested in this data. This poses a significant business opportunity.
- In a very real sense, the data generated by the car and driver becomes a valuable commodity that can be bought and sold. While the data transmitted from the car will likely go to one initial location in the cloud, from there the data can be separated and sold selectively by the data broker.

- For example, tire companies will pay for information from sensors related to your tires, but they won't get anything else. While information brokers have been around a long time, the technology used to aggregate and separate the data from connected cars in a secure and governed manner is rapidly developing and will continue to be a major focus of the IoT industry for years to come.
- Connected roadways are likely to be one of the biggest growth areas for innovation. Automobiles and the roads they use have seen incredible change over the past century, but the changes ahead of us are going to be just as astonishing.
- In the past few years alone, we have seen highway systems around the world adopt sophisticated sensors systems that can detect seismic vibrations, car accidents, severe weather conditions, traffic congestion, and more.
- Recent advancements in roadway fiber-optic sensing technology is now able to record not only how many cars are passing but their speed and type. Due to the many reasons already discussed, connected cars and roadways are early adopters of IoT technology.
- For a more in-depth discussion of IoT use cases and architectures in the transportation industry, "Transportation."

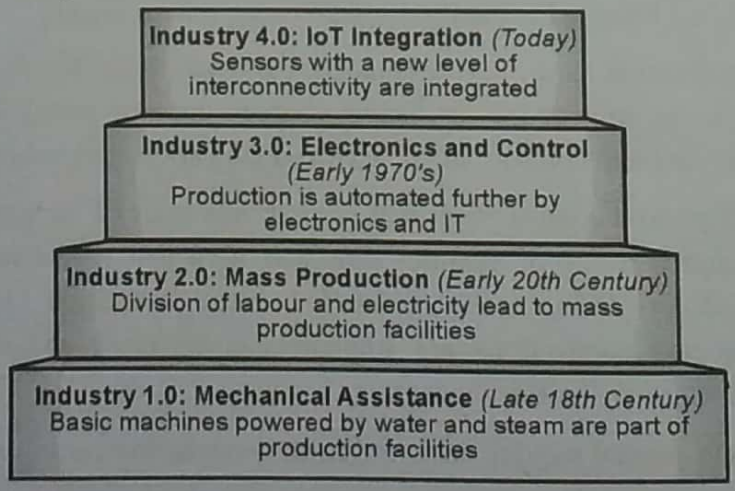
1.2.2 Connected Factory

GQ. Write short note on Connected factory ? **(2 Marks)**

- For years, traditional factories have been operating at a disadvantage, impeded by production environments that are "disconnected" or, at the very least, "strictly gated" to corporate business systems, supply chains, and customers and partners. Managers of these traditional factories are essentially "flying blind" and lack visibility into their operations. These operations are composed of plant floors, front offices, and suppliers operating in independent silos. Consequently, rectifying downtime issues, quality problems, and the root causes of various manufacturing inefficiencies is often difficult.
- The main challenges facing manufacturing in a factory environment today include the following :
  - Image Accelerating new product and service introductions to meet customer and market opportunities.
  - Image Increasing plant production, quality, and uptime while decreasing cost.
- Adding another level of complication to these challenges is the fact that they often need to be addressed at various levels of the manufacturing business.

- For example, executive management is looking for new ways to manufacture in a more cost-effective manner while balancing the rising energy and material costs. Product development has time to market as the top priority. Plant managers are entirely focused on gains in plant efficiency and operational agility. The controls and automation department looks after the plant networks, controls, and applications and therefore requires complete visibility into all these systems.
- Industrial enterprises around the world are retooling their factories with advanced technologies and architectures to resolve these problems and boost manufacturing flexibility and speed. These improvements help them achieve new levels of overall equipment effectiveness, supply chain responsiveness, and customer satisfaction.
- A convergence of factory-based operational technologies and architectures with global IT networks is starting to occur, and this is referred to as the connected factory.
- As with the IoT solutions for the connected roadways previously discussed, there are already large numbers of basic sensors on factory floors.
- However, with IoT, these sensors not only become more advanced but also attain a new level of connectivity. They are smarter and gain the ability to communicate, mainly using the Internet Protocol (IP) over an Ethernet infrastructure.
- In addition to sensors, the devices on the plant floor are becoming smarter in their ability to transmit and receive large quantities of real-time informational and diagnostic data. Ethernet connectivity is becoming pervasive and spreading beyond just the main controllers in a factory to devices such as the robots on the plant floor. In addition, more IP-enabled devices, including video cameras, diagnostic smart objects, and even personal mobile devices, are being added to the manufacturing environment.
- For example, a smelting facility extracts metals from their ores. The facility uses both heat and chemicals to decompose the ore, leaving behind the base metal. This is a multistage process, and the data and controls are all accessed via various control rooms in a facility.
- Operators must go to a control room that is often hundreds of meters away for data and production changes. Hours of operator time are often lost to the multiple trips to the control room needed during a shift. With IoT and a connected factory solution, true "machine-to-people" connections are implemented to bring sensor data directly to operators on the floor via mobile devices.
- Time is no longer wasted moving back and forth between the control rooms and the plant floor. In addition, because the operators now receive data in real time, decisions can be made immediately to improve production and fix any quality problems.

- Another example of a connected factory solution involves a real-time location system (RTLS). An RTLS utilizes small and easily deployed Wi-Fi RFID tags that attach to virtually any material and provide real-time location and status.
- These tags enable a facility to track production as it happens. These IoT sensors allow components and materials on an assembly line to "talk" to the network. If each assembly line's output is tracked in real time, decisions can be made to speed up or slow production to meet targets, and it is easy to determine how quickly employees are completing the various stages of production. Bottlenecks at any point in production and quality problems are also quickly identified.
- While we tend to look at IoT as an evolution of the Internet, it is also sparking an evolution of industry. In 2016 the World Economic Forum referred to the evolution of the Internet and the impact of IoT as the "fourth Industrial Revolution."
  - The first Industrial Revolution occurred in Europe in the late eighteenth century, with the application of steam and water to mechanical production.
  - The second Industrial Revolution, which took place between the early 1870s and the early twentieth century, saw the introduction of the electrical grid and mass production.
  - The third revolution came in the late 1960s/early 1970s, as computers and electronics began to make their mark on manufacturing and other industrial systems.
  - The fourth Industrial Revolution is happening now, and the Internet of Things is driving it. Fig. 1.2.5 summarizes these four Industrial Revolutions as Industry 1.0 through Industry 4.0.



(1A5)**Fig. 1.2.5 : The Four Industrial Revolutions**

- The IoT wave of Industry 4.0 takes manufacturing from a purely automated assembly line model of production to a model where the machines are intelligent and communicate with one another.
- IoT in manufacturing brings with it the opportunity for inserting intelligence into factories. This starts with creating smart objects, which involves embedding sensors, actuators, and controllers into just about everything related to production. Connections tie it all together so that people and machines work together to analyze the data and make intelligent decisions. Eventually this leads to machines predicting failures and self-healing and points to a world where human monitoring and intervention are no longer necessary.

1.2.3 Smart Connected Buildings

- Another place IoT is making a disruptive impact is in the smart connected buildings space. In the past several decades, buildings have become increasingly complex, with systems overlaid one upon another, resulting in complex intersections of structural, mechanical, electrical, and IT components. Over time, these operational networks that support the building environment have matured into sophisticated systems; however, for the most part, they are deployed and managed as separate systems that have little to no interaction with each other.
- The function of a building is to provide a work environment that keeps the workers comfortable, efficient, and safe. Work areas need to be well lit and kept at a comfortable temperature. To keep workers safe, the fire alarm and suppression system needs to be carefully managed, as do the door and physical security alarm systems.
- While intelligent systems for modern buildings are being deployed and improved for each of these functions, most of these systems currently run independently of each other and they rarely take into account where the occupants of the building actually are and how many of them are present in different parts of the building.
- However, many buildings are beginning to deploy sensors throughout the building to detect occupancy. These tend to be motion sensors or sensors tied to video cameras. Motion detection occupancy sensors work great if everyone is moving around in a crowded room and can automatically shut the lights off when everyone has left, but what if a person in the room is out of sight of the sensor? It is a frustrating matter to be at the mercy of an unintelligent sensor on the wall that wants to turn off the lights on you.
- Similarly, sensors are often used to control the heating, ventilation, and air-conditioning (HVAC) system.

- Temperature sensors are spread throughout the building and are used to influence the building management system's (BMS's) control of air flow into a room.
- Another interesting aspect of the smart building is that it makes them easier and cheaper to manage. Considering the massive costs involved in operating such complex structures, not to mention how many people spend their working lives inside a building, managers have become increasingly interested in ways to make buildings more efficient and cheaper to manage.
- Have you ever heard people complain that they had too little working space in their office, or that the office space wasn't being used efficiently? When people go to their managers and ask for a change to the floor plan, such as asking for an increase in the amount of space they work in, they are often asked to prove their case. But workplace floor efficiency and usage evidence tends to be anecdotal at best.
- When smart building sensors and occupancy detection are combined with the power of data analytics it becomes easy to demonstrate floor plan usage and prove your case.
- Alternatively, the building manager can use a similar approach to see where the floor is not being used efficiently and use this information to optimize the available space. This has brought about the age of building automation, empowered by IoT.
- While many technical solutions exist for looking after building systems, until recently they have all required separate overlay networks, each responsible for its assigned task. In an attempt to connect these systems into a single framework, the Building Automation System (BAS) has been developed to provide a single management system for the HVAC, lighting, fire alarm, and detection systems, as well as access control.
- All these systems may support different types of sensors and connections to the BAS. How do you connect them together so the building can be managed in a coherent way? This highlights one of the biggest challenges in IoT, which is discussed throughout this book : the heterogeneity of IoT systems.
- Before you can bring together heterogeneous systems, they need to converge at the network layer and support a common services layer that allows application integration. The value of converged networks is well documented.
- For example, in the early 2000s, Cisco and several other companies championed the convergence of voice and video onto single IP networks that were shared with other IT applications.

- The economies of scale and operational efficiencies gained were so massive that VoIP and collaboration technologies are now the norm. However, the convergence to IP and a common services framework for buildings has been slower.
- For example, the de facto communication protocol responsible for building automation is known as BACnet (Building Automation and Control Network). In a nutshell, the BACnet protocol defines a set of services that allow Ethernet-based communication between building devices such as HVAC, lighting, access control, and fire detection systems. The same building Ethernet switches used for IT may also be used for BACnet. This standardization also makes possible an intersection point to the IP network (which is run by the IT department) through the use of a gateway device. In addition, BACnet/IP has been defined to allow the "things" in the building network to communicate over IP, thus allowing closer consolidation of the building management system on a single network.

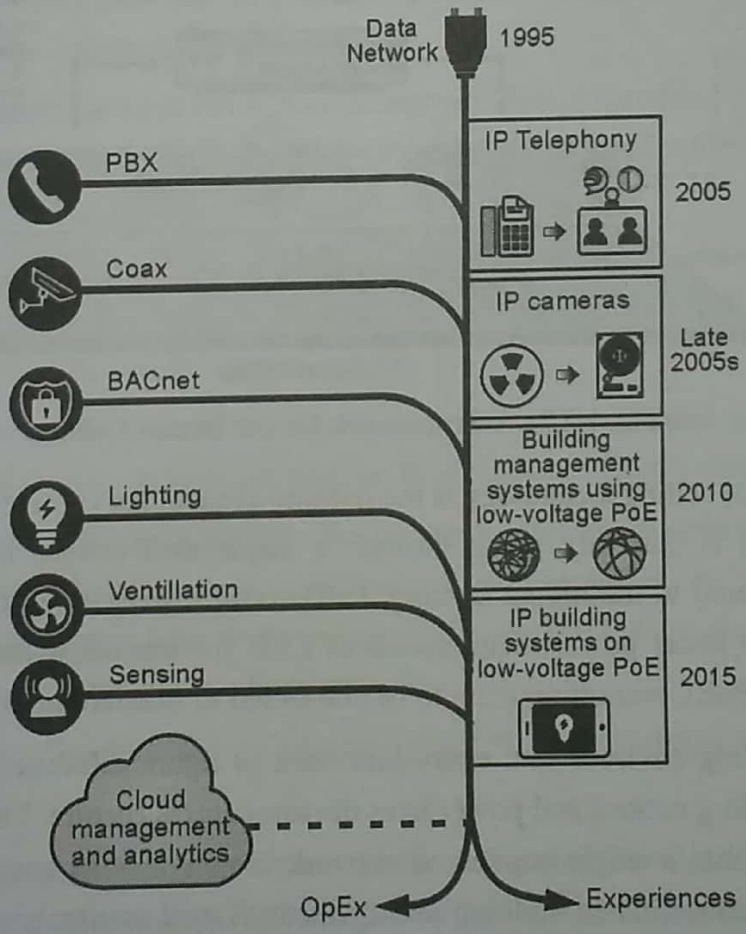
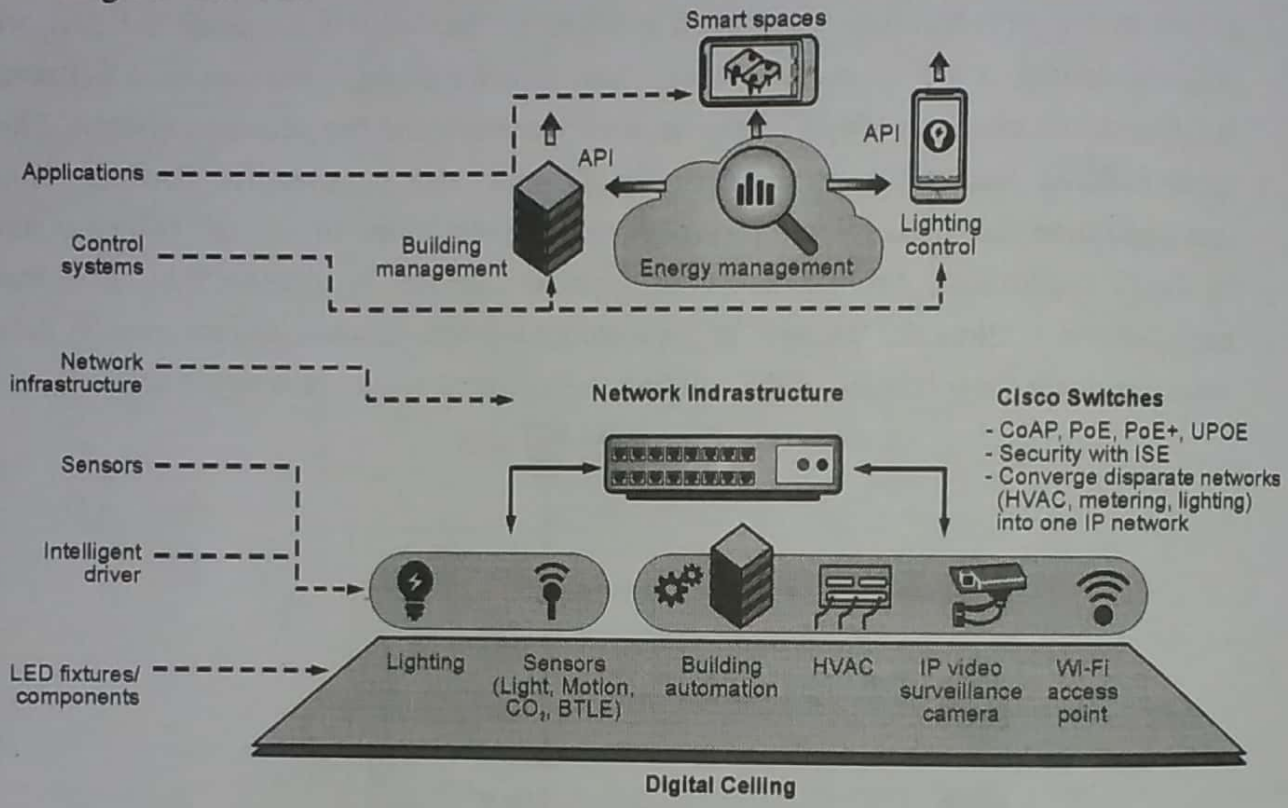


Fig. 1.2.6 illustrates the conversion of building protocols to IP over time.

- Another promising IoT technology in the smart connected building, and one that is seeing widespread adoption, is the "digital ceiling."

- The digital ceiling is more than just a lighting control system. This technology encompasses several of the building's different networks including lighting, HVAC, blinds, CCTV (closed-circuit television), and security systems and combines them into a single IP network.



(1A7)**Fig. 1.2.7 : A Framework for the Digital Ceiling**

- Central to digital ceiling technology is the lighting system. As you are probably aware, the lighting market is currently going through a major shift toward light-emitting diodes (LEDs). Compared to traditional lighting, LEDs offer lower energy consumption and far longer life. The lower power requirements of LED fixtures allow them to run on Power over Ethernet (PoE), permitting them to be connected to standard network switches.
- In a digital ceiling environment, every luminaire or lighting fixture is directly network-attached, providing control and power over the same infrastructure. This transition to LED lighting means that a single converged network is now able to encompasses luminaires that are part of consolidated building management as well as elements managed by the IT network, supporting voice, video, and other data applications.
- The next time you look at the ceiling in your office building, count the number of lights. The quantity of lights easily outnumbers the number of physical wired ports by a hefty margin.

- Obviously, supporting the larger number of Ethernet ports and density of IP addresses requires some redesign of the network, and it also requires a quiet, fanless PoE-capable switch in the ceiling. That being said, the long-term business case supporting reduced energy costs from LED luminaries versus traditional fluorescent or halogen lights is so significant that the added initial investment in the network is almost inconsequential.
- The business case for the digital ceiling becomes even stronger when a building is being renovated or a new structure is being built. In these cases, the cost benefit of running CAT 6/5e cables in the ceiling versus plenum-rated electrical wiring to every light is substantial.
- The energy savings value of PoE-enabled LED lighting in the ceiling is clear. However, having an IP-enabled sensor device in the ceiling at every point people may be present opens up an entirely new set of possibilities. For example, most modern LED ceiling fixtures support occupancy sensors.
- These sensors provide high-resolution occupancy data collection, which can be used to turn the lights on and off, and this same data can be combined with advanced analytics to control other systems, such as HVAC and security.
- Unlike traditional sensors that use rudimentary motion detection, modern lighting sensors integrate a variety of occupancy-sensing technologies, including Bluetooth low energy (BLE) and Wi-Fi. The science here is simple.
- Because almost every person these days carries a smart device that supports BLE and Wi-Fi, all the sensor has to do is detect BLE or Wi-Fi beacons from a nearby device.
- When someone walks near a light, the person's location is detected, and the wireless system can send information to control the air flow from the HVAC system into that zone in real time, maximizing the comfort of the office worker. Figure shows an example of an occupancy sensor in a digital ceiling light.
- You can begin to imagine the possibilities that IoT smart lighting brings to a workplace setting.
- Not only does it provide for optimized levels of lighting based on actual occupancy and building usage, it allows granular control of temperature, management of smoke and fire detection, video cameras, and building access control.
- IoT allows all this to run through a single network, requiring less installation time and a lower total cost of system ownership.

1.2.4 Smart Creatures

- When you think about IoT, you probably picture only inanimate objects and machines being connected. However, IoT also provides the ability to connect living things to the Internet. Sensors can be placed on animals and even insects just as easily as on machines, and the benefits can be just as impressive.
- One of the most well-known applications of IoT with respect to animals focuses on what is often referred to as the "connected cow." Sparked, a Dutch company, developed a sensor that is placed in a cow's ear. The sensor monitors various health aspects of the cow as well as its location and transmits the data wirelessly for analysis by the farmer.
- The data from each of these sensors is approximately 200 MB per year, and you obviously need a network infrastructure to make the connection with the sensors and store the information.
- Once the data is being collected, however, you get a complete view of the herd, with statistics on every cow. You can learn how environmental factors may be affecting the herd as a whole and about changes in diet. This enables early detection of disease as cows tend to eat less days before they show symptoms. These sensors even allow the detection of pregnancy in cows.
- Another application of IoT to organisms involves the placement of sensors on roaches. While the topic of roaches is a little unsettling to many folks, the potential benefits of IoT-enabled roaches could make a life-saving difference in disaster situations.
- Researchers at North Carolina State University are working with Madagascar hissing cockroaches in the hopes of helping emergency personnel rescue survivors after a disaster.

(1A8)**Fig. 1.2.8 : IoT-Enabled Roach Can Assist in Finding Survivors After a Disaster (Photo courtesy of Alper Bozkurt, NC State University)**

- As shown in Fig. 1.2.8, an electronic backpack attaches to a roach. This backpack communicates with the roach through parts of its body.
- Low-level electrical pulses to an antenna on one side makes the roach turn to the opposite side because it believes it is encountering an obstacle. The cerci of the roach are sensory organs on the abdomen that detect danger through changing air currents. When the backpack stimulates the cerci, the roach moves forward because it thinks a predator is approaching.
- The electronic backpack uses wireless communication to a controller and can be "driven" remotely. Imagine a fleet of these roaches being used in a disaster scenario, such as searching for survivors in a collapsed building after an earthquake. The roaches are naturally designed to efficiently move around objects in confined spaces. Technology has also been tested to keep the roaches in the disaster area; it is similar to the invisible fencing that is often used to keep dogs in a yard. The use of roaches in this manner allows for the mapping of spaces that rescue personnel cannot access, which helps search for survivors.
- To help with finding a person trapped in the rubble of a collapsed building, the electronic backpack is equipped with directional microphones that allow for the detection of certain sounds and the direction from which they are coming.
- Software can analyze the sounds to ensure that they are from a person rather than from, say, a leaking pipe. Roaches can then be steered toward the sounds that may indicate people who are trapped. In addition, the microphones provide the ability for rescue personnel to listen in on whatever sounds are detected.
- These examples show that IoT often goes beyond just adding sensors and more intelligence to nonliving "things." Living "things" can also be connected to the Internet and this connection can provide important results.

1.3 CONVERGENCE OF IT AND OT

GQ. Explain Converence of IT and OT. **(4 Marks)**

- Until recently, Information Technology (IT) and Operational Technology (OT) have for the most part lived in separate worlds. IT supports connections to the Internet along with related data and technology systems and is focused on the secure flow of data across an organization.

- OT monitors and controls devices and processes on physical operational systems. These systems include assembly lines, utility distribution networks, production facilities, roadway systems, and many more. Typically, IT did not get involved with the production and logistics of OT environments.
- Specifically, the IT organization is responsible for the information systems of a business, such as email, file and print services, databases, and so on.
- In comparison, OT is responsible for the devices and processes acting on industrial equipment, such as factory machines, meters, actuators, electrical distribution automation devices, SCADA (supervisory control and data acquisition) systems, and so on.
- Traditionally, OT has used dedicated networks with specialized communications protocols to connect these devices, and these networks have run completely separately from the IT networks.
- Management of OT is tied to the lifeblood of a company. For example, if the network connecting the machines in a factory fails, the machines cannot function, and production may come to a standstill, negatively impacting business on the order of millions of dollars. On the other hand, if the email server (run by the IT department) fails for a few hours, it may irritate people, but it is unlikely to impact business at anywhere near the same level.
- Table 1.3.1 highlights some of the differences between IT and OT networks and their various challenges.

Table 1.3.1 : Comparing Operational Technology (OT) and Information Technology (IT)

Criterion	Industrial OT Network	Enterprise IT Network
Operational focus	Keep the business operating 24 × 7	Manage the computers, data, and employee communication system in a secure way
Priorities	1. Availability	1. Security
	2.. Integrity	2. Integrity
	3. Security	3. Availability
Types of data	Monitoring, control, and supervisory data	Voice, video, transactional, and bulk data
Security	Controlled physical access to devices	Devices and users authenticated to the network

Criterion	Industrial OT Network	Enterprise IT Network
Implication of failure	OT network disruption directly impacts business	Can be business impacting, depending on industry, but workarounds may be possible
Network upgrades (software or hardware)	Only during operational maintenance windows	Often requires an outage window when workers are notonsitc; impact can be mitigated
Security vulnerability	Low: OT networks are isolated and often use proprietary protocols	High: continual patching of hosts is required, and the network is connected to Internet and requires vigilant protection

- With the rise of IoT and standards-based protocols, such as IPv6, the IT and OT worlds are converging or, more accurately, OT is beginning to adopt the network protocols, technology, transport, and methods of the IT organization, and the IT organization is beginning to support the operational requirements used by OT.
- When IT and OT begin using the same networks, protocols, and processes, there are clear economies of scale. Not only does convergence reduce the amount of capital infrastructure needed but networks become easier to operate, and the flexibility of open standards allows faster growth and adaptability to new technologies.
- However, as you can see from Table 1.3.1, the convergence of IT and OT to a single consolidated network poses several challenges. There are fundamental cultural and priority differences between these two organizations. IoT is forcing these groups to work together, when in the past they have operated rather autonomously.
- For example, the OT organization is baffled when IT schedules a weekend shutdown to update software without regard to production requirements. On the other hand, the IT group does not understand the prevalence of proprietary or specialized systems and solutions deployed by OT.
- Take the case of deploying quality of service (QoS) in a network. When the IT team deploys QoS, voice and video traffic are almost universally treated with the highest level of service.
- However, when the OT system shares the same network, a very strong argument can be made that the real-time OT traffic should be given a higher priority than even voice because any disruption in the OT network could impact the business.

- With the merging of OT and IT, improvements are being made to both systems. OT is looking more toward IT technologies with open standards, such as Ethernet and IP. At the same time, IT is becoming more of a business partner with OT by better understanding business outcomes and operational requirements.
- The overall benefit of IT and OT working together is a more efficient and profitable business due to reduced downtime, lower costs through economy of scale, reduced inventory, and improved delivery times. When IT/OT convergence is managed correctly, IoT becomes fully supported by both groups. This provides a "best of both worlds" scenario, where solid industrial control systems reside on an open, integrated, and secure technology foundation.6

☞ IoT Challenges

GQ. Explain different IOT challenges. **(4 Marks)**

- While an IoT-enabled future paints an impressive picture, it does not come without significant challenges.
- Many parts of IoT have become reality, but certain obstacles need to be overcome for IoT to become ubiquitous throughout industry and our everyday life.
- Table 1.3.2 highlights a few of the most significant challenges and problems that IoT is currently facing.

Table 1.3.2 : IoT Challenges

Privacy	As sensors become more prolific in our everyday lives, much of the data they gather will be specific to individuals and their activities. This data can range from health information to shopping patterns and transactions at a retail establishment. For businesses, this data has monetary value. Organizations are now discussing who owns this data and how individuals can control whether it is shared and with whom.
Big data and data analytics	IoT and its large number of sensors is going to trigger a deluge of data that must be handled, This data will provide critical information and insights if it can be processed in an efficient manner. The challenge, however, is evaluating massive amounts of data arriving from different sources in various forms and doing so in a timely mariner.

Interoperability	As with any other nascent technology, various protocols and architectures are jockeying for market share and standardization within IoT. Some of these protocols and architectures are based on proprietary elements, and others are open. Recent IoT standards arc helping minimize this problem, but there are often various protocols and implementations available for la networks. The prominent protocols and architectures especially open, standards-based implementations are the subject of this book.

☞ Summary

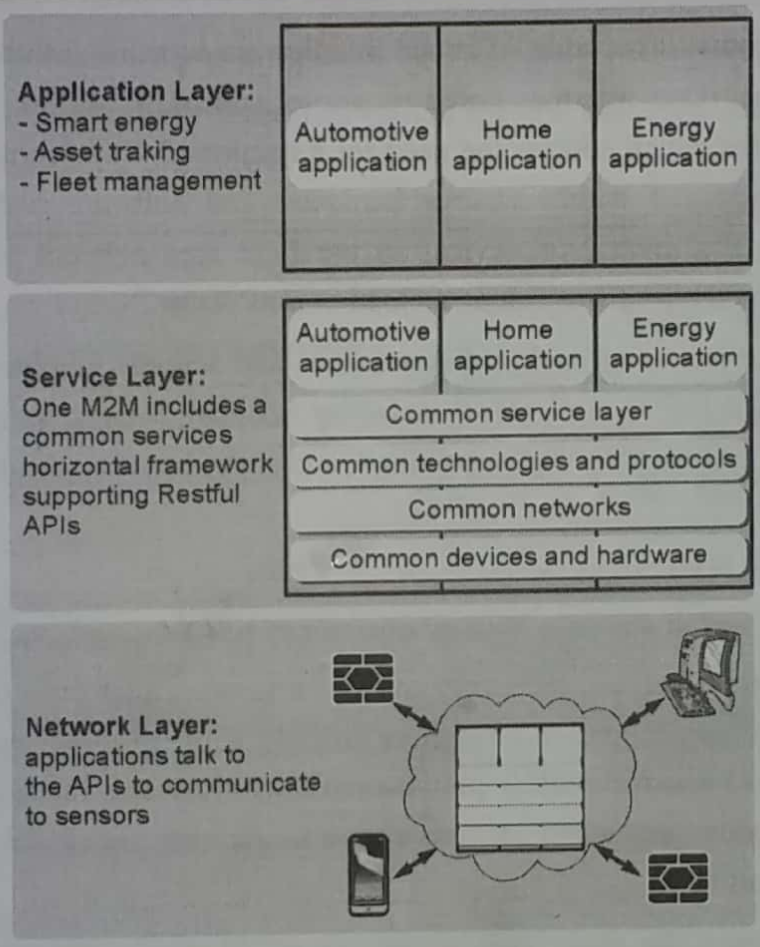
- This chapter provides an introductory look at the Internet of Things and answers the question "What is IoT?" IoT is about connecting the unconnected, enabling smart objects to communicate with other objects, systems, and people.
- The end result is an intelligent network that allows more control of the physical world and the enablement of advanced applications.
- This chapter also provides a historical look at IoT, along with a current view of IoT as the next evolutionary phase of the Internet. This chapter details a few high-level use cases to show the impact of IoT and some of the ways it will be changing our world.
- A number of IoT concepts and terms are defined throughout this chapter.
- The differences between IoT and digitization are discussed, as well as the convergence between IT and OT. The last section details the challenges faced by IoT.

⏭ 1.4 THE ONEM2M IOT STANDARDIZED ARCHITECTURE

GQ. Explain M2M IOT standardization Architecture. **(4 Marks)**

- In an effort to standardize the rapidly growing field of machine-to-machine (M2M) communications, the European Telecommunications Standards Institute (ETSI) created the M2M Technical Committee in 2008.

- The goal of this committee was to create a common architecture that would help accelerate the adoption of M2M applications and devices. Over time, the scope has expanded to include the Internet of Things.
- Other related bodies also began to create similar M2M architectures, and a common standard for M2M became necessary.
- Recognizing this need, in 2012 ETSI and 13 other founding members launched oneM2M as a global initiative designed to promote efficient M2M communication systems and IoT.
- The goal of oneM2M is to create a common services layer, which can be readily embedded in field devices to allow communication with application servers.1 oneM2M's framework focuses on IoT services, applications, and platforms.
- These include smart metering applications, smart grid, smart city automation, e-health, and connected vehicles.
- One of the greatest challenges in designing an IoT architecture is dealing with the heterogeneity of devices, software, and access methods. By developing a horizontal platform architecture, oneM2M is developing standards that allow interoperability at all levels of the IoT stack.
- For example, you might want to automate your HVAC system by connecting it with wireless temperature sensors spread throughout your office. You decide to deploy sensors that use LoRaWAN technology (discussed in Chapter 4, "Connecting Smart Objects").
- The problem is that the LoRaWAN network and the BACnet system that your HVAC and BMS run on are completely different systems and have no natural connection point. This is where the oneM2M common services architecture comes in. oneM2M's horizontal framework and RESTful APIs allow the LoRaWAN system to interface with the building management system over an IoT network, thus promoting end-to-end IoT communications in a consistent way, no matter how heterogeneous the networks.
- Fig. 1.4.1 illustrates the oneM2M IoT architecture.
- The oneM2M architecture divides IoT functions into three major domains: the application layer, the services layer, and the network layer.
- While this architecture may seem simple and somewhat generic at first glance, it is very rich and promotes interoperability through IT-friendly APIs and supports a wide range of IoT technologies.



(1A9)**Fig. 1.4.1 : The Main Elements of the oneM2M IoT Architecture**

Let's examine each of these domains in turn

(1) Image Applications layer

- The oneM2M architecture gives major attention to connectivity between devices and their applications.
- This domain includes the application-layer protocols and attempts to standardize northbound API definitions for interaction with business intelligence (BI) systems.
- Applications tend to be industry-specific and have their own sets of data models, and thus they are shown as vertical entities.

(2) Image Services layer

- This layer is shown as a horizontal framework across the vertical industry applications. At this layer, horizontal modules include the physical network that the IoT applications run on, the underlying management protocols, and the hardware. Examples include backhaul communications via cellular, MPLS networks, VPNs, and so on. Riding on top is the common services layer.

- This conceptual layer adds APIs and middleware supporting third-party services and applications. One of the stated goals of oneM2M is to "develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software nodes, and rely upon connecting the myriad of devices in the field area network to M2M application servers, which typically reside in a cloud or data center."
- A critical objective of oneM2M is to attract and actively involve organizations from M2M-related business domains, including telematics and intelligent transportation, healthcare, utility, industrial automation, and smart home applications, to name just a few.

(3) Image Network layer

- This is the communication domain for the IoT devices and endpoints. It includes the devices themselves and the communications network that links them. Embodiments of this communications infrastructure include wireless mesh technologies, such as IEEE 802.15.4, and wireless point-to-multipoint systems, such as IEEE 801.11ah. Also included are wired device connections, such as IEEE 1901 power line communications
- In many cases, the smart (and sometimes not-so-smart) devices communicate with each other. In other cases, machine-to-machine communication is not necessary, and the devices simply communicate through a field area network (FAN) to use-case-specific apps in the IoT application domain. Therefore, the device domain also includes the gateway device, which provides communications up into the core network and acts as a demarcation point between the device and network domains.
- Technical Specifications and Technical Reports published by oneM2M covering IoT functional architecture and other aspects can be found at www.onem2m.org.

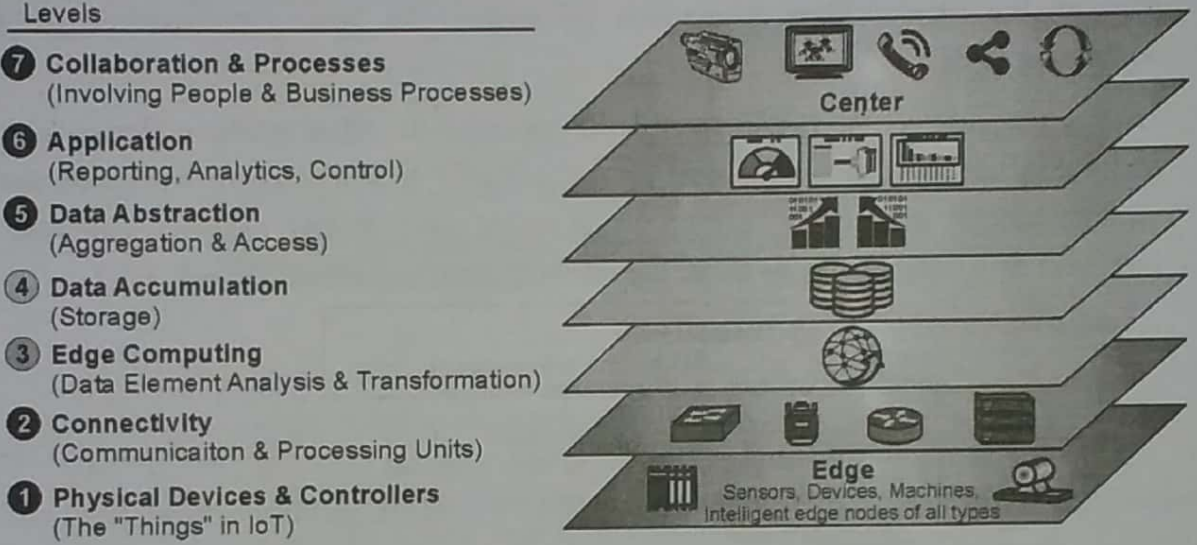
1.5 THE IOT WORLD FORUM (IOTWF) STANDARDIZED ARCHITECTURE

GQ. Explain IoTWF architecture in details. **(4 Marks)**

- In 2014 the IoTWF architectural committee (led by Cisco, IBM, Rockwell Automation, and others) published a seven-layer IoT architectural reference model.
- While various IoT reference models exist, the one put forth by the IoT World Forum offers a clean, simplified perspective on IoT and includes edge computing, data storage,

and access. It provides a succinct way of visualizing IoT from a technical perspective. Each of the seven layers is broken down into specific functions, and security encompasses the entire model.

- Fig. 1.5.1 details the IoT Reference Model published by the IoTWF.



(1A10)**Fig. 1.5.1 : IoT Reference Model Published by the IoT World Forum**

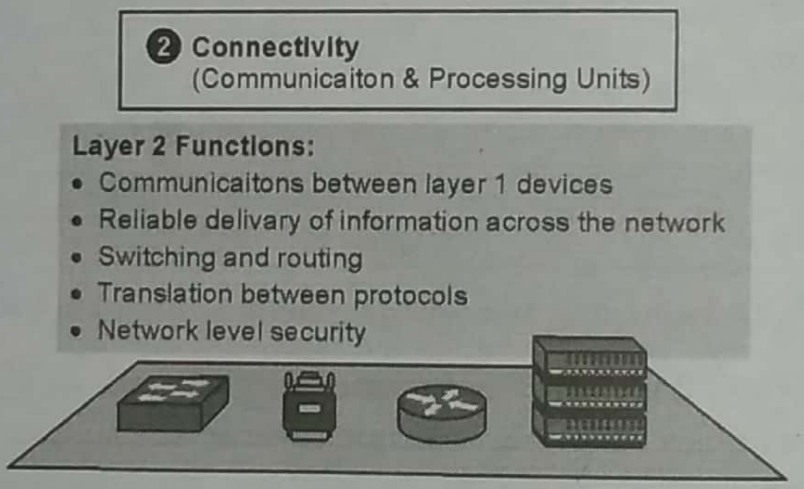
- As shown in Fig. 1.5.1, the IoT Reference Model defines a set of levels with control flowing from the center (this could be either a cloud service or a dedicated data center), to the edge, which includes sensors, devices, machines, and other types of intelligent end nodes.
- In general, data travels up the stack, originating from the edge, and goes northbound to the center. Using this reference model, we are able to achieve the following:
- The following sections look more closely at each of the seven layers of the IoT Reference Model.

Layer 1 : Physical Devices and Controllers Layer

- The first layer of the IoT Reference Model is the physical devices and controllers layer. This layer is home to the "things" in the Internet of Things, including the various endpoint devices and sensors that send and receive information.
- The size of these "things" can range from almost microscopic sensors to giant machines in a factory. Their primary function is generating data and being capable of being queried and/or controlled over a network.

Layer 2 : Connectivity Layer

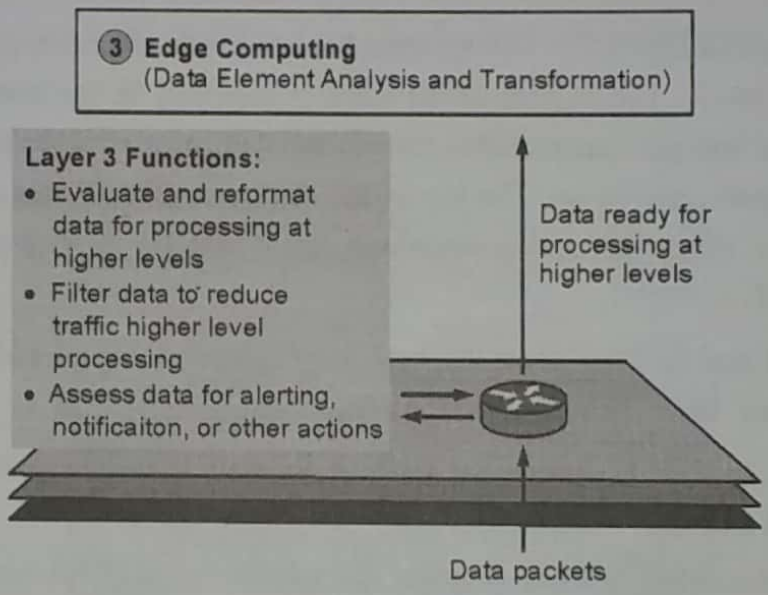
- In the second layer of the IoT Reference Model, the focus is on connectivity. The most important function of this IoT layer is the reliable and timely transmission of data. More specifically, this includes transmissions between Layer 1 devices and the network and between the network and information processing that occurs at Layer 3 (the edge computing layer).
- As you may notice, the connectivity layer encompasses all networking elements of IoT and doesn't really distinguish between the last-mile network (the network between the sensor/endpoint and the IoT gateway, discussed later in this chapter), gateway, and backhaul networks. Functions of the connectivity layer are detailed in Fig. 1.5.2.



(1A11)**Fig. 1.5.2 : IoT Reference Model Connectivity Layer Functions**

Layer 3 : Edge Computing Layer

- Edge computing is the role of Layer 3. Edge computing is often referred to as the "fog" layer and is discussed in the section "Fog Computing," later in this chapter.
- At this layer, the emphasis is on data reduction and converting network data flows into information that is ready for storage and processing by higher layers. One of the basic principles of this reference model is that information processing is initiated as early and as close to the edge of the network as possible.
- Fig. 1.5.3 highlights the functions handled by Layer 3 of the IoT Reference Model.
- Another important function that occurs at Layer 3 is the evaluation of data to see if it can be filtered or aggregated before being sent to a higher layer. This also allows for data to be reformatted or decoded, making additional processing by other systems easier. Thus, a critical function is assessing the data to see if predefined thresholds are crossed and any action or alerts need to be sent.



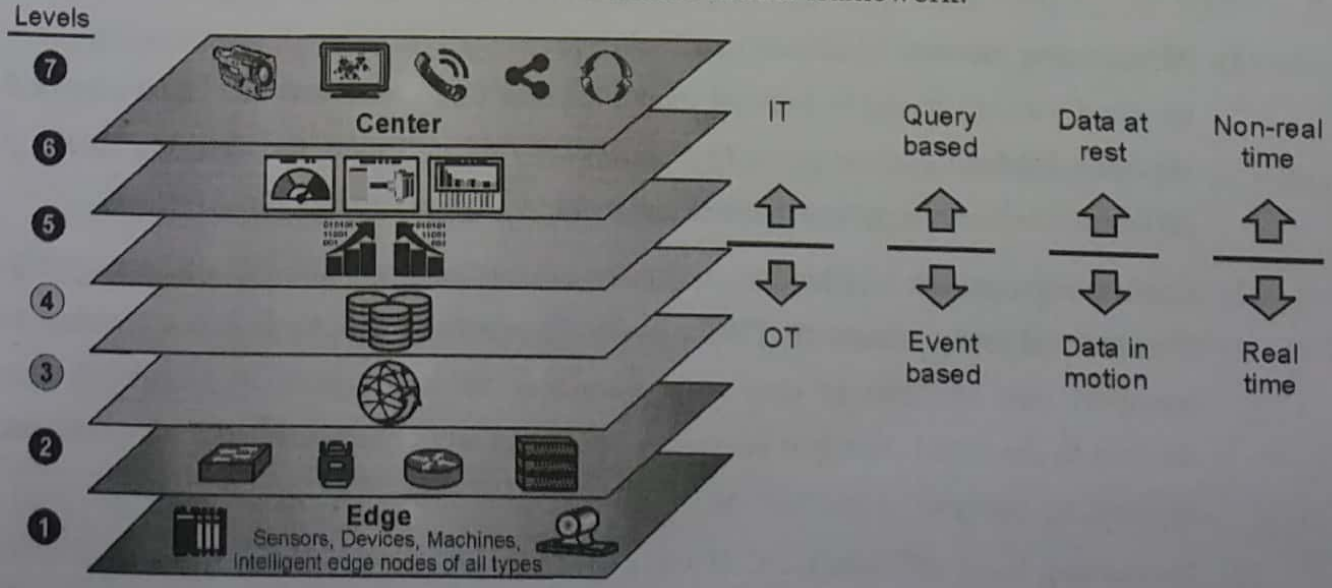
(1A12)**Fig. 1.5.3 : IoT Reference Model Layer 3 Functions**

Upper Layers: Layers 4–7

- The upper layers deal with handling and processing the IoT data generated by the bottom layer.
- For the sake of completeness, Layers 4–7 of the IoT Reference Model are summarized

IT and OT Responsibilities in the IoT Reference Model

- An interesting aspect of visualizing an IoT architecture this way is that you can start to organize responsibilities along IT and OT lines. Fig. 1.5.4 illustrates a natural demarcation point between IT and OT in the IoT Reference Model framework.



(1A13)**Fig. 1.5.4 : IoT Reference Model Separation of IT and OT**

- As demonstrated in Fig. 1.5.4, IoT systems have to cross several boundaries beyond just the functional layers. The bottom of the stack is generally in the domain of OT. For an industry like oil and gas, this includes sensors and devices connected to pipelines, oil rigs, refinery machinery, and so on. The top of the stack is in the IT area and includes things like the servers, databases, and applications, all of which run on a part of the network controlled by IT.
- In the past, OT and IT have generally been very independent and had little need to even talk to each other. IoT is changing that paradigm.
- At the bottom, in the OT layers, the devices generate real-time data at their own rate-sometimes vast amounts on a daily basis.
- Not only does this result in a huge amount of data transiting the IoT network, but the sheer volume of data suggests that applications at the top layer will be able to ingest that much data at the rate required. To meet this requirement, data has to be buffered or stored at certain points within the IoT stack.
- Layering data management in this way throughout the stack helps the top four layers handle data at their own speed.

IOT Data Management And Compute Stack

- This model also has limitations. As data volume, the variety of objects connecting to the network, and the need for more efficiency increase, new requirements appear, and those requirements tend to bring the need for data analysis closer to the IoT system.
- These new requirements include the following :

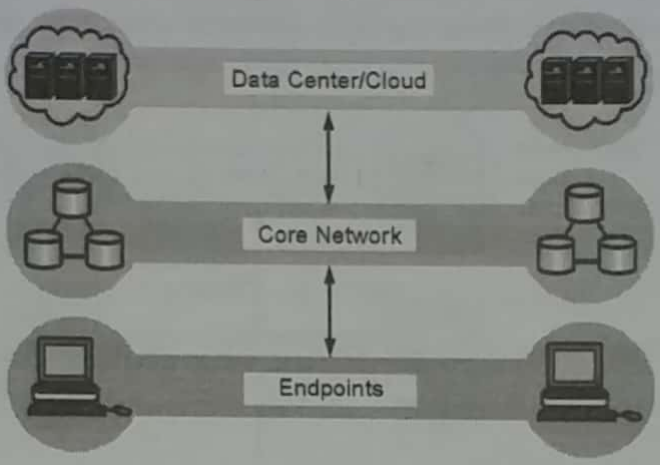
(1) **Minimizing latency :** Milliseconds matter for many types of industrial systems, such as when you are trying to prevent manufacturing line shutdowns or restore electrical service. Analyzing data close to the device that collected the data can make a difference between averting disaster and a cascading system failure.

(2) Conserving network bandwidth : Offshore oil rigs generate 500 GB of data weekly. Commercial jets generate 10 TB for every 30 minutes of flight. It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the cloud. Nor is it necessary because many critical analyses do not require cloud-scale processing and storage.

(3) **Increasing local efficiency :** Collecting and securing data across a wide geographic area with different environmental conditions may not be useful. The environmental conditions in one area will trigger a local response independent from the conditions of

another site hundreds of miles away. Analyzing both areas in the same cloud system may not be necessary for immediate efficiency.

☞ The Traditional IT Cloud Computing Model



(1A14)**Fig. 1.5.5 Cloud Computing Model**

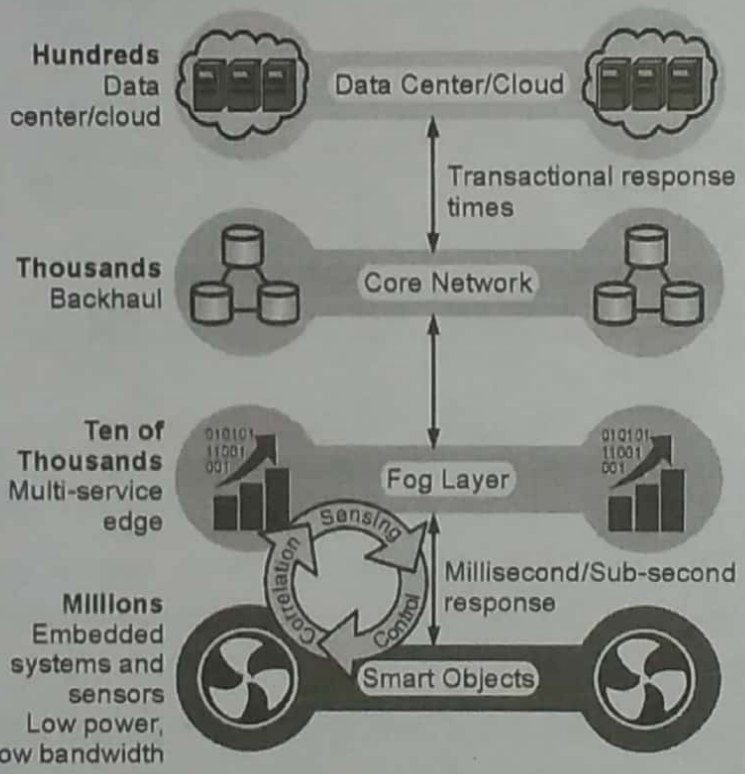
- IoT systems function differently. Several data-related problems need to be addressed
- Bandwidth in last-mile IoT networks is very limited. When dealing with thousands/millions of devices, available bandwidth may be on order of tens of Kbps per device or even less.
- Latency can be very high. Instead of dealing with latency in the milliseconds range, large IoT networks often introduce latency of hundreds to thousands of milliseconds.
- Network backhaul from the gateway can be unreliable and often depends on 3G/LTE or even satellite links. Backhaul links can also be expensive if a per-byte data usage model is necessary.
- The volume of data transmitted over the backhaul can be high, and much of the data may not really be that interesting (such as simple polling messages).
- Big data is getting bigger. The concept of storing and analyzing all sensor data in the cloud is impractical. The sheer volume of data generated makes real-time analysis and response to the data almost impossible.

☞ Fog Computing

GQ. Explain Fog Computing. **(4 Marks)**

- The solution to the challenges mentioned in the previous section is to distribute data management throughout the IoT system, as close to the edge of the IP network as possible. The best-known embodiment of edge services in IoT is fog computing.

- Any device with computing, storage, and network connectivity can be a fog node. Examples include industrial controllers, switches, routers, embedded servers, and IoT gateways. Analyzing IoT data close to where it is collected minimizes latency, offloads gigabytes of network traffic from the core network, and keeps sensitive data inside the local network.



(1A15)**Fig. 1.5.6 : The IoT Data Management and Compute Stack with Fog Computing**

- Fog services are typically accomplished very close to the edge device, sitting as close to the IoT endpoints as possible. One significant advantage of this is that the fog node has contextual awareness of the sensors it is managing because of its geographic proximity to those sensors.
- For example, there might be a fog router on an oil derrick that is monitoring all the sensor activity at that location.
- Because the fog node is able to analyze information from all the sensors on that derrick, it can provide contextual analysis of the messages it is receiving and may decide to send back only the relevant information over the backhaul network to the cloud.
- In this way, it is performing distributed analytics such that the volume of data sent upstream is greatly reduced and is much more useful to application and analytics servers residing in the cloud.

- Fog applications are as diverse as the Internet of Things itself. What they have in common is data reduction monitoring or analyzing real-time data from network-connected things and then initiating an action, such as locking a door, changing equipment settings, applying the brakes on a train, zooming a video camera, opening a valve in response to a pressure reading, creating a bar chart, or sending an alert to a technician to make a preventive repair.
- The defining characteristic of fog computing are as follows:
  (1) **Contextual location awareness and low latency :** The fog node sits as close to the IoT endpoint as possible to deliver distributed computing.
  (2) **Geographic distribution :** In sharp contrast to the more centralized cloud, the services and applications targeted by the fog nodes demand widely distributed deployments.
  (3) **Deployment near IoT endpoints :** Fog nodes are typically deployed in the presence of a large number of IoT endpoints. For example, typical metering deployments often see 3000 to 4000 nodes per gateway router, which also functions as the fog computing node.
  (4) **Wireless communication between the fog and the IoT endpoint :** Although it is possible to connect wired nodes, the advantages of fog are greatest when dealing with a large number of endpoints, and wireless access is the easiest way to achieve such scale.
  (5) **Use for real-time interactions :** Important fog applications involve real-time interactions rather than batch processing. Preprocessing of data in the fog nodes allows upper-layer applications to perform batch processing on a subset of the data.

☞ Edge Computing

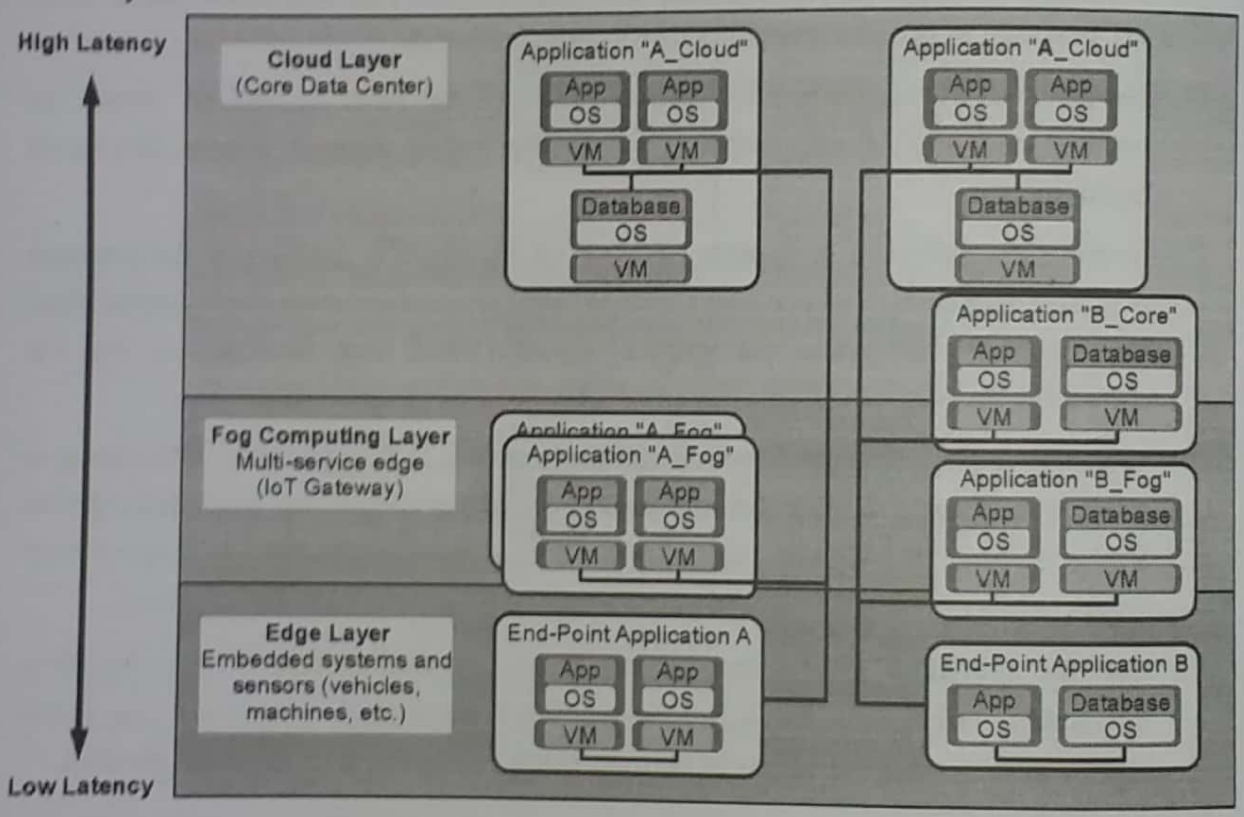
GQ. Explain Edge Computing. **(4 Marks)**

- Fog computing solutions are being adopted by many industries, and efforts to develop distributed applications and analytics tools are being introduced at an accelerating pace.
- The natural place for a fog node is in the network device that sits closest to the IoT endpoints, and these nodes are typically spread throughout an IoT network.

Note : Edge computing is also sometimes called "mist" computing. If clouds exist in the sky, and fog sits near the ground, then mist is what actually sits on the ground. Thus, the concept of mist is to extend fog to the furthest point possible, right into the IoT endpoint device itself.

The Hierarchy of Edge, Fog, and Cloud

- It is important to stress that edge or fog computing in no way replaces the cloud. Rather, they complement each other, and many use cases actually require strong cooperation between layers.
- In the same way that lower courts do not replace the supreme court of a country, edge and fog computing layers simply act as a first line of defense for filtering, analyzing, and otherwise managing data endpoints. This saves the cloud from being queried by each and every node for each event.



(1A16)**Fig. 1.5.7 : Distributed Compute and Data Management Across an IoT System**

- From an architectural standpoint, fog nodes closest to the network edge receive the data from IoT devices.
- The fog IoT application then directs different types of data to the optimal place for analysis:
- The most time-sensitive data is analyzed on the edge or fog node closest to the things generating the data.
- Data that can wait seconds or minutes for action is passed along to an aggregation node for analysis and action.

- Data that is less time sensitive is sent to the cloud for historical analysis, big data analytics, and long-term storage. For example, each of thousands or hundreds of thousands of fog nodes might send periodic summaries of data to the cloud for historical analysis and storage.
- In summary, when architecting an IoT network, you should consider the amount of data to be analyzed and the time sensitivity of this data. Understanding these factors will help you decide whether cloud computing is enough or whether edge or fog computing would improve your system efficiency.
- Fog computing accelerates awareness and response to events by eliminating a round trip to the cloud for analysis. It avoids the need for costly bandwidth additions by offloading gigabytes of network traffic from the core network. It also protects sensitive IoT data by analyzing it inside company walls.

...Chapter ends

❑❑❑

MODULE 2

CHAPTER 2

Things in IoT

Syllabus

Sensors/Transducers - Definition, Principles, Classifications, Types, Characteristics and Specifications, Actuators - Definition, Principles, Classifications, Types, Characteristics and Specifications, Smart Object - Definition, Characteristics and Trends, Sensor Networks – Architecture of Wireless Sensor Network, Network Topologies, Enabling IoT Technologies - Radio Frequency Identification Technology, Micro Electro-Mechanical Systems (MEMS), NFC (Near Field Communication), Bluetooth Low Energy (BLE), LTE-A (LTE Advanced), IEEE 802.15.4 - Standardization and Alliances, ZigBee.

2.1 INTRODUCTION TO SENSORS AND TRANSDUCERS

Introduction

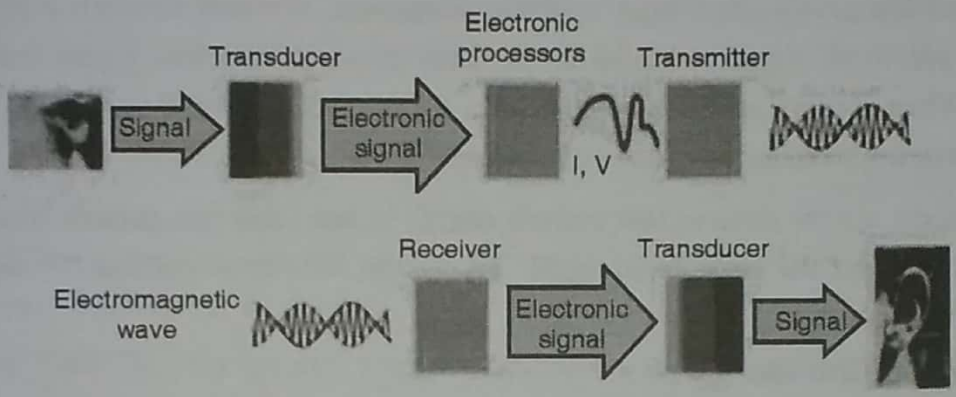


Fig. 2.1.1 : Introduction to Sensors and Transducers

Measurement is an important subsystem in any major system, whether it may be a mechanical system or an electronic system. A measurement system consists of sensors, actuators, transducers and signal processing devices. The use of these elements and devices is not limited to measuring systems.

These are also used in the systems which perform specific tasks, to communicate with the real world. The communication can be anything like reading the status of a signal from a switch or to trigger a particular output to light up an LED.

2.2 SENSOR AND TRANSDUCER DEFINITIONS

GQ. Define Sensor and Transducer. **(4 Marks)**

- The words sensors and transducers are widely used in association with measurement systems. The sensor is an element that produces signals relating to the quantity that is being measured. According to Instrument Society of America, "a sensor is a device that provides usable output in response to a specified quantity which is measured." The word sensor is derived from the original meaning 'to perceive'.
- In simple terms, a sensor is a device that detects changes and events in a physical stimulus and provides a corresponding output signal that can be measured and/or recorded. Here, the output signal can be any measurable signal and is generally an electrical quantity.
- Sensors are devices that perform input function in a system as they 'sense' the changes in a quantity. The best example of a sensor is mercury thermometer. Here the quantity that is being measured is heat or temperature.

- The measured temperature is converted to a readable value on the calibrated glass tube, based on the expansion and contraction of liquid mercury.
- Actuators are devices that work opposite to sensors. A sensor converts a physical event into an electrical signal, whereas an actuator converts electrical signal into a physical event. When sensors are used at input of a system, actuators are used to perform output function in a system as they control an external device.
- Transducers are the devices that convert energy in one form into another form. Generally the energy is in the form of a signal. Transducer is a term collectively used for both sensors and actuators.

☞ Criteria to Choose a Sensor

GQ. Explain different criteria to choose Sensor. **(4 Marks)**

The following are certain features that are considered when choosing a sensor.

1. **Type of Sensing :** The parameter that is being sensed like temperature or pressure.
2. **Operating Principle :** The principle of operation of the sensor.
3. **Power Consumption :** The power consumed by the sensor will play an important role in defining the total power of the system.
4. **Accuracy :** The accuracy of the sensor is a key factor in selecting a sensor.
5. **Environmental Conditions :** The conditions in which the sensor is being used will be a factor in choosing the quality of a sensor.
6. **Cost :** Depending on the cost of application, a low cost sensor or high cost sensor can be used.
7. **Resolution and Range :** The smallest value that can be sensed and the limit of measurement are important.
8. **Calibration and Repeatability :** Change of values with time and ability to repeat measurements under similar conditions.

☞ Basic Requirements of a Sensor or Transducer

GQ. Explain basic requirement of a Sensor or Transducer.

The basic requirements of a sensor are :

1. **Range :** It indicates the limits of the input in which it can vary. In case of temperature measurement, a thermocouple can have a range of 25 – 250°C.

2. **Accuracy :** It is the degree of exactness between actual measurement and true value. Accuracy is expressed as percentage of full range output.
3. **Sensitivity :** Sensitivity is a relationship between input physical signal and output electrical signal. It is the ratio of change in output of the sensor to unit change in input value that causes change in output.
4. **Stability :** It is the ability of the sensor to produce the same output for constant input over a period of time.
5. **Repeatability :** It is the ability of the sensor to produce same output for different applications with same input value.
6. **Response Time :** It is the speed of change in output on a stepwise change in input.
7. **Linearity :** It is specified in terms of percentage of nonlinearity. Nonlinearity is an indication of deviation of curve of actual measurement from the curve of ideal measurement.
8. **Ruggedness :** It is a measure of the durability when the sensor is used under extreme operating conditions.
9. **Hysteresis :** The hysteresis is defined as the maximum difference in output at any measurable value within the sensor's specified range when approaching the point first with increasing and then with decreasing the input parameter. Hysteresis is a characteristic that a transducer has in being unable to repeat its functionality faithfully when used in the opposite direction of operation.

☞ Classification of Sensors

GQ. Explain different types of sensor. **(4 Marks)**

The scheme of classifying sensors can range from very simple to very complex. The stimulus that is being sensed is an important factor in this classification.

Some of the stimuli are :

1. **Acoustic :** Wave, spectrum and wave velocity.
2. **Electric :** Current, charge, potential, electric field, permittivity and conductivity.
3. **Magnetic :** Magnetic field, magnetic flux and permeability.
4. **Thermal :** Temperature, specific heat and thermal conductivity.
5. **Mechanical :** Position, acceleration, force, pressure, stress, strain, mass, density, momentum, torque, shape, orientation, roughness, stiffness, compliance, crystallinity and structural.

6. **Optical :** Wave, wave velocity, refractive index, reflectivity, absorption and emissivity.

Fig. 2.2.1 : Different Types of Sensors

The sensors' conversion phenomenon is also an important factor in classification of sensors. Some of the conversion phenomena are magneto electric, thermoelectric and photoelectric.

Based on the applications of sensors, their classification can be made as follows.

I. Displacement, Position and Proximity Sensors

- Resistive Element or Potentiometer
- Capacitive Elements
- Strain Gauged Element
- Inductive Proximity Sensors
- Eddy Current Proximity Sensors
- Differential Transformers
- Optical Encoders
- Hall Effect Sensors

- Pneumatic Sensors
- Proximity Switches
- Rotary Encoders

II. Temperature Sensors

- Thermistors
- Thermocouple
- Bimetallic Strips
- Resistance Temperature Detectors
- Thermostat

III. Light Sensors

- Photo Diode
- Phototransistor
- Light Dependent Resistor

IV. Velocity and Motion

- Pyroelectric Sensors
- Tachogenerator
- Incremental encoder

V. Fluid Pressure

- Diaphragm Pressure Gauge
- Tactile Sensor
- Piezoelectric Sensors
- Capsules, Bellows, Pressure Tubes

VI. Liquid Flow and Level

- Turbine Meter
- Orifice Plate and Venturi Tube

VII. IR Sensor

- Infrared Transmitter and Receiver Pair

VIII. Force

- Strain Gauge
- Load Cell

IX. Touch Sensors

- Resistive Touch Sensor
- Capacitive Touch Sensors

X. UV Sensors

- Ultraviolet Light Detector
- Photo Stability Sensors
- UV Photo Tubes
- Germicidal UV Detectors

All the sensors can be classified into two types based on the power or signal requirement. They are Active sensors and passive sensors.

In order to operate active sensors, require power signal from an external source. This signal is called an excitation signal, and based on this excitation signal the sensor produces output. Strain gauge is an example of active sensor. It is a pressure sensitive resistive bridge network and doesn't produce the output electrical signal on its own. The amount of force applied can be measured by relating it to the resistance of the network. The resistance can be measured by passing current through it. Current acts as the excitation signal.

In contrast, passive sensors directly produce the output electrical signal in response to the input stimulus. All the power required by a passive sensor is obtained from the measurand. A thermocouple is a passive sensor.

Commonly used Sensors and Transducers

Some of the most commonly used sensors and transducers for different stimuli (the quantity to be measured) are :

- For sensing light, the input devices or sensors are photo diode, photo transistor, light dependent resistor and solar cells. The output devices or actuators are LEDs, displays, lamps and fiber optics.
- For sensing temperature, the sensors are thermistor, thermocouple, resistance temperature detectors and thermostat. The actuators are heaters.

- For sensing position, the input devices are potentiometer, proximity sensor, and differential transformer. The output devices are motor and panel meter.
- For sensing pressure, the sensors are strain gauge and load cell. The actuators are lifts and jacks and electromagnetic vibrations.
- For sensing sound, the input devices are microphones and output devices are loudspeakers and buzzers.
- For sensing speed, the sensors used are tachogenerator and Doppler Effect sensors. The actuators are motors and brakes.

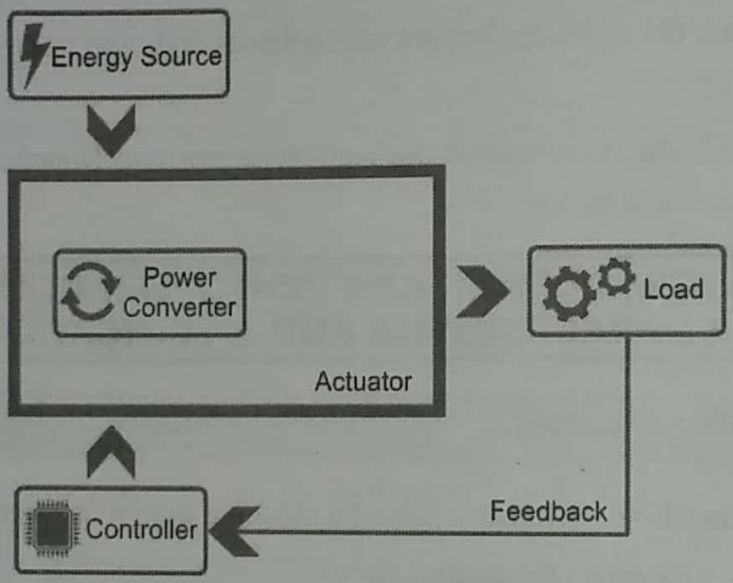
2.3 ACTUATORS - DEFINITION, PRINCIPLES, CLASSIFICATIONS, TYPES, CHARACTERISTICS AND SPECIFICATIONS

GQ. Explain in details Actuators. **(4 Marks)**

- An actuator is a machine, or rather a part of a machine used to convert externally available energy into motion based on the control signals.
- Much like how hands and legs enable humans to move around and perform actions, actuators let machines perform various mechanical movements. The topic for discussion for this article is actuators. We will explain what is an actuator, how actuators work, and what are the different types of actuators used in industrial and domestic applications.
- From the perspective of systems engineering, functions of any engineering product can be classified into three distinct categories; the collection of input, processing and producing an output.
- For electromechanical systems, the input is detected and measured by a device called a sensor. The task of a sensor is to sample the signals available to it and convert them into a form understandable by the system. The system then processes the information and decides how to respond.
- But how exactly does a system respond? The answer is, with the help of an Actuator.
- Typically, an actuator consists of :

(1) **Energy source :** Energy sources provide actuators with the ability to do work. Actuators draw electrical or mechanical energy from external sources for carrying out their operation. The energy available to the actuator can be regulated or unregulated depending on the system that it is a part of.

(2) **Power converter :** If the energy source attached to the actuators is unregulated, it requires some additional apparatus to regulate it and convert it into a form suitable for the actuation action. Hydraulic valves or solid-state power electronic converters are examples of converters used in industrial actuators.



(1B1)**Fig. 2.3.1 : Power Converter**

Functional block diagram of an actuator

(1) **Controller :** In addition to enabling the operation of the power converter, a control unit is responsible for generating actuating signals. In some systems, it provides the user with an interface to provide inputs or check the system's status.

(2) **Load :** The mechanical system attached to the actuator that uses the motion of the actuator is called the load. Characteristics like Force/Torque and Speed are carefully tuned before interfacing an actuator with the load.

☞ Classification of actuators based on the motion

GQ. Explain Different types of Actuators. **(4 Marks)**

The most apparent and basic classification of actuators is based on the type of motion that it produces.

1. Rotary Actuator

The actuators that can provide a circular motion at their output can be classified under the category of rotary actuators. When it comes to rotational motion, it is hard to think of any other device than the motors, which we shall discuss in the next section of this article.

2. Linear Actuators

The actuators that can provide motion in a straight line at their output can be classified under the category of linear actuators. Hydraulic or Pneumatic actuators are the most common linear actuators used in the industry. We will also discuss these devices in detail.

(1B2)**Fig. 2.3.2 : Linear Actuators**

With the help of suitable equipment, it is possible to use a rotary actuator to produce linear motion and a linear actuator to produce rotary motion

☞ Classification of actuators based on the energy source

The energy source can be another means of classification for the actuators.

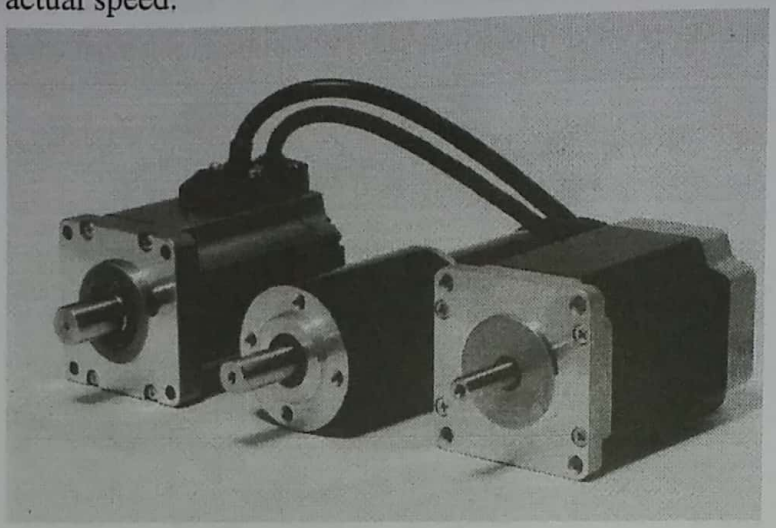
1. Electromagnetic Actuators

Electromagnetic actuators make use of electricity and magnetism to perform actuation. These actuators are among the most commonly used actuators in the industries.

2. AC and DC Servo Motor actuators

- Electrical motors are among the most versatile actuators suitable for a plethora of different application scenarios.
- Servo drives can be powered by an AC or DC power supply and consist of a motor, feedback unit, control unit, and sometimes a gearbox. The working of a servo motor greatly differs from that of ordinary AC or DC motors. To operate a servo motor, a control signal is required in addition to the power.
- Initially, when a voltage is applied to the terminals of a servo motor, it begins to rotate. The position of the shaft is continuously monitored by a rotary encoder, and the voltage-current levels are kept in check by the voltmeter-ammeter combination.

The controller then computes the motor's actual speed, compares it with the target speed, and adjusts the voltage and current levels to reduce the error between the target speed and actual speed.



(1B3) **Fig. 2.3.3 : AC and DC Servo Motor**

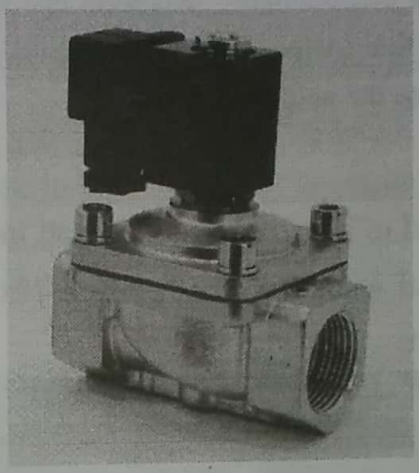
3. Stepper Motor Actuators

- Stepper motors are used for applications where the angular position of the shaft needs to be accurately controlled. The control scheme of the stepper motor is simple, accurate and doesn't require any feedback. This is the reason why they are often more affordable.
- The stator of the stepper motor contains multiple teeth, each acting as a pole for the rotor. When a particular pole or a set of poles are energised, the rotor reorients itself to allow maximum MMF to pass through it. When the next step of the poles is energised, the rotor shifts its position. This allows the rotor to complete a revolution in several distinct steps, and that's how the motor gets its name.

4. Solenoid Actuators

- A solenoid actuator consists of a conducting coil wound on a ferromagnetic core with a flat head on one side and a spring connected on the other. The whole apparatus is placed in a hollow cylindrical body.
- Whenever current flows through the wire, the coil acts as an electromagnet, attracting the ferromagnetic core in one direction and compressing the spring during the process.
- Solenoid Valves are used in controlling flow of liquids in industrial processes

- Once the power supply is removed, the spring pushes the core back to the original position. The strength of the actuator depends upon the number of turns in the coil. The setup looks and acts a lot like a piston.



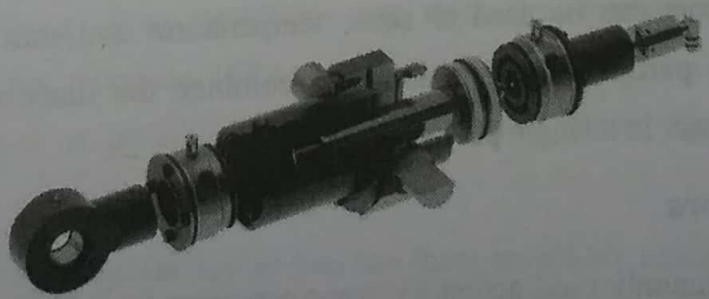
(1B4)Fig. 2.3.4 : Solenoid Actuators

5. Fluid Power Actuators

- The actuators that make use of liquids or gasses are called fluid power actuators. On a very superficial level, we can think of a fluid power actuator as a moving disk inside a hollow cylinder filled with fluid forming a piston.
- he movement of the disk appears as the motion of the actuator. Advanced fluid actuators with dual-acting cylinders make use of fluid for both extension and retracement strokes.

6. Hydraulic Actuators

- These actuators make use of liquids as a driving force to produce mechanical work. Hydraulic Actuators are probably the most widely used linear actuators in real-life applications. These devices are used when stable, but high actuating thrust/forces are required in a small region.



(1B5)Fig. 2.3.5 : Hydraulic Actuators

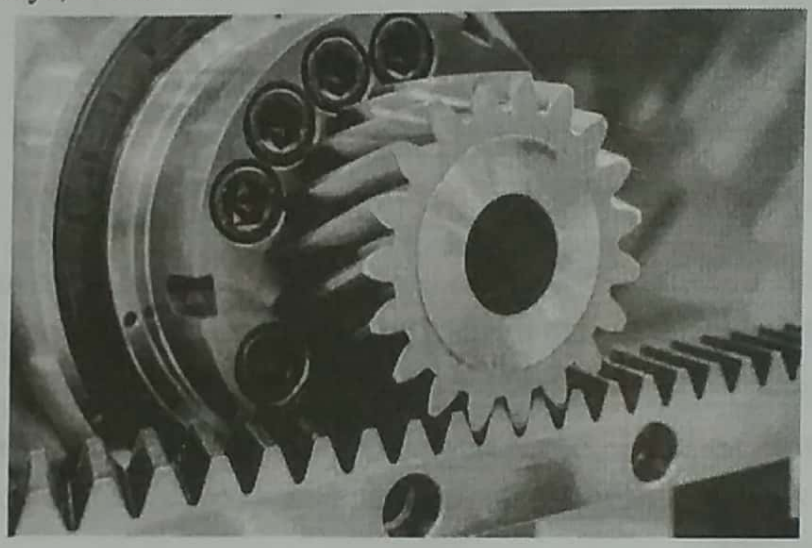
- Hydraulic and pneumatic actuators use the power of fluids to apply a force

7. Pneumatic Actuators

The design and construction of pneumatic actuators are very similar to that of hydraulic actuators. The difference is that instead of using a liquid, energy from compressed gases or vacuum is used to facilitate the actuation process.

8. Mechanical Actuators

- These actuators are used to interconvert rotary and linear motion in machines. Some examples of mechanical actuators are rack and pinion arrangements, crankshafts, gears, pulleys, and chains.



(1B6)**Fig. 2.3.6 : Mechanical Actuators**

- Rack and pinion arrangement for converting rotational motion into linear motion and vice versa

9. Thermal Actuators

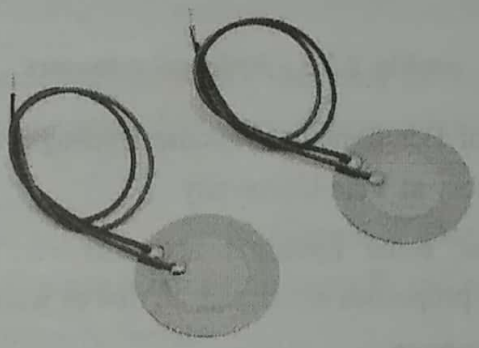
Thermal actuators make use of materials that expand or contract by the application of heat. These actuators can be used to sense temperatures and shut off a supply to the system they are a part of. Thermal actuators combine the functions of a temperature switch and an actuator in a single package.

10. Special Actuators

Apart from the commonly used actuators, some actuators are still under research and find their application in limited fields.

11. Piezoelectric Actuators

- Piezoelectric materials exhibit a contraction/expansion whenever a voltage is applied to them. By applying a controlled signal, this property of piezoelectric materials can be used to build actuators for small but highly precise and rapid positioning mechanisms.
- Piezoelectric plates are used in mist makers to atomise water into small droplets and create mist.



(1B7)**Fig. 2.3.7 : Piezoelectric Actuators**

12. Shape Memory Alloy Actuators

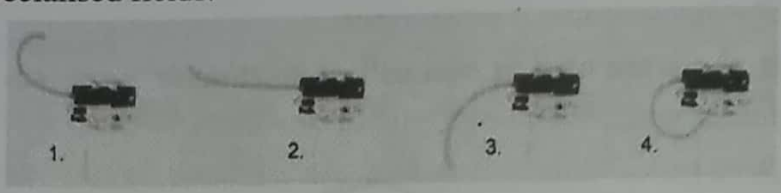
- Shape Memory Alloys (SMAs) undergo a change in their molecular arrangement when they are heated or cooled. When a force is applied to alloys like Nitinol (Nickel-Titanium), they experience a deformation that can be reversed with heating.
- Heating can be done directly by application of thermal energy or with the help of electric power. This property of SMAs can be used to build actuators.

13. Supercoiled Polymer Actuators

- It gets challenging to downsize conventional actuators like electric motors beyond a certain limit, making them unsuitable for miniature machines. This is where Supercoiled Polymer Actuators (SPAs) come in. Supercoiling is a property of DNA strands that makes it possible for them to relieve stress by twisting around themselves.
- SPAs are inspired by a similar design that lets them reversibly change their shape and size when stimulated. These structures respond quickly and can last for millions of cycles.

14. Hydrogel actuators

- Hydrogel actuators demonstrate a change in their shape with changes in the temperature, light, pH and concentration of certain substances. The fact that hydrogels can be effective only in aqueous medium limits their applications to some specific specialised fields.



(1B8)**Fig. 2.3.8 : Hydrogel actuators**

- Bending behaviour of Polydimethylsiloxane Hydrogel actuator in aqueous solution. Source : The Faboratory at Yale University
- Research shows that some hydrogel actuators can be optically and sonically camouflaged as their properties are similar to that of water.

☞ Applications of Actuators

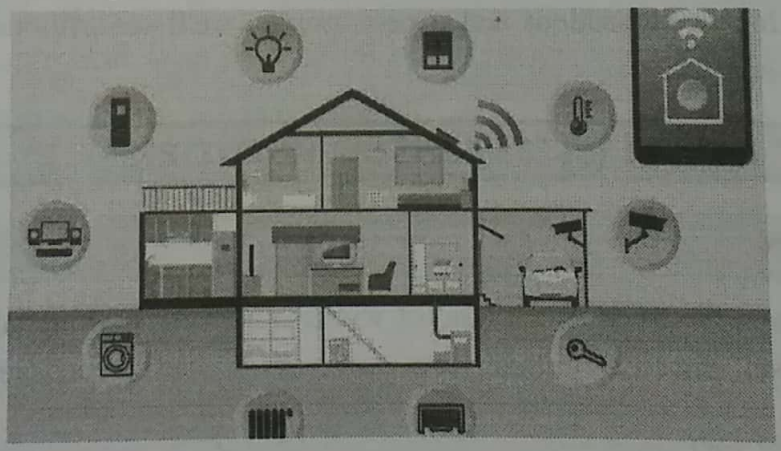
- An actuator that can generate sufficient force has suitable load-speed characteristics, works in the operating range with high efficiency, and comes with a robust design is considered ideal for a given application.
- Industrial automation and robotics are the two fields where it is just impossible to imagine getting anything done without actuators. These parts enable production machines to move from one place to another and grab objects. Actuators are also widely used in heavy construction equipment and agricultural machinery to enable several different sets of movements. Another beautiful application of actuators can be in solar panels. As the sun rises and sets during the day, the solar panels equipped with actuators keep changing their angle to harness maximum solar energy.
- Coming to household applications, actuators can be found in almost every smart home appliance, from furniture to robotic vacuum cleaners that require any sort of manoeuvre. A lot of toys too contain some small actuators built-in them. The applications are endless.

⏭ 2.4 SMART OBJECT

GQ. Write a short note on Smart Object. **(2 Marks)**

- A **smart object** is an object that enhances the interaction with other smart objects as well as with people also.

- The world of IoT is the network of interconnected heterogeneous objects (such as smart devices, smart objects, sensors, actuators, RFID, embedded computers, etc.) uniquely addressable and based on standard communication protocols.
- In a day to day life, people have a lot of object with internet or wireless or wired connection. Such as :
  - Smartphone
  - Tablets
  - TV computer
- These objects can be interconnected among them and facilitate our daily life (smart home, smart cities) no matter the situation, localization, accessibility to a sensor, size, scenario or the risk of danger.
- Smart objects are the building blocks of the Internet of Things (IoT). In the past, I've built an Infrared Temperature Scanner using a Raspberry Pi and some accessories. A standalone device like this can be extremely useful.
- However, "*the real power of smart objects in IoT comes from being networked together rather than being isolated as standalone objects. This ability to communicate over a network has a multiplicative effect and allows for very sophisticated correlation and interaction between disparate smart objects*"



(1B9)**Fig. 2.4.1 : Smart Objects**

By **definition**, a smart object must contain the following features :

1. **Processing Unit :** A small computer, typically featuring an AMD chipset, which receives input from sensors and produces output for actuators and/or for communication with other devices (which can include other smart objects, controllers, gateways, routers, back haul network)

2. **Sensor(s) and/or actuator(s) :** Sensors collect or measure data, which is then processed by the processing unit (see above) to produce a digital representation of that data, which can then be acted upon, either by actuation or communication. Actuators do things and are usually classified by the type of motion they produce, their power output, whether they're binary or continuous, their area of application or their type of energy (mechanical, electrical, hydraulic, electromagnetic, etc.)
3. **Communication device(s) :** This unit is responsible for connecting the smart object with other smart objects and/or the network. In IoT Edge devices, communication is usually wireless.
4. **Power source :** because IoT devices are often scattered in the field, it's often impractical to power them externally. This, most smart objects are battery-powered (long-lasting) or utilize solar or other power which can be claimed from the surrounding environment.

☞ **Trends in Smart Objects**

(1) Size is decreasing
(2) Power consumption is decreasing
(3) Processing power is increasing
(4) Communication capabilities are improving
(5) Communication is being increasingly standardized

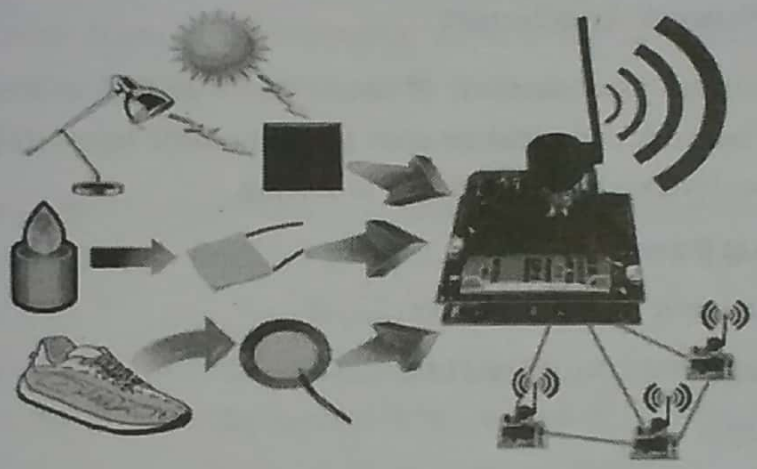
The future of IoT is tremendous and experts predict we'll see trillions of sensors in the field within a few years.

⏭ 2.5 WHAT IS A WIRELESS SENSOR NETWORK?

GQ. Explain WSN. **(4 Marks)**

- A Wireless Sensor Network is one kind of wireless network that includes a large number of circulating, self-directed, minute, low powered devices named sensor nodes called motes.
- These networks certainly cover a huge number of spatially distributed, little, battery-operated, embedded devices that are networked to caringly collect, process, and transfer data to the operators, and it has controlled the capabilities of computing & processing. Nodes are tiny computers, which work jointly to form networks.
- The sensor node is a multi-functional, energy-efficient wireless device. The applications of motes in industrial are widespread. A collection of sensor nodes collects the data from the surroundings to achieve specific application objectives.

- The communication between motes can be done with each other using transceivers. In a wireless sensor network, the number of motes can be in the order of hundreds/ even thousands. In contrast with sensor networks, Ad Hoc networks will have fewer nodes without any structure.



(1B10) **Fig. 2.5.1 : Wireless Sensor Network**

Wireless Sensor Network Architecture

- The most common wireless sensor network architecture follows the OSI architecture Model. The architecture of the WSN includes five layers and three cross layers.
- Mostly in sensor network, we require five layers, namely application, transport, network, data link and physical layer. The three cross planes are namely power management, mobility management, and task management.
- These layers of the WSN are used to accomplish the n/w and make the sensors work together in order to raise the complete efficiency of the network. Please follow the below link for Types of wireless sensor networks and WSN topologies

☞ Types of WSN Architectures

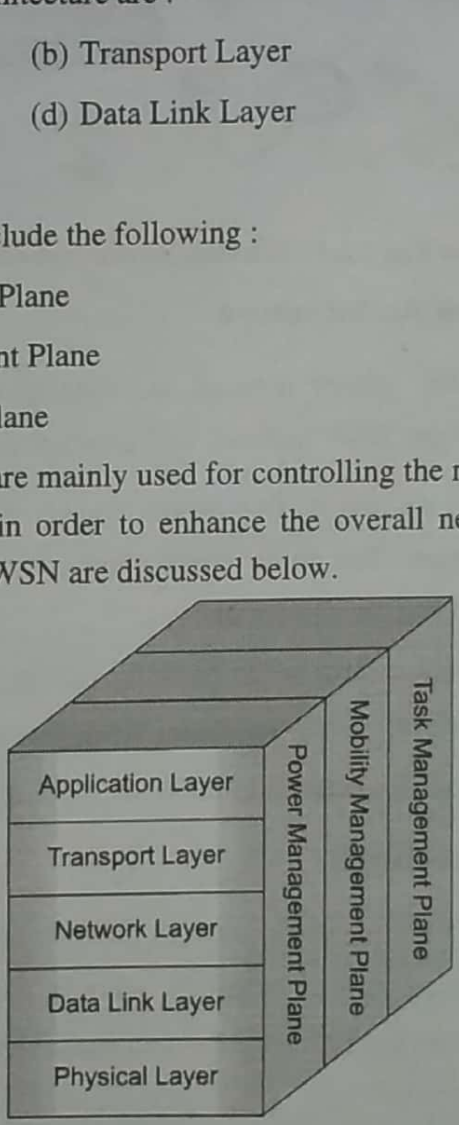
- The architecture used in WSN is sensor network architecture. This kind of architecture is applicable in different places such as hospitals, schools, roads, buildings as well as it is used in different applications such as security management, disaster management & crisis management, etc.
- There are two types of architectures used in wireless sensor networks which include the following :

- There are 2 types of wireless sensor architectures :

1. Layered Network Architecture
2. Clustered Network Architecture

1. Layered Network Architecture

- This kind of network uses hundreds of sensor nodes as well as a base station. Here the arrangement of network nodes can be done into concentric layers. It comprises five layers as well as 3 cross layers which include the following.
- The five layers in the architecture are :
  (a) Application Layer (b) Transport Layer
  (c) Network Layer (d) Data Link Layer
  (e) Physical Layer
- The three cross layers include the following :
  (1) Power Management Plane
  (2) Mobility Management Plane
  (3) Task Management Plane
- These three cross layers are mainly used for controlling the network as well as to make the sensors function as one in order to enhance the overall network efficiency. The above mentioned five layers of WSN are discussed below.



(1B11)**Fig. 2.5.2 : Wireless Sensor Network Architecture**

(a) Application Layer

- The application layer is liable for traffic management and offers software for numerous applications that convert the data in a clear form to find positive information.
- Sensor networks arranged in numerous applications in different fields such as agricultural, military, environment, medical, etc.

(b) Transport Layer

- The function of the transport layer is to deliver congestion avoidance and reliability where a lot of protocols intended to offer this function are either practical on the upstream.
- These protocols use dissimilar mechanisms for loss recognition and loss recovery. The transport layer is exactly needed when a system is planned to contact other networks.
- Providing a reliable loss recovery is more energy-efficient and that is one of the main reasons why TCP is not fit for WSN.
- In general, Transport layers can be separated into Packet driven, Event-driven. There are some popular protocols in the transport layer namely STCP (Sensor Transmission Control Protocol), PORT (Price-Oriented Reliable Transport Protocol and PSFQ (pump slow fetch quick).

(c) Network Layer

- The main function of the network layer is routing, it has a lot of tasks based on the application, but actually, the main tasks are in the power conserving, partial memory, buffers, and sensor don't have a universal ID and have to be self-organized.
- The simple idea of the routing protocol is to explain a reliable lane and redundant lanes, according to a convincing scale called a metric, which varies from protocol to protocol.
- There are a lot of existing protocols for this network layer, they can be separated into; flat routing and hierarchal routing or can be separated into time-driven, query-driven & event-driven.

(d) Data Link Layer

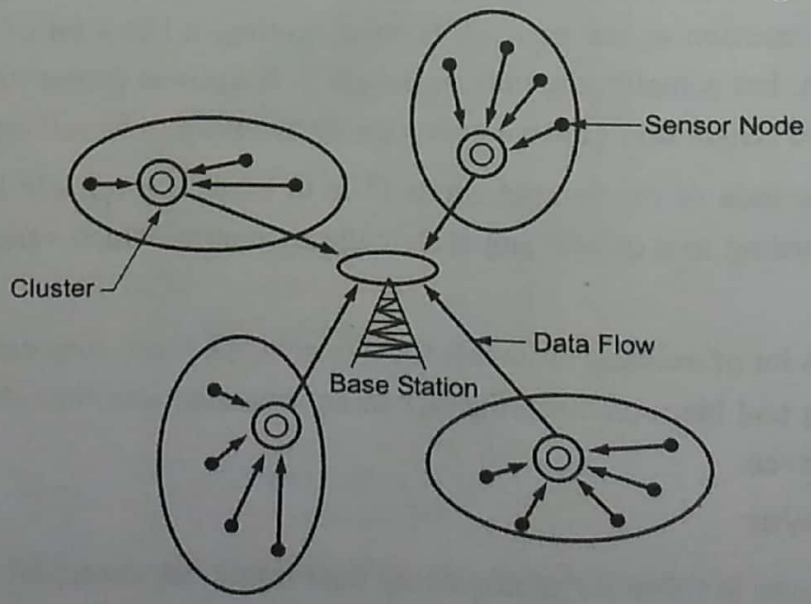
The data link layer is liable for multiplexing data frame detection, data streams, MAC, & error control, confirm the reliability of point–point (or) point– multipoint.

(e) Physical Layer

- The physical layer provides an edge for transferring a stream of bits above the physical medium.
- This layer is responsible for the selection of frequency, generation of a carrier frequency, signal detection, Modulation and data encryption. IEEE 802.15.4 is suggested as typical for low rate particular areas and wireless sensor networks with low cost, power consumption, density, the range of communication to improve the battery life.
- CSMA/CA is used to support star & peer to peer topology. There are several versions of IEEE 802.15.4.V.
- The main benefits of using this kind of architecture in WSN is that every node involves simply in less-distance, low- power transmissions to the neighboring nodes due to which power utilization is low as compared with other kinds of sensor network architecture. This kind of network is scalable as well as includes a high fault tolerance.

2. Clustered Network Architecture

- In this kind of architecture, separately sensor nodes add into groups known as clusters which depend on the "Leach Protocol" because it uses clusters.
- The term 'Leach Protocol' stands for "Low Energy Adaptive Clustering Hierarchy". The main properties of this protocol mainly include the following.



(1B12)**Fig. 2.5.3 : Clustered Network**

☞ Clustered Network Architecture

- This is a two-tier hierarchy clustering architecture.
- This distributed algorithm is used to arrange the sensor nodes into groups, known as clusters.
  - In every cluster which is formed separately, the head nodes of the cluster will create the TDMA (Time-division multiple access) plans.
  - It uses the Data Fusion concept so that it will make the network energy efficient.
- This kind of network architecture is extremely used due to the data fusion property. In every cluster, every node can interact through the head of the cluster to get the data.
- All the clusters will share their collected data toward the base station. The formation of a cluster, as well as its head selection in each cluster, is an independent as well as autonomous distributed method.

☞ Design Issues of Wireless Sensor Network Architecture

GQ. Explain Design Issues of WSN. **(4 Marks)**

The design issues of wireless sensor network architecture mainly include the following.

1. Energy Consumption	2. Localization
3. Coverage	4. Clocks
5. Computation	6. Cost of Production
7. Design of Hardware	8. Quality of Service

1. Energy Consumption

- In WSN, power consumption is one of the main issues. As an energy source, the battery is used by equipping with sensor nodes.
- The sensor network is arranged within dangerous situations so it turns complicated for changing otherwise recharging batteries. The energy consumption mainly depends on the sensor nodes' operations like communication, sensing & data processing.
- Throughout communication, the energy consumption is very high. So, energy consumption can be avoided at every layer by using efficient routing protocols.

2. Localization

- For the operation of the network, the basic, as well as critical problem, is sensor localization. So sensor nodes are arranged in an ad-hoc manner so they don't know about their location.
- The difficulty of determining the sensor's physical location once they have been arranged is known as localization. This difficulty can be resolved through GPS, beacon nodes, localization based on proximity.

3. Coverage

- The sensor nodes in the wireless sensor network utilize a coverage algorithm for detecting data as well as transmit them to sink through the routing algorithm. To cover the whole network, the sensor nodes should be chosen.
- There efficient methods like least and highest exposure path algorithms as well as coverage design protocol are recommended.

4. Clocks

- In WSN, clock synchronization is a serious service. The main function of this synchronization is to offer an ordinary timescale for the nodes of local clocks within sensor networks.
- These clocks must be synchronized within some applications like monitoring as well as tracking.

5. Computation

- The computation can be defined as the sum of data that continues through each node. The main issue within computation is that it must reduce the utilization of resources.
- If the life span of the base station is more dangerous, then data processing will be completed at each node before data transmitting toward the base station. At every node, if we have some resources then the whole computation should be done at the sink.

6. Production Cost

- In WSN, the large number of sensor nodes is arranged. So if the single node price is very high then the overall network price will also be high.
- Ultimately, the price of each sensor node has to be kept less. So the price of every sensor node within the wireless sensor network is a demanding problem.

7. Hardware Design

- When designing any sensor network's hardware like power control, micro-controller and communication unit must be energy-efficient.
- Its design can be done in such a way that it uses low-energy.

8. Quality of Service

- The quality of service or QoS is nothing but, the data must be distributed in time. Because some of the real-time sensor-based applications mainly depend on time. So if the data is not distributed on time toward the receiver then the data will turn useless.
- In WSNs, there are different types of QoS issues like network topology that may modify frequently as well as the accessible state of information used for routing can be imprecise.

☞ Structure of a Wireless Sensor Network

The structure of WSN mainly comprises various topologies used for radio communications networks like a star, mesh, and hybrid star.

These topologies are discussed below in brief.

Star Network

- The communication topology like a star network is used wherever only the base station can transmit or receive a message toward remote nodes. There is a number of nodes are available which are not allowed to transmit messages to each other. The benefits of this network mainly comprise simplicity, capable of keeping the power utilization of remote nodes to a minimum.
- It also lets communications with less latency among the base station as well as a remote node. The main drawback of this network is that the base station should be in the range of radio for all the separate nodes. It is not robust like other networks because it depends on a single node to handle the network.

Mesh Network

- This kind of network permits to the transmission of the data from one node to another within the network that is in the range of radio transmission.
- If a node needs to transmit a message to another node and that is out of radio communications range, then it can utilize a node like an intermediate to send the message toward the preferred node.

- The main benefit of a mesh network is scalability as well as redundancy. When an individual node stops working, a remote node can converse to any other type of node within the range, then forwards the message toward the preferred location.
- Additionally, the network range is not automatically restricted through the range among single nodes; it can extend simply by adding a number of nodes to the system.
- The main drawback of this kind of network is power utilization for the network nodes that execute the communications like multi-hop are usually higher than other nodes that don't have this capacity of limiting the life of battery frequently.
- Moreover, when the number of communication hops increases toward a destination, then the time taken to send the message will also increase, particularly if the low power process of the nodes is a necessity.

Hybrid Star – Mesh Network

- A hybrid among the two networks like star and mesh provides a strong and flexible communications network while maintaining the power consumption of wireless sensor nodes to a minimum.
- In this kind of network topology, the sensor nodes with less power are not allowed to transmit the messages. This permits to maintenance least power utilization.
- But, other network nodes are allowed with the capability of multi-hop by allowing them to transmit messages from one node to another on the network.
- Usually, the nodes with the multi-hop capacity have high power and are frequently plugged into the mains line.
- This is the implemented topology through the upcoming standard mesh networking called ZigBee.

☞ Structure of a Wireless Sensor Node

- The components used to make a wireless sensor node are different units like sensing, processing, transceiver and power. It also includes additional components that depend on an application like a power generator, a location finding system and a mobilizer.
- Generally, sensing units include two subunits namely ADCs as well as sensors. Here sensors generate analog signals which can be changed to digital signals with the help of ADC, after that it transmits to the processing unit.
- Generally, this unit can be associated through a tiny storage unit to handle the actions to make the sensor node work with the other nodes to achieve the allocated sensing tasks.

- The sensor node can be connected to the network with the help of a transceiver unit. In the sensor node, one of the essential components is a sensor node. The power-units are supported through power scavenge units like solar cells whereas the other subunits depend on the application.
- A wireless sensing nodes functional block diagram is shown above. These modules give a versatile platform to deal with the requirements of wide applications. For instance, based on the sensors to be arranged, the replacement of signal conditioning block can be done.
- This permits to use of different sensors along with the wireless sensing node. Likewise, the radio link can be exchanged for a specified application.

☞ Characteristics of Wireless Sensor Network

The characteristics of WSN include the following :

(1) The consumption of Power limits for nodes with batteries

(2) Capacity to handle node failures

(3) Some mobility of nodes and Heterogeneity of nodes

(4) Scalability to a large scale of distribution

(5) Capability to ensure strict environmental conditions

(6) Simple to use

(7) Cross-layer design

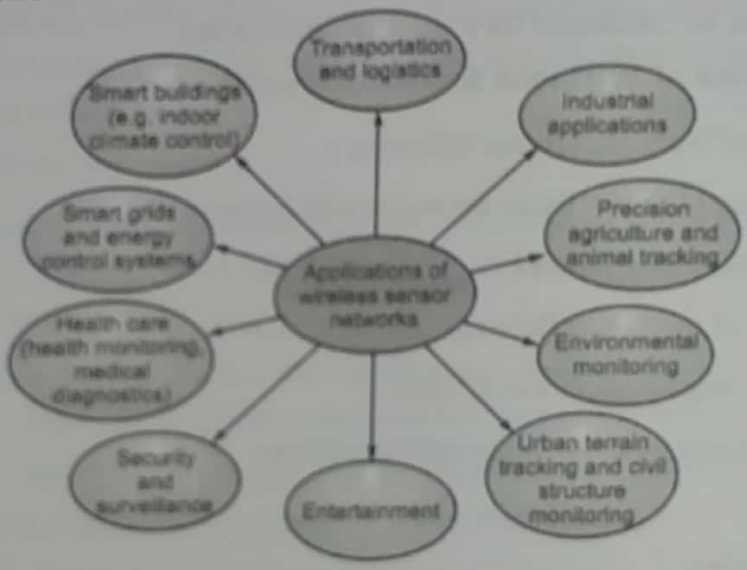
☞ Advantages of Wireless Sensor Networks

The advantages of WSN include the following

1. Network arrangements can be carried out without immovable infrastructure.
2. Apt for the non-reachable places like mountains, over the sea, rural areas, and deep forests.
3. Flexible if there is a casual situation when an additional workstation is required.
4. Execution pricing is inexpensive.
5. It avoids plenty of wiring.
6. It might provide accommodations for the new devices at any time.
7. It can be opened by using centralized monitoring.

Wireless Sensor Network Applications

- Wireless sensor networks may comprise numerous different types of sensors like low sampling rate, seismic, magnetic, thermal, visual, infrared, radar, and acoustic, which are clever to monitor a wide range of ambient situations.
- Sensor nodes are used for constant sensing, event ID, event detection & local control of actuators.
- The applications of wireless sensor networks mainly include health, military, environmental, home and other commercial areas.



(1813)Fig. 2.5.4 : Application of WSN

WSN Application

GQ. Explain different Application of WSN. **(4 Marks)**

(1) Military Applications
(2) Health Applications
(3) Environmental Applications
(4) Home Applications
(5) Commercial Applications
(6) Area monitoring
(7) Health care monitoring
(8) Environmental/Earth sensing
(9) Air pollution monitoring
(10) Forest fire detection
(11) Landslide detection
(12) Water quality monitoring
(13) Industrial monitoring

What are the different types of wireless sensor networks?

- The development of network technologies has prompted sensor folks to consider alternatives that reduce costs and complexity and improve reliability.
- Early sensor networks used simple twisted shielded–pair (TSP) implementations for each sensor. Later, the industry adopted multidrop buses (e.g., Ethernet).
- Now we're starting to see true web-based networks (e.g., the World Wide Web) implemented on the factory floor.
- As wireless sensors become real commodities on the market, new options or new arguments for old options are causing professionals to consider network strategies once ruled out.
- Let's look at the three classic network topologies (point-to-point, multidrop, and web), assess their strengths and weaknesses, and look at how the rules have changed now that wireless systems are coming online.
- In addition, to build functional sensor networks, you'll probable have to integrate hardware and software from multiple vendors (see the sidebar "Network Questions,").
- So along with everything else, you have to come to terms with standards and protocols those that exist, those that are emerging, and those needed to ensure interoperability on the factory floor.

☞ Point-to-Point Networks

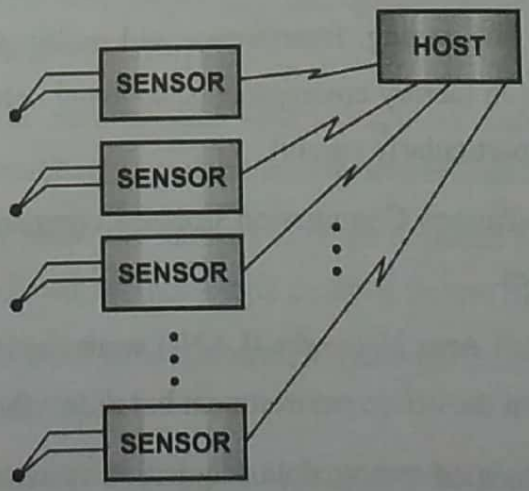


Fig. 2.5.5 : point-to-point network topologies

- Theoretically, these systems are the most reliable because there is only one single point of failure in the topology .

- You can improve the system by adding redundant hosts, but wiring two hosts can be a problem. The 4–20 mA standard allows multiple readout circuits if the standard loads are used at each readout.
- Problems can arise if readout devices load the circuit beyond its capability, but most designers are familiar with the limitations and are sufficiently careful.
- each sensor node puts its information onto a common medium. This requires careful attention to protocols in hardware and software. The single-wire connection represents a potential single-point failure. But some vendors supply redundant connections to mitigate this potential problem
- Some networks provide frequency-modulated (FM) signals on the wires to carry multiple sensor readings on separate FM channels. Some standards (e.g., the HART bus) support multiplexing of digital signals on the existing analog wiring in older plants.
- These architectures blur the distinction between point-to-point and multidrop networks.
- Early wireless networks were simple radio-frequency (RF) implementations of this topology. These networks used RF modems to convert the RS-232 signal to a radio signal and back again.
- Fluke (Everett, Washington) developed a digital voltmeter that could be configured to accept a voltage signal and transmit the signal over a dedicated radio frequency channel.
- The reliability of these implementations was sometimes suspect because most were designed with simple FM coding. Interference and multipath propagation effects caused significant degradation in factory environments, so many networks proved to be unreliable unless designers were particularly careful.
- The Federal Communications Commission licensed companies and devices to operate at the allocated frequencies.
- Complete wireless Local Area Networks (LANs) were implemented using this technique. These were successful in the office environment but didn't fare as well in factories.
- Many designers implemented remote data acquisition systems with this topology by using a data concentrator in the field to feed the data to a radio transmitter for transmission to the hosts, where the signals were demultiplexed into the original sensor signals.

☞ Multidrop Networks

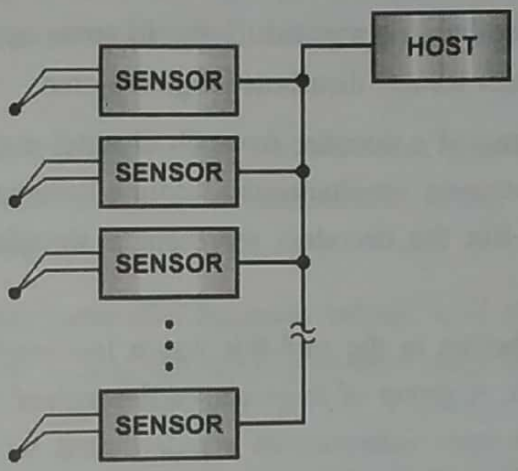
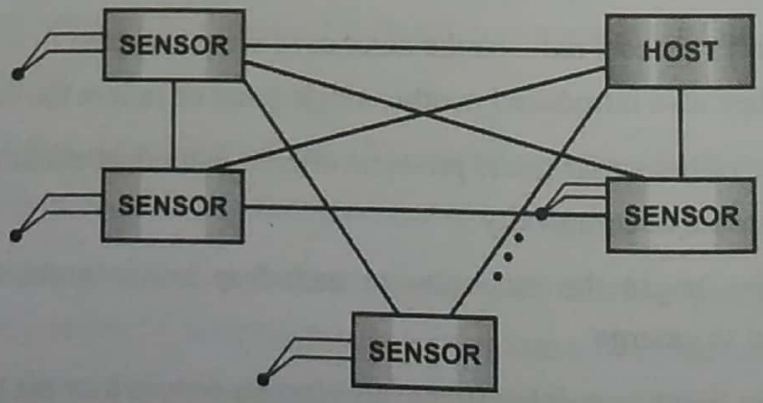


Fig. 2.5.6 : Multidrop Network

- In a web topology, all nodes are potentially connected to all other nodes. Connectivity among a large collection of sensors gets complex because all nodes must have a connection to all other nodes. Some connections can be eliminated by using repeaters and routers to make virtual connections. The World Wide Web is a good example of this topology
- Multidrop buses began to appear in the late 70s and early 80s. One of these, Modbus from Modicon (Schneider Auto mation, North Andover, Massa chusetts), led the way into the industrial sphere, followed by several proprietary and open buses (e.g., the Manufacturing Auto mation Protocol, QBus, and VME Bus).
- The emergence of intelligent sensors and microcomputers capable of operating in industrial environments irrevocably changed the sensor network landscape.
- Multidrop networks (buses) reduced the number of wires required to connect field devices to the host, but they also introduced another single point of failure the cable.
- Several suppliers of industrial-grade products offered redundant cabling designs, but these came with an increase in complexity .
- Once the industry began the migration to multidrop buses, problems associated with digitization began to emerge.
- With the previous point-to-point systems, digitization occurred in the host, where a single clock could be used to time stamp when the analog signals from multiple sensors were acquired.

- With the distributed intelligence required to implement a multidrop network, synchronization of clocks became a critical issue in some applications. This remains an important design parameter for any distributed digital system.
- An architecture consisting of a decoder for each channel and a direct-sequence spread-spectrum receiver can perform simultaneous sampling because the same baseband signal goes to each decoder. But the decoders represent a significant cost, power, and size limitation.
- The introduction of Ethernet in the mid-80s was a landmark in standardization, if not technological innovation. A group of large companies agreed that the future of computer networking required an open interconnect standard that would allow multiple-vendor systems to work together with minimal difficulty.
- Researchers looked closely at the carrier sense multiple access with collision detection (CSMA/CD) protocol when they investigated the behavior of networks under stress. But they considered most industrial applications too time critical for such a nondeterministic protocol. Now, fifteen years later, most factories have converted their shop floor networks to Ethernet because it is the best compromise between cost and performance. Many companies now offer solutions that use Ethernet to implement suitable robust industrial networks.
- Wireless systems use the same types of protocols to implement multidrop topologies, simulating hard-wired connections with RF links. The IEEE-802.11 standard was the first wireless standard that promised to bring the interoperability of Ethernet connectivity to wireless networks. Many of these, however, are not compatible at the over-the-air level.

☞ Web Networks



(1B16)**Fig. 2.5.7 : Web Network**

- Simultaneous sampling is more difficult with this receiver architecture. The selected channel codes can be stored and stepped through so that each channel's data gets to the data system bus.
- The promise of the web topology (i.e., when all nodes are connected all the time) had to wait until vendors developed a way to interconnect nodes without the required wiring connections.
- A network of any appreciable size becomes infeasible if all wires must be connected specifically for the network.Early star topologies were successful as long as the star wasn't too large.
- The World Wide Web illustrates what is possible, though, if you can use wiring that is already in place. The telephone network provides the available connectivity in most parts of the country, although at less than suitable speeds in many locations.
- The advantages of web connectivity for sensor networks become clear as the level of intelligence in each sensor increases.
- Cooperating sensors can form a temporary configuration that provides sufficient capacity to replace the host. Self-hosting networks then become self-configuring and finally, years from now, perhaps even self-aware.
- But several problems remain and are the topic of significant research, such as size and power consumption reduction, throughput and performance during transmissions, and algorithms for allocating priorities and authority.
- In a wireless web network, individual nodes have the potential of being constantly connected (physically) with many other nodes in the network. How the network is configured at any instant becomes a matter of how the software configures it. In a code division multiple access (CDMA) network, the radios can receive all channels at once.
- The architecture suggested in Fig.2.4.8 requires a separate decoder for each channel. This requires hardware to be dedicated to channels that may not be currently important but could be required later. Fig. 2.4.9 eliminates the need for dedicated hardware but introduces the problem of simultaneous sampling.
- The decoder-per-channel implementation samples the data stream looking for a particular channel code embedded in the chip stream.

- The single decoder will decode a new data stream for each channel unless the data stream is stored and decoded over and over with different candidate codes for each channel. Both implementations represent a compromise and should be implemented carefully, depending on the application.
- Network routing is a serious concern in web architectures. Because all nodes can't reach all other nodes in a single hop, a repeating mechanism is required.
- The assigned input and output channels dictate to each node which signals are meant for its own use and which should be passed on to the next node. The routing is one of the things that makes web architectures more complicated to implement than the others.
- In sensor or mobile phone networks, nodes can come and go frequently. How the network responds to the reconfiguration has a severe impact on performance and reliability.
- Mobile ad hoc networking is a hot topic in the research community because reconfiguring on the fly makes all networks better. Without this technology, sensor networks will be severely limited in harsh environments, where connections can change quickly as the RF environment changes.

So What?

- Network topologies usually work best when they map closely to the topology of the application. If the application looks hierarchical, then a hierarchical (point-to-point or multidrop) topology might be most suitable. But if the application looks like a collection of peers interacting and cooperating, then a web architecture might work best.
- The potential for web connectivity in the sensor world seems most tempting. The dynamic nature provides the opportunity for cooperating sensors to form smart clusters that can work together to solve a problem, then reorganize to solve the next one. As the hardware and software technologies mature, you'll see more and more web implementations showing up on factory floors. Watch for them.

NOTES

2.6 ENABLING IOT TECHNOLOGIES

GQ. Explain different Enabling IOT Technologies. **(6 Marks)**

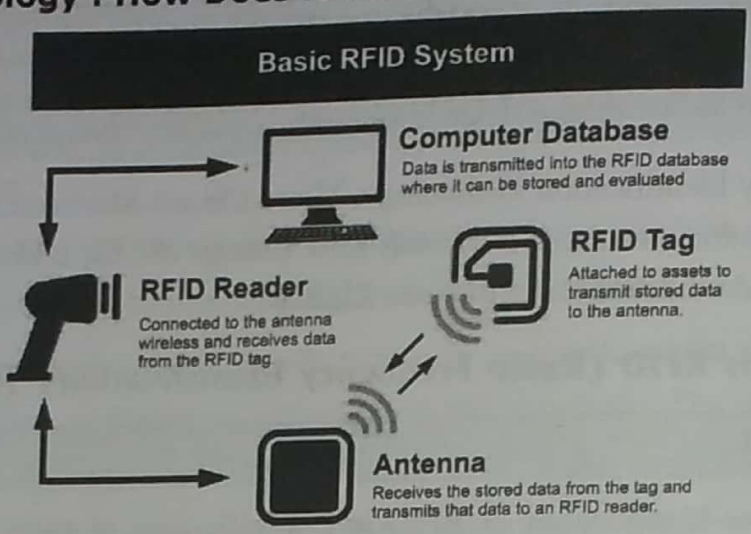
Radio Frequency Identification Technology, Micro Electro-Mechanical Systems (MEMS), NFC (Near Field Communication), Bluetooth Low Energy (BLE), LTE-A (LTE Advanced), IEEE 802.15.4–Standardization and Alliances, ZigBee.

2.6.1 What is RFID (Radio Frequency Identification) Technology?

GQ. Explain RFID. **(4 Marks)**

- Radio Frequency Identification or RFID is a specific type of radio technology that uses radio waves to identify tags attached to an object and thus identify the object.
- The tag contains a transceiver chip which is triggered by the electromagnetic wave from the RFID reader and transmits an identification number back to the reader. The identification number is then used for the inventory of the objects with tags.
- Tags can be passive or active. Passive tags are only powered by the incident electromagnetic wave from the reader and thus have a shorter operating range. Active tags are powered by a battery and can have greater range, up to hundreds of meters. With the use of wireless technology, RFID tags do not need a direct line-of-sight to the RFID reader, which brings some significant advantages compared to the barcode scanners widely used in the industry today.
- The RFID tag can be embedded or hidden in the object, and several tags can be identified at the same time by a single reader. A barcode scanner has to 'see' a barcode to gather data.
- RFID is used in many applications and industries, including pharma, retail, agriculture and medical care, as well as tracking vehicles, pets, and livestock. For example, an object with an embedded RFID tag that is moving through a production line or a warehouse equipped with RFID readers, can be scanned at different production stations and thus its progress can be automatically tracked.
- The technology has continued to improve over the years, and the cost of implementing and using an RFID system has continued to decrease, making RFID a cost-effective and efficient alternative to conventional optical scanning.
- Standard specifications have been developed for RFID technology, addressing security and privacy concerns. Such standards use on-chip cryptography methods for untraceability and tag and reader authentication using digital signature data.

RFID Technology : How Does it Work?



(1B19)**Fig. 2.6.1 : RFID**

Source

GQ. What are the Main Components of RFID Technology?

(1) Tags

- RFID tags are what stores and transmits the data that needs to be deciphered. The tags can be attached to assets to send data to the antenna.
- The microchip embedded in the tag is what stores the tag's ID and programmable data related to the asset. This stored data is then transferred to the reader through antennas.

(2) Antennas

- Antennas are necessary elements in an RFID system because they transmit the RFID tag's data to the reader.
- Without some type of RFID antenna, whether integrated or standalone, the RFID reader cannot correctly send and receive signals to RFID tags.

(3) Readers

- RFID readers are connected to the antenna and receive data from the RFID tag. The reader is what receives and converts the radio waves into digital data on a computer database.
- There are two types of readers. There are Fixed Readers and Mobile Readers. Fixed readers are typically mounted to walls or other objects and stay in one location to read data stored in a tag. Mobile readers can be installed or carried anywhere it is needed.

(4) Computer Database

- The RFID system requires a computer database to process data stored in tags.
- This software can program tags, manage devices and data, remote monitoring and hardware configuration.

☞ RFID Tags : Categories, Frequencies, and Applications

RFID transmits data to a reader through different frequencies of electromagnetic fields.

RFID tags are categorised according to the frequency at which they are designed to operate. There are three major frequency ranges that RFID tags operate.

1. Low-Frequency (LF) Tags
2. High-Frequency (HF) Tags
3. Ultra-High Frequency (UHF) Tags - passive and active

1. Low-Frequency Tags (LF)

- The primary frequency range of 125kHz – 134kHz
- Can read a span of a few inches
- Lowest data transfer rate among all the RFID frequencies
- Store a small amount of data
- LF Applications – Animal Tracking, Access Control, Car Key-Fob, Asset Tracking, and Healthcare

2. High-Frequency Tags (HF)

Most widely used around the world

- The primary frequency range of 13.56MHz
- Read range: 30 cm
- The capability of reading multiple tags simultaneously
- Can store up to 4k of data
- Easily read while attached to objects containing water, tissues, metal, wood, and liquids.
- HF Applications – Library Books, Personal ID Cards, Airline Baggage, and Credit Cards

3. Ultra-High Frequency Tags (UHF)

- There are two types of tags that use different frequencies under UHF RFID.
- UHF Passive Tags - use energy from the RFID reader
  - The primary frequency range: 860MHz – 960MHz
  - Read Range: 25 meters
  - High data transmission rate
  - Wide variety of tag sizes
- UHF Passive Tag Applications – Supply Chain Tracking, Manufacturing, Pharmaceuticals and Electronic Tolling
- UHF Active Tags - battery operated
  - The primary frequency range: 433MHz
  - Read Range: 30 - 100+ meters
  - Large memory capacity
  - High data transfer rate
- UHF Active Tag Applications – Vehicle Tracking, Auto Manufacturing, and Construction

☞ Pros and Cons of RFID

- RFID can be used to reduce production costs and optimise operations.

However, If you are considering RFID technology to streamline production, track, and analyze data collection and more, there are pros and cons to weigh.

Pros of RFID in Manufacturing	Cons of RFID in Manufacturing
Does not require line of sight to be scanned or identified	Initial system costs are higher than with conventional optical scanning
Readers can read hundreds of tags within seconds	Partner companies may not use the same technology causing a disconnect
Tags can be rewritten, and reused	vulnerability to software attacks (viruses and security breaches)
Tag data is encrypted and can also be locked for extra security	If a tag does become damaged, a redundant system is required

Pros of RFID in Manufacturing	Cons of RFID in Manufacturing
Tags are durable and can withstand impact	Privacy concerns
Tags can have additional information printed on them such as instructions. barcodes, or company names	
RFID systems can be susceptible to certain materials and environmental factors	
Systems can be integrated with other internal systems or processes	
Tags can hold more data than other types of tags or labels	

- The most significant benefit of using RFID technology over other methods in manufacturing is that it does not need a line of sight to be scanned or identified. This gives more flexibility to the production and supply chain process.

2.6.2 Micro-electromechanical Systems (MEMS)

GQ. What is MEMS?

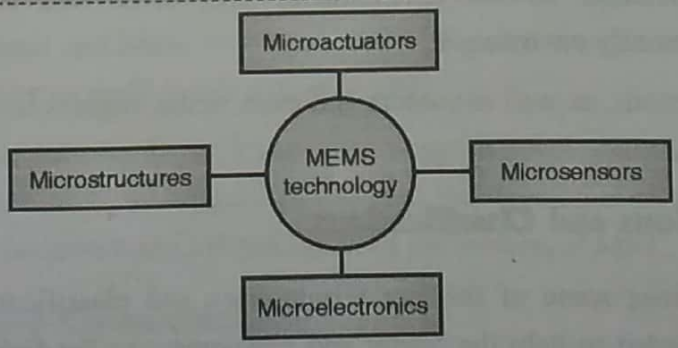


Fig.2.6.2 : Schematic illustration of MEMS components

- Micro-electromechanical systems (MEMS) is a process technology used to create tiny integrated devices or systems that combine mechanical and electrical components.
- They are fabricated using integrated circuit (IC) batch processing techniques and can range in size from a few micrometers to millimetres. These devices (or systems) have the ability to sense, control and actuate on the micro scale, and generate effects on the macro scale.

- An Introduction to MEMS Prime Faraday Technology Watch - January 20022MEMS, an acronym that originated in the United States, is also referred to as Microsystems Technology (MST) in Europe and Micromachines in Japan.
- Regardless of terminology, the uniting factor of a MEMS device is in the way it is made. While the device electronics are fabricated using 'computer chip' IC technology, the micromechanical components are fabricated by sophisticated manipulations of silicon and other substrates using micromachining processes.
- Processes such as bulk and surface micromachining, as well as High-Aspect-Ratio Micromachining (HARM) selectively remove parts of the silicon or add additional structural layers to form the mechanical and electromechanical components.
- While integrated circuits are designed to exploit the electrical properties of silicon, MEMS takes advantage of either silicon's mechanical properties or both its electrical and mechanical properties.
- In the most general form, MEMS consist of mechanical microstructures, microsensors, microactuators and microelectronics, all integrated onto the same silicon chip. This is shown schematically in Fig. 2.6.2.
- Microsensors detect changes in the system's environment by measuring mechanical, thermal, magnetic, chemical or electromagnetic information or phenomena. Microelectronics process this information and signal the microactuators to react and create some form of changes to the environment. MEMS devices are very small; their components are usually microscopic.
- Levers, gears, pistons, as well as motors and even steam engines have all been fabricated by MEMS .

2.6.3 Definitions and Classifications.

- This section defines some of the key terminology and classifications associated with MEMS. It is intended to help the reader and newcomers to the field of micromachining become familiar with some of the more common terms. A more detailed glossary of terms has been included in Appendix A.
- Fig. 2.6.3 illustrates the classifications of microsystems technology (MST). Although MEMS is also referred to as MST, strictly speaking, MEMS is a process technology used to create these tiny mechanical devices or systems, and as a result, it is a subset of MST.

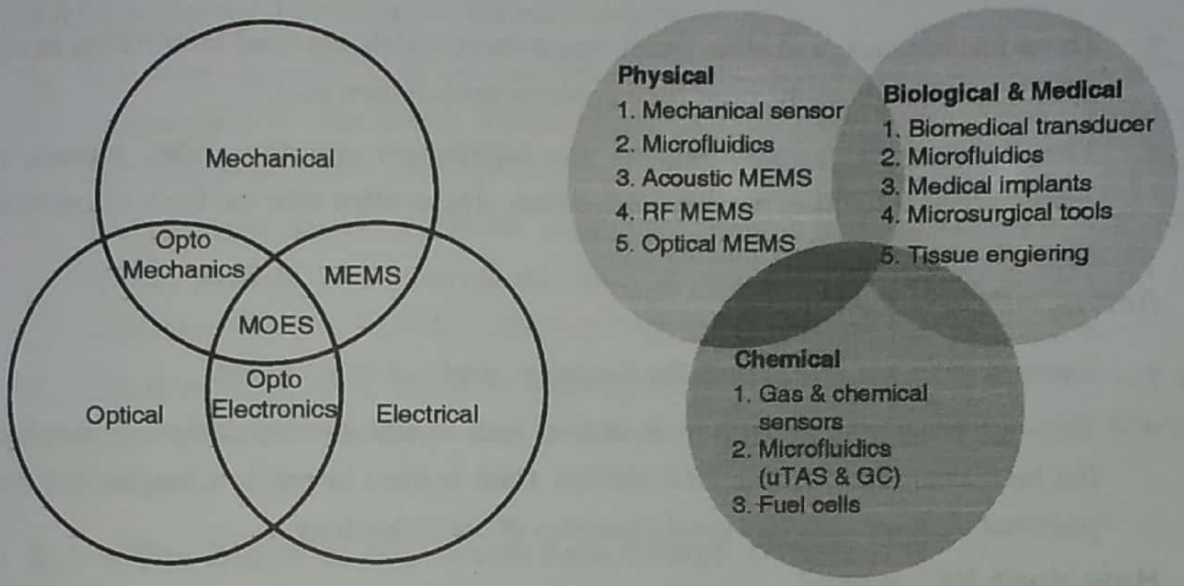


Fig. 2.6.3 : Classifications of microsystems technology .

- An Introduction to MEMS Prime Faraday Technology Watch – January 20024Micro-optoelectromechanical systems (MOEMS) is also a subset of MST and together with MEMS forms the specialized technology fields using miniaturized combinations of optics, electronics and mechanics. Both their microsystems incorporate the use of microelectronics batch processing techniques for their design and fabrication.
- There are considerable overlaps between fields in terms of their integrating technology and their applications and hence it is extremely difficult to categorise MEMS devices in terms of sensing domain and/or their subset of MST.
- The real difference between MEMS and MST is that MEMS tends to use semiconductor processes to create a mechanical part. In contrast, the deposition of a material on silicon for example, does not constitute MEMS but is an application of MST.

2.6.4 Near Field Communication (NFC)

GQ. Short note on NFC. **(2 Marks)**

NFC stands for Near Field Communication. It enables short range communication between compatible devices. At least one transmitting device and another receiving device is needed to transmit the signal. Many devices can use the NFC standard and are considered either passive or active.

So NFC devices can be classified into 2 types:

1. Passive NFC devices

- These include tags, and other small transmitters which can send information to other NFC devices without the need for a power source of their own.
- These devices don't really process any information sent from other sources, and cannot connect to other passive components. These often take the form of interactive signs on walls or advertisements.

2. Active NFC devices

- These devices are able to both the things i.e. send and receive data.
- They can communicate with each other as well as with passive devices. Smartphones the best example of active NFC device. Card readers in public transport and touch payment terminals are also good examples of the technology.

☞ How does NFC work?

- Like other wireless signals Bluetooth and WiFi, NFC works on the principle of sending information over radio waves.
- Near Field Communication is another standard for wireless data transition which means devices must adhere to certain specifications in order to communicate with each other properly.
- The technology used in NFC is based on older technology which is the RFID (Radio-frequency identification) that used electromagnetic induction in order to transmit information.
- This creates one major difference between NFC and Bluetooth/WiFi. NFC can be used to induce electric currents within passive components rather than just send data.
- This means that their own power supply is not required by passive devices. Instead they can be powered by the electromagnetic field produced by an active NFC component when it comes into range.
- NFC technology unfortunately does not command enough inductance to charge our smartphones, but QI charging is based on the same principle.
- The transmission frequency is 13.56 megahertz for data across NFC. Data can be sent at either 106, 212, or 424 kilobits per second which is quick enough for a range of data transfers like contact details to swapping pictures and music.

- The NFC standard currently has three distinct modes of operation to determine what sort of information will be exchanged between devices.
  1. The most common used in smartphones is the peer-to-peer mode. Exchange of various piece of information is allowed between 2 devices. In this mode both devices switch between active when sending data and passive when receiving.
  2. The second mode i.e. read/write mode is a one-way data transmission. The active device, possibly your smartphone, links up with another device in order to read information from it. NFC advertisement tags use this mode.
  3. The third mode of operation is card emulation. The NFC device can function as a smart or contactless credit card and make payments or tap into public transport system

2.6.5 The Basics of Bluetooth Low Energy (BLE)

GQ. Write short note on BLE. **(2 Marks)**

- Bluetooth Low Energy (BLE) is a low power wireless technology used for connecting devices with each other. BLE operates in the 2.4 GHz ISM (Industrial, Scientific, and Medical) band, and is targeted towards applications that need to consume less power and may need to run on batteries for longer periods of time months, and even years.
- Bluetooth started as a short-distance cable replacement technology. For example, to replace wires in devices such as a mouse, keyboard, or a PC communicating with a Personal Digital Assistant (PDA) which were popular in the late 1990s and early 2000s.
- The first official version of Bluetooth was released by Ericsson in 1994, named after King Harald "Bluetooth" Gormsson of Denmark who helped unify warring factions in the 10th century CE.
- Bluetooth Low Energy (BLE), however, was introduced in the 4.0 version of the Bluetooth specification in 2010.
- The original Bluetooth defined in the previous versions is referred to as Bluetooth Classic. BLE was not an upgrade to the original Bluetooth: Bluetooth Classic, but rather it's a new technology that utilizes the Bluetooth brand but focuses on the Internet of Things (IoT) applications where small amounts of data are transferred at lower speeds.
- It's important to note that there's a big difference between Bluetooth Classic and Bluetooth Low Energy in terms of technical specification, implementation and the types of applications they're each suitable for.

- Some of the notable differences include :
  (1) **Bluetooth Classic :** used for streaming applications such as audio streaming and file transfers.
  (2) **BLE :** used for sensor data, control of devices, and low-bandwidth applications.
  (3) **BLE :** low power, low duty data cycles.
  (4) **Bluetooth Classic :** not optimized for low power, has a higher data rate.
  (5) **BLE :** Operates over 40 RF (Radio Frequency) channels.
  (6) **Bluetooth Classic :** Operates over 79 RF channels.
  (7) **BLE :** connections are much quicker (discovery occurs on 3 channels).
  (8) **Bluetooth Classic :** discovery on 32 channels, leading to slower connections.
- BLE has gone through some major revisions and changes in the short time since its official release in 2010, with the most recent major update being Bluetooth 5 in December 2016.
- Bluetooth 5.0 introduced many important upgrades to the Bluetooth specification, most of which were focused on BLE.
- Some of the most important enhancements include twice the speed, four times the range, and eight times the advertising data capacity.

☞ Advantages and Disadvantages

Every technology has its own benefits and limitations, and BLE is no exception. It's important to know these pros and cons to be able to determine whether BLE is suitable for your specific application and use case or not.

☞ Benefits of BLE

1. Lower power consumption even when compared to other low power technologies. BLE achieves the optimized and low power consumption by keeping the radio off as much as possible and sending small amounts of data at low transfer speeds.
2. No cost to access the official specification documents. With most other wireless protocols and technologies, you would have to be a member of the official group or consortium for that technology in order to access the specification.
3. Lower cost of modules and chipsets, even when compared to other similar technologies.

4. Most importantly, its existence in most smartphones in the market.

☞ Limitations of BLE

(1) **Data Throughput :** the data throughput of BLE is limited by the physical radio layer (PHY) data rate, which is the rate at which the radio transmits data.

(2) This rate depends on the Bluetooth version used. For Bluetooth 4.2 and earlier, the rate is fixed at 1 Mbps. For Bluetooth 5 and later, however, the rate varies depending on the mode and PHY used. The rate can be 1 Mbps like earlier versions, or 2 Mbps when utilizing the high-speed feature.

Range

- Bluetooth Low Energy (and Bluetooth in general) was designed for short range applications and hence its range of operation is limited.
- There are a few factors that limit the range of BLE :
  (1) BLE operates in the 2.4 GHz ISM spectrum which is greatly affected by obstacles that exist all around us such as metal objects, walls, and water (especially human bodies)
  (2) Performance and design of the antenna of the BLE device.
  (3) Physical enclosure of the device.
  (4) Device orientation.
- Gateway Requirement for Internet Connectivity: In order to transfer data from a BLE-only device to the Internet, another BLE device that has an IP connection is needed to receive this data and then, in turn, relay it to another IP device (or to the Internet).

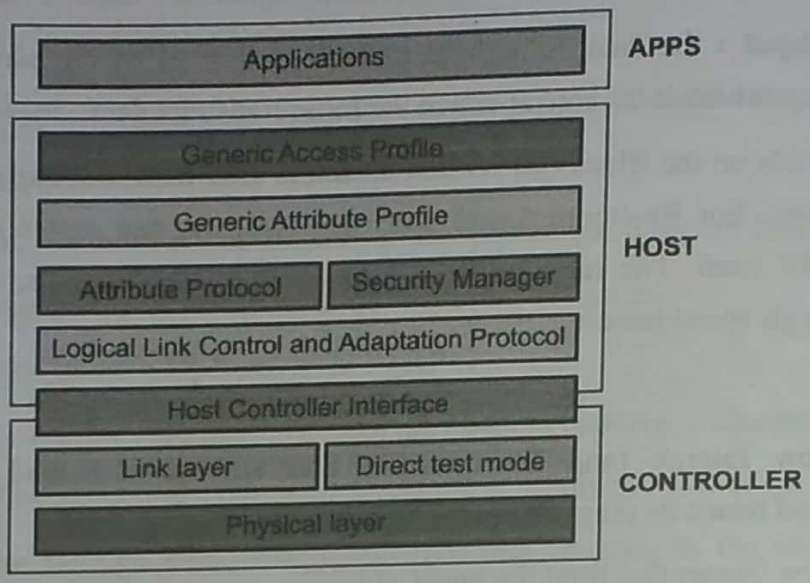
☞ Bluetooth Low Energy Architecture

GQ. Explain BLE Architecture. **(4 Marks)**

Here's a diagram showing the different levels of the architecture of BLE :

NOTES

Bluthooth Low Energy Architecture

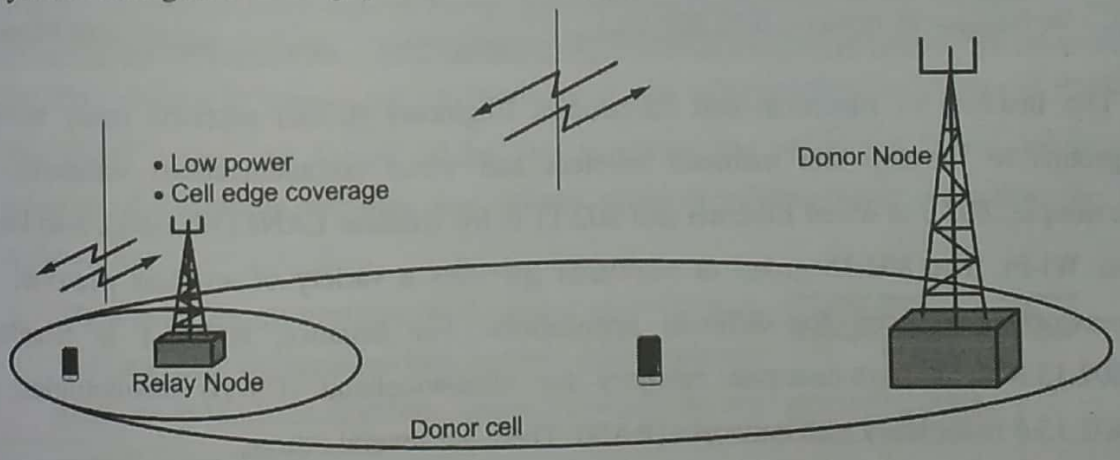


(1B20)**Fig. 2.6.5 : BLE Architecture**

- The good thing is that, as a developer looking to develop BLE applications, you won't have to worry much about the layers below the Security Manager and Attribute Protocol.
- But lets at least cover the definitions of these layers:
- The physical layer (PHY) refers to the physical radio used for communication and for modulating/ demodulating the data. It operates in the ISM band (2.4 GHz spectrum).
- The Link Layer is the layer that interfaces with the Physical Layer (Radio) and provides the higher levels an abstraction and a way to interact with the radio (through an intermediary level called the HCI layer which we'll discuss shortly).
- It is responsible for managing the state of the radio as well as the timing requirements for adhering to the Bluetooth Low Energy specification.
- Direct Test Mode : the purpose of this mode is to test the operation of the radio at the physical level (such as transmission power, receiver sensitivity, etc.).
- The Host Controller Interface (HCI) layer is a standard protocol defined by the Bluetooth specification that allows the Host layer to communicate with the Controller layer. These layers could exist on separate chips, or they could exist on the same chip.
- The Logical Link Control and Adaptation Protocol (L2CAP) layer acts as a protocol multiplexing layer. It takes multiple protocols from the upper layers and places them in standard BLE packets that are passed down to the lower layers beneath it.

2.6.6 LTE-A or LTE Advanced

- LTE-A or LTE Advanced is the upgraded version of LTE, which increases the stability, bandwidth, and speed of traditional LTE networks.
- According to 3GPP- "The main new functionalities introduced in LTE-Advanced are Carrier Aggregation (CA), enhanced use of multi-antenna techniques (MIMO) and support for Relay Nodes (RN)".
- Carrier Aggregation (CA) is a feature of LTE-Advanced that allows mobile operators to combine two or more LTE carriers into single data channel to increase the capacity of the network and the data rates by exploiting fragmented spectrum allocations. For more information about Carrier Aggregation, click here.
- Multi-Input Multi-Output (MIMO) technology is the use of multiple receive and transmit antennas to establish a communications link between two, or more, communications systems with greater throughput than would be possible with a single antenna system.



(1B22)**Fig. 2.6.6 : MIMO Spatial Multiplexing**

- Relay Nodes are low powered base stations that increases the coverage and capacity at cell edges. They also provide coverage in the areas where there is no fiber connection.

LTE-Advanced features

- Increased peak data rate: Downlink 3 Gbps, Uplink 1.5 Gbps
- Higher spectral efficiency: Uplink 16bps/Hz, Downlink 30 bps/Hz
- Increased number of simultaneously active subscribers
- Improved performance at cell edges, e.g. for Downlink 2x2 MIMO by at least 2.40 bps/Hz/cell

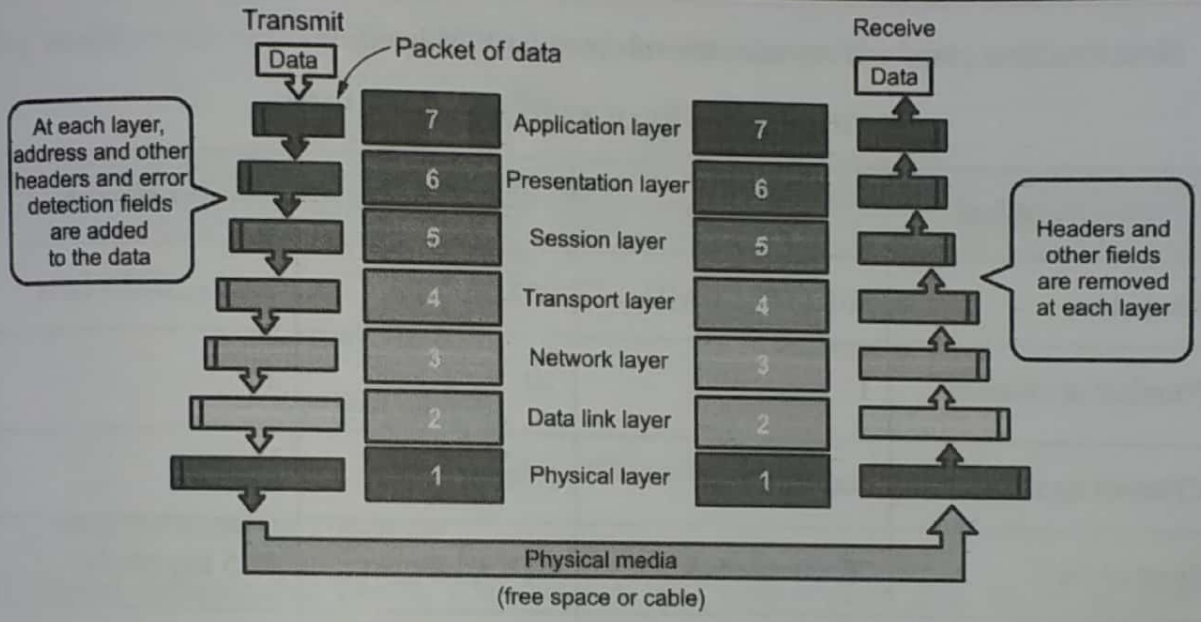
☞ Comparison of LTE-A with other technologies

	WCDMA (UMTS)	HSPA+	LTE	LTE-A
Downlink speed	384 Kbps	1-28 Mbps	10 – 100 Mbps	1 Gbps
Uplink speed	128 Kbps	11 Mbps	5 – 50 Mbps	500 Mbps
Latency	150 ms	50ms (max)	~10 ms	less than 5 ms
3GPP Releases	Rel 99/4	Rel 7	Rel 8	Rel 10
Access Methodology	CDMA	CDMA	OFDMA / SC-FDMA	OFDMA / SC-FDMA

2.6.7 IEEE 802.15.4

GQ. Write a short note on IEEE 802.15.4. **(2 Marks)**

- The Institute of Electrical and Electronics Engineers (IEEE) supports many working groups to develop and maintain wireless and wired communications standards. For example, 802.3 is wired Ethernet and 802.11 is for wireless LANs (WLANs), also known as Wi-Fi. The 802.15 group of standards specifies a variety of wireless personal area networks (WPANs) for different applications. For instance, 802.15.1 is Bluetooth, 802.15.3 is a high-data-rate category for ultra-wideband (UWB) technologies, and 802.15.6 is for body area networks (BAN). There are several others.
- The 802.15.4 category is probably the largest standard for low-data-rate WPANs. It has many subcategories. The 802.15.4 category was developed for low-data-rate monitor and control applications and extended-life low-power-consumption uses. The basic standard with the most recent updates and enhancements is 802.15.4a/b, with 802.15.4c for China, 802.15.4d for Japan, 802.15.4e for industrial applications, 802.15.4f for active (battery powered) radio-frequency identification (RFID) uses, and 802.15.4g for smart utility networks (SUNs) for monitoring the Smart Grid. All of these special versions use the same base radio technology and protocol as defined in 802.15.4a/b.



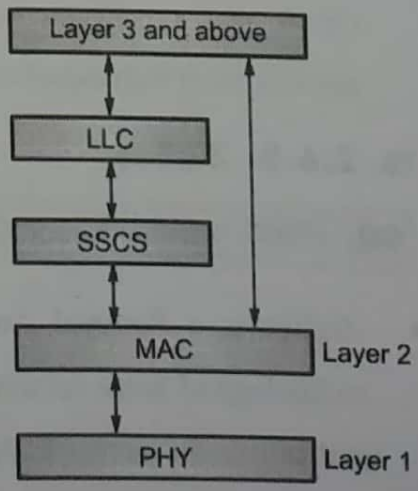
(1B23)**Fig. 2.6.7 : IEEE 802.15.4 Architecture**

- The 802.15.4 standard defines the physical layer (PHY) and media access control (MAC) layer of the Open Systems Interconnection (OSI) model of network operation *(Fig. 2.6.7)*. The PHY defines frequency, power, modulation, and other wireless conditions of the link.
- The MAC defines the format of the data handling. The remaining layers define other measures for handing the data and related protocol enhancements including the final application.

1. Most networking systems, both wired and wireless, use the OSI communications model. Most systems also use at least the first four layers, but many do not use all seven layers.

   More specifically, Fig. 2.6.8 shows the layer 1 and layer 2 details of 802.15.4.

2. The 802.15.4 standard uses only the first two layers plus the logical link control (LLC) and service specific convergence sub-layer (SSCS) additions to communicate with all upper layers as defined by additional standards.



(1B24)**Fig.2.6.8**

- The goal of the standard is to provide a base format to which other protocols and features could be added by way of the upper layers (layers 3 through 7). While three frequency assignments are available, the 2.4-GHz band is by far the most widely used *(see the table)*.

Most available chips and modules use this popular ISM band.

OPTIONS FOR FREQUENCY ASSIGNMENTS

Geographical	Europe	Americas	Worldwide
Frequency	868 to 868.6 MHz	902 to9.28	2.4 to 2.4835 GHz
Number at channels	1	10	16
Channel bandwidth	600 kHz	2 MHz	5 MHz
Symbol rate	20 ksymbols/s	40 k symbols/s	62.5 ksymbols/s
Data rate	20 kbits/s	40 kbits/s	250 kbits/s
Modulation	BPSK	BPSK	Q-QPSK

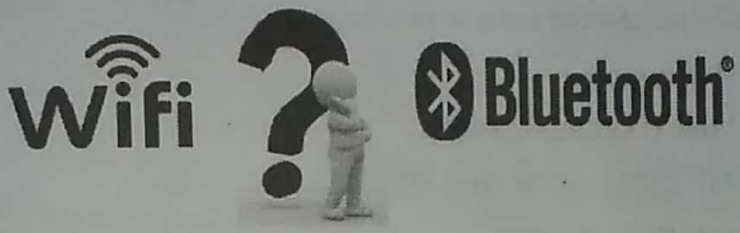
- The standard uses direct sequence spread spectrum (DSSS) modulation. It is highly tolerant of noise and interference and offers coding gain to improve link reliability.
- Standard binary phase-shift keying (BPSK) is used in the two low-speed versions, while offset-quadrature phase-shift keying (O-QPSK) is used for the higher-data-rate version. O-QPSK has a constant wave envelope meaning that more efficient non-linear power amplification techniques can be used to minimize power consumption.

2.6.8 ZigBee

GQ. Write a short note on ZigBee.

- ZigBee is a Personal Area Network task group with low rate task group 4. It is a technology of home networking. ZigBee is a technological standard created for controlling and sensor the network. As we know that ZigBee is the Personal Area network of task group 4 so it is based on IEEE 802.14.4 and is created by Zigbee Alliance.
- ZigBee is a standard that addresses the need of very low-cost implementation of Low power devices with Low data rate for short-range wireless communications.

Why another short-range communication standard?



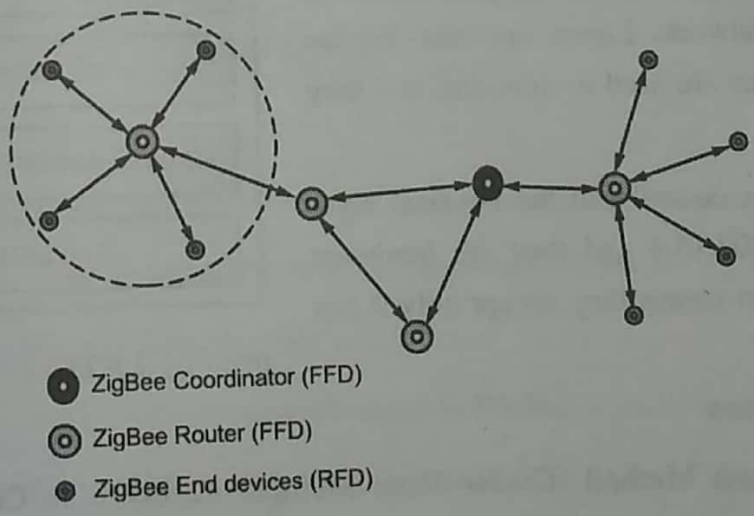
(1B25)**Fig. 2.6.9 : Wifi and Bluetooth**

☞ Types of ZigBee Devices

(1) **Zigbee Coordinator Device :** It communicates with routers. This device is used for connecting the devices.

(2) **Zigbee Router :** It is used for passing the data between devices.

(3) **Zigbee End Device :** It is the device that is going to be controlled



(1B26)**Fig. 2.6.10**

☞ General Characteristics of Zigbee Standard

- Low Power Consumption
- Low Data Rate (20- 250 kbps)
- Short-Range (75-100 meters)
- Network Join Time (~ 30 msec)
- Support Small and Large Networks (up to 65000 devices (Theory); 240 devices (Practically))
- Low Cost of Products and Cheap Implementation (Open Source Protocol)

☞ Operating Frequency Bands

(Only one channel will be selected for use in a network):

Channel 0 : 868 MHz (Europe)

Channel 1-10 : 915 MHz (US and Australia)

Channel 11-26 : 2.4 GHz (Across the World)

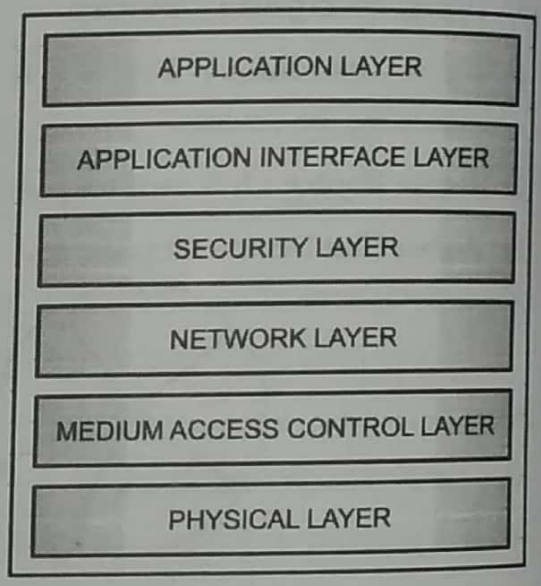
☞ Zigbee Network Topologies

- Star Topology (ZigBee Smart Energy)
- Mesh Topology (Self Healing Process)
- Tree Topology

☞ Architecture of Zigbee

Zigbee architecture is a combination of 6 layers.

- The Application layer is present at the user level.
- The Application Interface Layer, Security Layer, and Network Layer are the Zigbee Alliance and they are used to store data and they use the stack.
- Medium Access control and the Physical layer are the IEEE 802.15.4 and they are hardware which are silicon means they accept only 0 and 1.



(1B27)**Fig. 2.6.11 : Zigbee Architecture**

☞ Channel Access

1. **Contention Based Method** (Carrier-Sense Multiple Access With Collision Avoidance Mechanism)
2. **Contention Free Method** (Coordinator dedicates specific time slot to each device (Guaranteed Time Slot (GTS)))

☞ Zigbee Applications

1. Home Automation
2. Medical Data Collection
3. Industrial Control Systems

...Chapter Ends...

❑❑❑

MODULE 3

CHAPTER 3

The Core IoT Functional Stack

Syllabus

Layer 1 - Things : Sensors and Actuators Layer, Layer 2 - Communications Network Layer, Access Network Sublayer, Gateways and Backhaul Sublayer, Network Transport Sublayer, IoT Network Management Sublayer, Layer 3 - Applications and Analytics Layer, Analytics Vs. Control Applications, Data Vs. Network Analytics, Data Analytics Vs. Business Benefits, Smart Services.

3.1 LAYER 1 : THINGS: SENSORS AND ACTUATORS LAYER

GQ. Explain things: Sensors and Actuators layer ? **(4 Marks)**

"**Smart Objects : The 'Things' in IoT,**" provides more in-depth information about smart objects. From an architectural standpoint, the variety of smart object types, shapes, and needs drive the variety of IoT protocols and architectures. One architectural classification could be :

(1) **Battery-powered or power-connected :** This classification is based on whether the object carries its own energy supply or receives continuous power from an external power source.

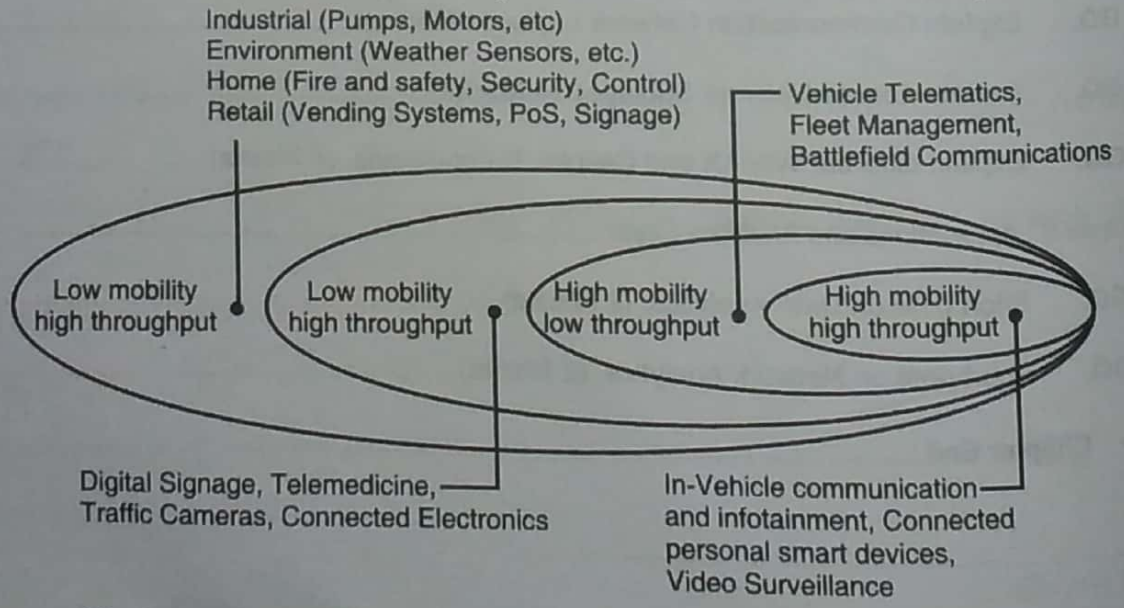
(2) **Mobile or static :** This classification is based on whether the "thing" should move or always stay at the same location. A sensor may be mobile because it is moved from one object to another or because it is attached to a moving.

(3) **Low or high reporting frequency :** This classification is based on how often the object should report monitored parameters. A rust sensor may report values once a month. A motion sensor may report acceleration several hundred times per second.

(4) **Simple or rich data :** This classification is based on the quantity of data exchanged at each report cycle.

(5) **Report range :** This classification is based on the distance at which the gateway is located. For example, for your fitness band to communicate with your phone, it needs to be located a few meters away at most.

(6) **Object density per cell :** This classification is based on the number of smart objects (with a similar need to communicate) over a given area, connected to the same gateway.



(1C1) **Fig. 3.1.1 : Example of Sensor Applications Based Mobility and Throughput**

Fig. 3.1.1 provides some examples of applications matching the combination of mobility and throughput requirements.

3.2 LAYER 2 : COMMUNICATIONS NETWORK LAYER

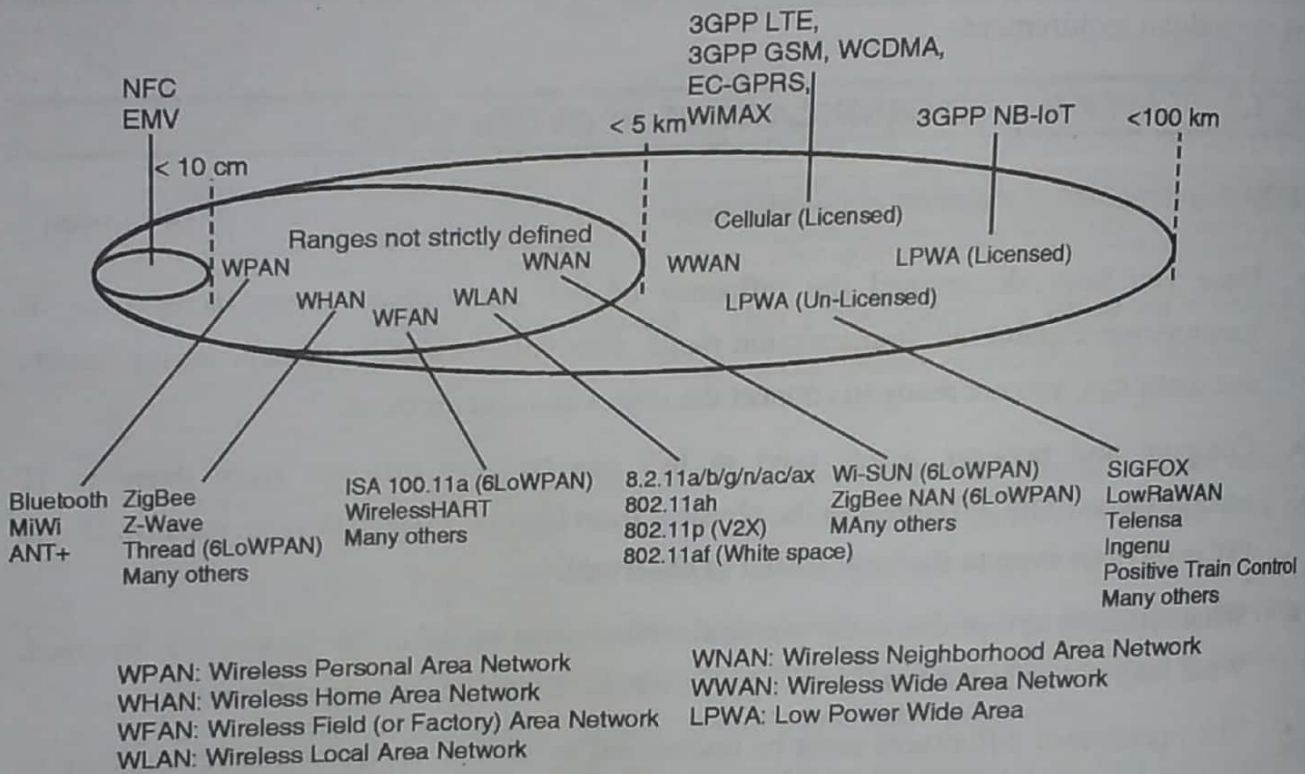
GQ. Explain Communication Network Layer. **(4 Marks)**

- Once you have determined the influence of the smart object form factor over its transmission capabilities (transmission range, data volume and frequency, sensor density and mobility), you are ready to connect the object and communicate.
- Compute and network assets used in IoT can be very different from those in IT environments. The difference in the physical form factors between devices used by IT and OT is obvious even to the most casual of observers.
- What typically drives this is the physical environment in which the devices are deployed. What may not be as inherently obvious, however, is their operational differences.
- The operational differences must be understood in order to apply the correct handling to secure the target assets.

Access Network Sublayer

GQ. Explain Access Network Sublayer. **(4 Marks)**

- There is a direct relationship between the IoT network technology you choose and the type of connectivity topology this technology allows.
- Each technology was designed with a certain number of use cases in mind (what to connect, where to connect, how much data to transport at what interval and over what distance).
- These use cases determined the frequency band that was expected to be most suitable, the frame structure matching the expected data pattern (packet size and communication intervals), and the possible topologies that these use cases illustrate.
- One key parameter determining the choice of access technology is the range between the smart object and the information collector.
- Fig. 3.2.1 lists some access technologies you may encounter in the IoT world and the expected transmission distances.



(1C2)**Fig. 3.2.1 : Access Technologies and Distances**

Range estimates are grouped by category names that illustrate the environment or the vertical where data collection over that range is expected. Common groups are as follows :

(1) **PAN (personal area network) :** Scale of a few meters. This is the personal space around a person. A common wireless technology for this scale is Bluetooth.

(2) **HAN (home area network) :** Scale of a few tens of meters. At this scale, common wireless technologies for IoT include ZigBee and Bluetooth Low Energy (BLE).

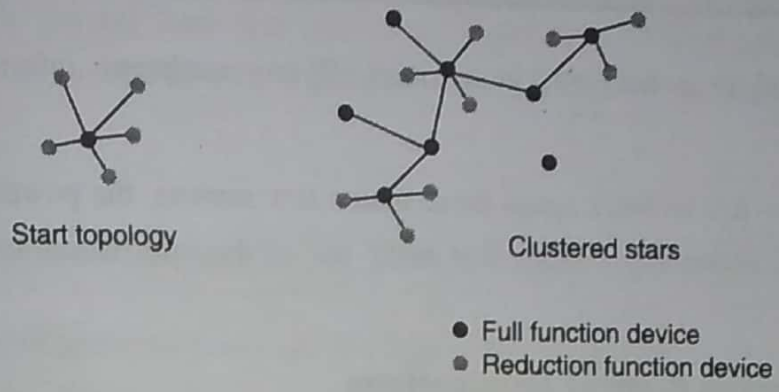
(3) **NAN (neighborhood area network) :** Scale of a few hundreds of meters. The term NAN is often used to refer to a group of house units from which data is collected.

(4) **FAN (field area network) :** Scale of several tens of meters to several hundred meters. FAN typically refers to an outdoor area larger than a single group of house units. The FAN is often seen as "open space" (and therefore not secured and not controlled).

(5) **LAN (local area network) :** Scale of up to 100 m. This term is very common in networking, and it is therefore also commonly used in the IoT space when standard networking technologies (such as Ethernet or IEEE 802.11) are used.

Similar ranges also do not mean similar topologies. Some technologies offer flexible connectivity structure to extend communication possibilities:

☞ Point-to-point topologies Point-to-multipoint



(1C3)**Fig. 3.2.2 : Star and Clustered Star Topologies**

☞ Comparison of the main solutions from an architectural angle.

Technology	Type and Range	Architectural Characteristics
Ethernet	Wired, 100 m max	Requires a cable per sensor/sensor group; adapted to static sensor position in a stable environment; range is limited; link is very reliable
Wi-Fi (2.4 3Hz, 5 GHz)	Wireless, 100 m (multipoint) to a few kilometers (P2P)	Can connect multiple clients (typically fewer than 200) to a single AP; range is limited; adapted to cases where client power is not an issue (continuous power or client battery recharged easily); large bandwidth available, but interference from other systems likely; AP needs a cable
802.11ah (Halo W, Wi-Fi in sub-1 GHz)	Wireless, 1.5 km (multipoint), 10 km (P2P)	Can connect a large number of clients (up to 6000 per AP); longer range than traditional Wi-Fi; power efficient; limited bandwidth; low adoption; and cost may be an issue
WiMAX(802.16)	Wireless, several kilometers (last mile), up to 50 km (backhaul)	Can connect a large number of clients; large bandwidth available in licensed spectrum (fee-based); reduced bandwidth in license-free spectrum (interferences from other systems likely) : adoption varies on location
Cellular (for example, LTE)	Wireless, several kilometers	Can connect a large number of clients; large bandwidth available; licensed spectrum (interference-free; license-based)

3.3 LAYER 3 : APPLICATIONS AND ANALYTICS LAYER

- Once connected to a network, your smart objects exchange information with other systems.
- As soon as your IoT network spans more than a few sensors, the power of the Internet of Things appears in the applications that make use of the information exchanged with the smart objects.

Analytics Versus Control Applications

Multiple applications can help increase the efficiency of an IoT network. Each application collects data and provides a range of functions based on analyzing the collected data. It can be difficult to compare the features offered. From an architectural standpoint, one basic classification can be as follows :

(1) Analytics application

- This type of application collects data from multiple smart objects, processes the collected data, and displays information resulting from the data that was processed.
- The display can be about any aspect of the IoT network, from historical reports, statistics, or trends to individual system states.
- The important aspect is that the application processes the data to convey a view of the network that cannot be obtained from solely looking at the information displayed by a single smart object.

(2) Control application

- This type of application controls the behavior of the smart object or the behavior of an object related to the smart object. For example, a pressure sensor may be connected to a pump.
- A control application increases the pump speed when the connected sensor detects a drop in pressure. Control applications are very useful for controlling complex aspects of an IoT network with a logic that cannot be programmed inside a single IoT object, either because the configured changes are too complex to fit into the local system or because the configured changes rely on parameters that include elements outside the IoT object.

☞ Data Versus Network Analytics

Analytics is a general term that describes processing information to make sense of collected data. In the world of IoT, a possible classification of the analytics function is as follows:

(1) Data analytics

GQ. Short note on Data Analytics. **(2 Marks)**

- This type of analytics processes the data collected by smart objects and combines it to provide an intelligent view related to the IoT system. At a very basic level, a dashboard can display an alarm when a weight sensor detects that a shelf is empty in a store.
- In a more complex case, temperature, pressure, wind, humidity, and light levels collected from thousands of sensors may be combined and then processed to determine the likelihood of a storm and its possible path .

(2) Network analytics

GQ. Short note on Network Analytics. **(2 Marks)**

- Most IoT systems are built around smart objects connected to the network. A loss or degradation in connectivity is likely to affect the efficiency of the system. Such a loss can have dramatic effects. For example, open mines use wireless networks to automatically pilot dump trucks.
- A lasting loss of connectivity may result in an accident or degradation of operations efficiency (automated dump trucks typically stop upon connectivity loss). On a more minor scale, loss of connectivity means that data stops being fed to your data analytics platform, and the system stops making intelligent analyses of the IoT system.

☞ Data Analytics Versus Business Benefits

- Data analytics is undoubtedly a field where the value of IoT is booming. Almost any object can be connected, and multiple types of sensors can be installed on a given object.
- Collecting and interpreting the data generated by these devices is where the value of IoT is realized.

☞ Smart Services

- The ability to use IoT to improve operations is often termed "smart services." This term is generic, and in many cases the term is used but its meaning is often stretched to include one form of service or another where an additional level of intelligence is provided.
- Smart services can also be used to measure the efficiency of machines by detecting machine output, speed, or other forms of usage evaluation.
- Smart services can be integrated into an IoT system. For example, sensors can be integrated in a light bulb. A sensor can turn a light on or off based on the presence of a human in the room

Chapter Ends...

❑❑❑

MODULE 4

CHAPTER 4

Application Protocols for IoT

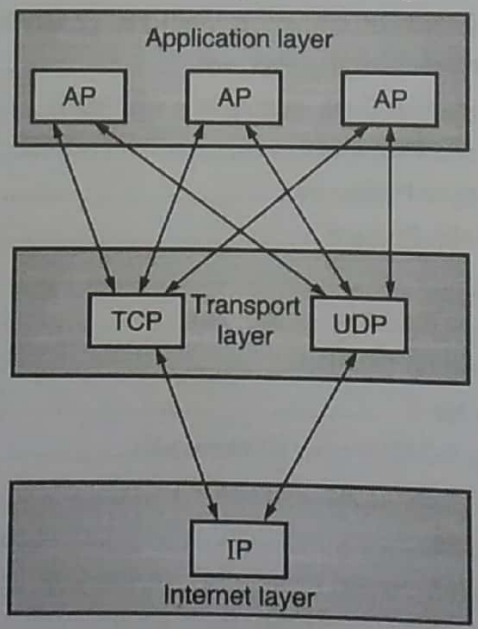
Syllabus

The Transport Layer, IoT Application Transport Methods, Application Layer Protocol Not Present SCADA - Background on SCADA, Adapting SCADA for IP, Tunneling Legacy SCADA over IP Networks, SCADA Protocol Translation, SCADA Transport over LLNs with MAP-T, Generic Web-Based Protocols, IoT Application Layer Protocols – CoAP and MQTT.

4.1 TRANSPORT LAYER

GQ. Explain transport Layer. **(4 Marks)**

- The transport layer is a 4th layer from the top.
- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
- The transport layer provides a logical communication between application processes running on different hosts. Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.
- The transport layer protocols are implemented in the end systems but not in the network routers.
- A computer network provides more than one protocol to the network applications. For example, TCP and UDP are two transport layer protocols that provide a different set of services to the network layer.
- All transport layer protocols provide multiplexing/ demultiplexing service. It also provides other services such as reliable data transfer, bandwidth guarantees, and delay guarantees.



(1D1) **Fig. 4.1.1 Transport layer**

- Each of the applications in the application layer has the ability to send a message by using TCP or UDP. The application communicates by using either of these two protocols.
- Both TCP and UDP will then communicate with the internet protocol in the internet layer.

- The applications can read and write to the transport layer. Therefore, we can say that communication is a two-way process.

(1) The Transport Layer

- This section reviews the selection of a protocol for the transport layer as supported by the TCP/IP architecture in the context of IoT networks.
- With the TCP/IP protocol, two main protocols are specified for the transport layer:

(2) Transmission Control Protocol (TCP)

- This connection-oriented protocol requires a session to get established between the source and destination before exchanging data.
- You can view it as an equivalent to a traditional telephone conversation, in which two phones must be connected and the communication link established before the parties can talk.

(3) User Datagram Protocol (UDP)

- With this connectionless protocol, data can be quickly sent between source and destination but with no guarantee of delivery.
- This is analogous to the traditional mail delivery system, in which a letter is mailed to a destination. Confirmation of there ception of this letter does not happen until another letter is sent in response.
- With the predominance of human interactions over the Internet, TCP is the main protocol used at the transport layer.
- This is largely due to its inherent characteristics, such as its ability to transport large volumes of data into smaller sets of packets.
- In addition, it ensures reassembly in a correct sequence, flow control and window adjustment, and retransmission of lost packets.
- These benefits occur with the cost of overhead per packet and per session, potentially impacting overall packet per second performances and latency.

4.2 IOT APPLICATION TRANSPORT METHODS

GQ. Explain IOT Application of Transport Methods. **(2 Marks)**

- Because of the diverse types of IoT application protocols, there are various means for transporting these protocols across a network.

- Sometimes you may be dealing with legacy utility and industrial IoT protocols that have certain requirements, while other times you might need to consider the transport requirements of more modern application layer protocols.
- To make these decisions easier, it makes sense to categorize the common IoT application protocols and then focus on the transport methods available for each category.
- The following categories of IoT application protocols and their transport methods are explored in the following sections:

4.2.1 Application Layer Protocol Not Present

In this case, the data payload is directly transported on top of the lower layers. No application layer protocol is used.

4.2.2 Supervisory control And Data Acquisition (SCADA)

SCADA is one of the most common industrial protocols in the world, but it was developed long before the days of IP, and it has been adapted for IP networks.

4.2.3 Generic Web-Based Protocols

Generic protocols, such as Ethernet, Wi-Fi, and 4G/LTE, are found on many consumer- and enterprise-class IoT devices that communicate over non-constrained networks.

4.2.4 IoT Application Layer Protocols

- IoT application layer protocols are devised to run on constrained nodes with a small compute footprint and are well adapted to the network bandwidth constraints on cellular or satellite links or constrained 6LoWPAN networks.
- Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), covered later in this chapter, are two well-known examples of IoT application layer protocols.

4.3 APPLICATION LAYER PROTOCOL NOT PRESENT

- As introduced in IETF RFC 7228 devices defined as class 0 send or receive only a few bytes of data.
- For myriad reasons, such as processing capability, power constraints, and cost, these devices do not implement a fully structured network protocol stack, such as IP, TCP, or UDP, or even an application layer protocol.

- Class 0 devices are usually simple smart objects that are severely constrained. Implementing a robust protocol stack is usually not useful and sometimes not even possible with the limited available resources.
- For example, consider low-cost temperature and relative humidity (RH) sensors sending data over an LPWA LoRaWAN infrastructure. is represented as 2 bytes and RH as another 2 bytes of data.
- Therefore, this small data payload is directly transported on top of the LoRaWAN MAC layer, without the use of TCP/IP.

4.4 SCADA

GQ. Write Short Note on SCADA. **(2 Marks)**

- In the world of networking technologies and protocols, IoT is relatively new. Combined with the fact that IP is the de facto standard for computer networking in general, older protocols that connected sensors and actuators have evolved and adapted themselves to utilize IP.
- A prime example of this evolution is supervisory control and data acquisition (SCADA). Designed decades ago, SCADA is an automation control system that was initially implemented without IP over serial links, before being adapted to Ethernet and IPv4.

4.4.1 A Little Background on SCADA

- For many years, vertical industries have developed communication protocols that fit their specific requirements.
- Many of them were defined and implemented when the most common networking technologies were serial link-based, such as RS-232 and RS-485.
- This led to SCADA networking protocols, which were well structured compared to the protocols described in the previous section, running directly over serial physical and data link layers.
- At a high level, SCADA systems collect sensor data and telemetry from remote devices, while also providing the ability to control them.
- Used in today's networks, SCADA systems allow global, real-time, data-driven decisions to be made about how to improve business processes.
- SCADA networks can be found across various industries, but you find SCADA mainly concentrated in the utilities and manufacturing/industrial verticals.

- Within these specific industries, SCADA commonly uses certain protocols for communications between devices and applications.
- For example, Modbus and its variants are industrial protocols used to monitor and program remote devices via a master/slave relationship. Modbus is also found in building management, transportation, and energy applications.
- The DNP3 and International Electrotechnical Commission (IEC) 60870-5-101 protocols are found mainly in the utilities industry, along with DLMS/COSEM and ANSI C12 for advanced meter reading (AMR).
- Both DNP3 and IEC 60870-5-101 are discussed in more detail later in this chapter. As mentioned previously, these protocols go back decades and are serial based. So, transporting them over current IoT and traditional networks requires that certain accommodations be made from both protocol and implementation perspectives. These accommodations and other adjustments form various SCADA transport methods that are the focus of upcoming sections.

4.4.2 Adapting SCADA for IP

- In the 1990s, the rapid adoption of Ethernet networks in the industrial world drove the evolution of SCADA application layer protocols.
- For example, the IEC adopted the Open System Interconnection (OSI) layer model to define its protocol framework. Other protocol user groups also slightly modified their protocols to run over an IP infrastructure.
- Benefits of this move to Ethernet and IP include the ability to leverage existing equipment and standards while integrating seamlessly the SCADA subnetworks to the corporate WAN infrastructures. To further facilitate the support of legacy industrial protocols over IP networks, protocol specifications were updated and published, documenting the use of IP for each protocol.
- This included assigning TCP/UDP port numbers to the protocols, such as the following :

  DNP3 (adopted by IEEE 1815-2012) specifies the use of TCP or UDP on port 20000 for transporting DNP3 messages over IP.
- The Modbus messaging service utilizes TCP port 502. IEC 60870-5-104 is the evolution of IEC 60870-5-101 serial for running over Ethernet and IPv4 using port 2404 DLMS User Association specified a communication profile based on TCP/IP in the DLMS/COSEM Green Book (Edition 5 or higher), or in the IEC 62056-53 and IEC 62056-47 standards, allowing data exchange via IP and port 4059.

4.4.3 Tunneling Legacy SCADA over IP Networks

- Deployments of legacy industrial protocols, such as DNP3 and other SCADA protocols, in modern IP networks call for flexibility when integrating several generations of devices or operations that are tied to various releases and versions of application servers. Native support for IP can vary and may require different solutions.
- Ideally, end-to-end native IP support is preferred, using a solution like IEEE 1815-2012 in the case of DNP3.

4.4.4 SCADA Transport over LLNs with MAP-T

- Due to the constrained nature of LLNs, the implementation of industrial protocols should at a minimum be done over UDP. This in turn requires that both the application servers and devices support and implement UDP.
- While the long-term evolution of SCADA and other legacy industrial protocols is to natively support IPv6, it must be highlighted that most, if not all, of the industrial devices supporting IP today support IPv4 only.
- When deployed over LLN subnetworks that are IPv6 only, a transition mechanism, such as MAP-T (Mapping of Address and Port using Translation, RFC 7599), needs to be implemented. This allows the deployment to take advantage of native IPv6 transport transparently to the application and devices. depicts a scenario in which a legacy endpoint is connected across an LLN running 6LoWPAN to an IP-capable SCADA server.
- The legacy endpoint could be running various industrial and SCADA protocols, including DNP3/IP, Modbus/TCP, or IEC 60870-5-104. In this scenario, the legacy devices and the SCADA server support only IPv4 (typical in the industry today).
- However, IPv6 (with 6LoWPAN and RPL) is being used for connectivity to the endpoint. 6LoWPAN is a standardized protocol designed for constrained networks, but it only supports IPv6. In this situation, the end devices, the endpoints, and the SCADA server support only IPv4, but the network in the middle supports only IPv6.

4.5 GENERIC WEB-BASED PROTOCOLS

GQ. Explain Generic Web-Based Protocols. **(4 Marks)**

- Over the years, web-based protocols have become common in consumer and enterprise applications and services.

- Therefore, it makes sense to try to leverage these protocols when developing IoT applications, services, and devices in order to ease the integration of data and devices from prototyping to production.
- The level of familiarity with generic web-based protocols is high. Therefore, programmers with basic web programming skills can work on IoT applications, and this may lead to innovative ways to deliver and handle real-time IoT data.
- For example, an IoT device generating an event can have the result of launching a video capture, while at the same time a notification is sent to a collaboration tool, such as a Cisco Spark room. This notification allows technicians and engineers to immediately start working on this alert.
- In addition to a generally high level of familiarity with web-based protocols, scaling methods for web environments are also well understood and this is crucial when developing consumer applications for potentially large numbers of IoT devices.
- Once again, the definition of constrained nodes and networks must be analyzed to select the most appropriate protocol. On non-constrained networks, such as Ethernet, Wi-Fi, or 3G/4G cellular, where bandwidth is not perceived as a potential issue, data payloads based on a verbose data model representation, including XML or JavaScript Object Notation (JSON), can be transported over HTTP/HTTPS or WebSocket. This allows implementers to develop their IoT applications in contexts similar to web applications.
- The HTTP/HTTPS client/server model serves as the foundation for the World Wide Web. Recent evolutions of embedded web server software with advanced features are now implemented with very little memory (in the range of tens of kilobytes in some cases). This enables the use of embedded web services software on some constrained devices MQTT and CoAP both are the most popular Internet of Things protocols. During the next post, we will talk about pros and cons of each one.

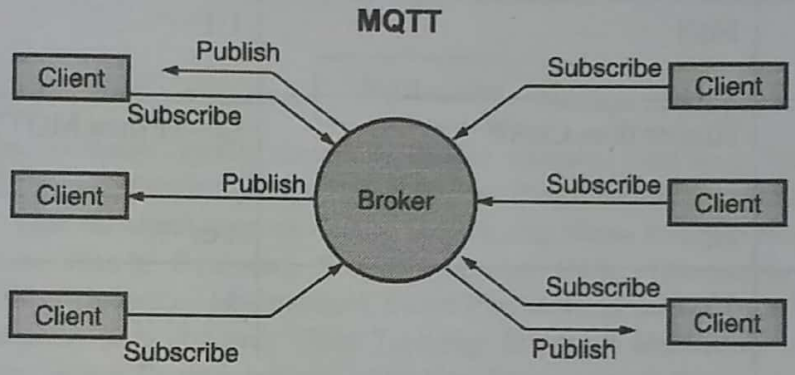
4.6 IOT APPLICATION LAYER PROTOCOLS

- When considering constrained networks and/or a large-scale deployment of constrained nodes, verbose web-based and data model protocols, as discussed in the previous section, may be too heavy for IoT applications.
- To address this problem, the IoT industry is working on new lightweight protocols that are better suited to large numbers of constrained nodes and networks. Two of the most popular protocols are CoAP and MQTT

What is MQTT?

GQ. Write a short note on MQTT. **(2 Marks)**

- Message Queue Telemetry Transport (MQTT), is a publish-subscribe protocol that facilitates one-to-many communication mediated by brokers.
- Clients can publish messages to a broker and/or subscribe to a broker to receive certain messages. Messages are organized by topics, which essentially are "labels" that act as a system for dispatching messages to subscribers.

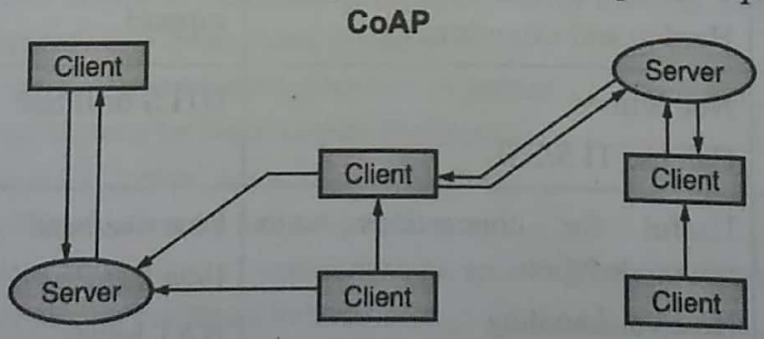


(1D2)**Fig. 4.6.1 MQTT**

4.6.1 What is CoAP?

GQ. Write a short note on COAP. **(2 Marks)**

- Constrained Application Protocol (CoAP), is a **client-server protocol** that, unlike MQTT, is not yet standardized. With CoAP, a **client node can command another node** by sending a CoAP packet.
- The CoAP server will interpret it, extract the payload, and decide what to do depending on its logic. The server does not necessarily have to acknowledge the request.



(1D3)**Fig. 4.6.2 COAP**

The following table **compares** different features and shows the **strengths and debilities** of each protocol :

Features	MQTT	CoAP
Base protocol	TCP	UDP
Model used for communication	Publish-Subscribe	Request-Response Publish-Subscribe
Communication node	M:N	1:1
Power consumption	Higher than CoAP	Lower than MQTT
RESTful	No	Yes
Number of messages type used	16	4
Header size	2 Bytes	4 Bytes
Messaging	Asynchronous	Asynchronous & Synchronous
Reliability	3 Quality of service levels QoS 0: Delivery not guaranteed QoS 1: Delivery confirmation QoS 2: Delivery double confirmation	Confirmable messages Non-confirmable messages Acknowledgements Retransmissions
Implementation	Easy to implement Hard to add extensions	Few existing libraries and support
Security	Not defined Can use TLS/SSL	DTLS or IPSec
Other	Useful for connections with remote location No error-handling	Low overhead Low latency NAT issues

...Chapter ends

❑❑❑

MODULE 5

CHAPTER 5

Domain Specific IoTs

Syllabus

Home Automation - Smart Lighting, Smart Appliances, Intrusion Detection, Smoke/Gas Detectors, Cities - Smart Parking, Smart Lighting, Smart Roads, Structural Health Monitoring, Surveillance, Environment - Weather Monitoring, Air Pollution Monitoring, Noise Pollution Monitoring, Forest Fire Detection, River Floods Detection, Energy - Smart Grids, Renewable Energy Systems, Prognostics, Retail - Inventory Management, Smart Payments, Smart Vending Machines, Logistics - Route Generation & Scheduling, Fleet Tracking, Shipment Monitoring, Agriculture - Smart Irrigation, Green House Control, Industry - Machine Diagnostics & Prognosis, Indoor Air Quality Monitoring, Health & Lifestyle - Health & Fitness Monitoring, Wearable Electronics.

5.1 HOME AUTOMATION

GQ. Explain Home Automation IOT Example. **(4 Marks)**

Fig. 5.1.1

a) **Smart Lighting :** helps in saving energy by adapting the lighting to the ambient conditions and switching on/off or diming the light when needed.

b) **Smart Appliances :** make the management easier and also provide status information to the users remotely.

c) **Intrusion Detection :** use security cameras and sensors (PIR sensors and door sensors) to detect intrusion and raise alerts. Alerts can be in the form of SMS or email sent to the user.

d) **Smoke/Gas Detectors :** Smoke detectors are installed in homes and buildings to detect smoke that is typically an early sign of fire. Alerts raised by smoke detectors can be in the form of signals to a fire alarm system. Gas detectors can detect the presence of harmful gases such as CO, LPG etc.

- Home automation is constructing automation for a domestic, mentioned as a sensible home or smart house. In the IoT home automation ecosystem, you can control your devices like light, fan, TV, etc.
- A domestic automation system can monitor and/or manage home attributes adore lighting, climate, enjoyment systems, and appliances. It is very helpful to control your home devices.
- It's going to in addition incorporates domestic security such as access management and alarm systems. Once it coupled with the internet, domestic gadgets are a very important constituent of the Internet of Things.

- A domestic automation system usually connects controlled devices to a central hub or gateway.
- The program for control of the system makes use of both wall-mounted terminals, tablet or desktop computers, a smartphone application, or an online interface that may even be approachable off-site through the Internet.

5.1.1 Smart Home Components

Here, you will see the smart home components like smart lighting, smart appliances, intrusion detection, smoke/gas detector, etc. So, let's discuss it.

Component-1 : Smart Lighting

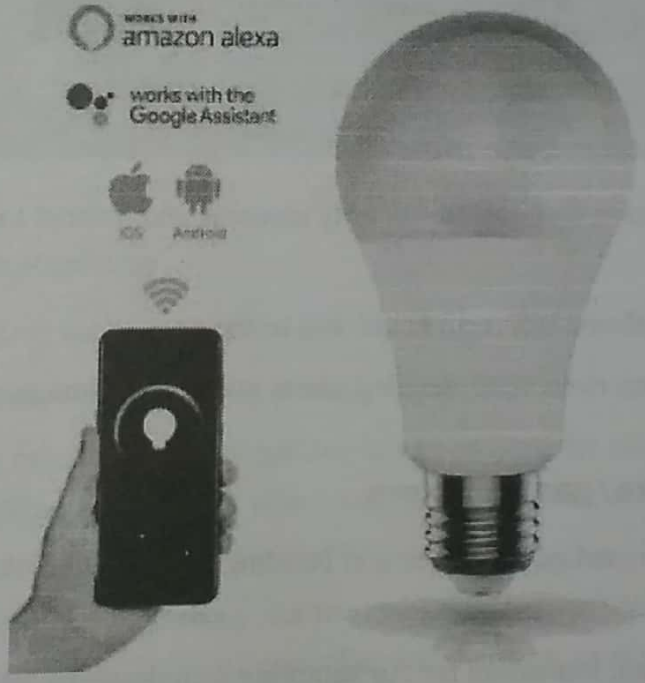


Fig. 5.1.2

- Smart lighting for home helps in saving energy by adapting the life to the ambient condition and switching on/off or dimming the light when needed.
- Smart lighting solutions for homes achieve energy saving by sensing the human movements and their environments and controlling the lights accordingly.

Component-2 : Smart Appliances

- Smart appliances with the management are here and also provide status information to the users remotely.

- Smart washer/dryer can be controlled remotely and notify when the washing and drying are complete.
- Smart refrigerators can keep track of the item store and send updates to the users when an item is low on stock.

Fig. 5.1.3

Component-3 : Intrusion Detection

- Home intrusion detection systems use security cameras and sensors to detect intrusion and raise alerts.
- Alert can we inform of an SMS or an email sent to the user.
- Advanced systems can even send detailed alerts such as an image shoot or short video clips.

Component-4 : Smoke/gas detectors

- Smoke detectors are installed in homes and buildings to detect smoke that is typically an early sign of Fire.
- It uses optical detection, ionization for Air sampling techniques to detect smoke.
- Gas detectors can detect the presence of harmful gases such as CO, LPG, etc.
- It can raise alerts in the human voice describing where the problem is.

5.2 CITIES IOT APPLICATIONS FOR SMART CITIES

GQ. Explain IOT Application for smart Cities. **(4 Marks)**

- Smart Parking
- Smart Lighting for Road
- Smart Road

- Structural Health Monitoring
- Surveillance
- Emergency Response

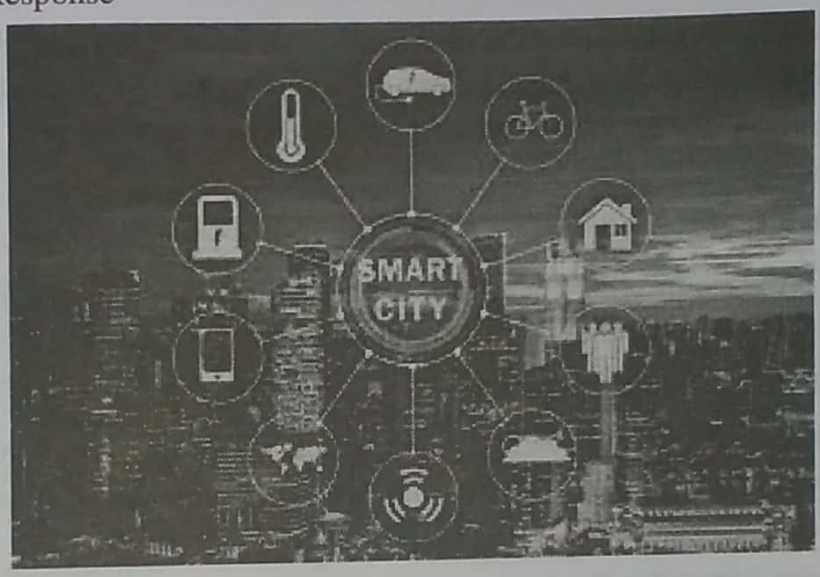


Fig. 5.2.1

☞ Cities Smart Parking

- Finding the parking space in the crowded city can be time consuming and frustrating
- Smart parking makes the search for parking space easier and convenient for driver.
- It can detect the number of empty parking slots and send the information over the Internet to the smart parking applications which can be accessed by the drivers using their smart phones, tablets, and in car navigation systems.
- Sensors are used for each parking slot to detect whether the slot is empty or not, and this information is aggregated by local controller and then sent over the Internet to database.
- **Paper :** Design and implementation of a prototype Smart Parking (SPARK) system using WSN [International Conference on Advanced Information Networking and Applications Workshop, 2009]-> designed and implemented a prototype smart parking system based on wireless sensor network technology with features like remote parking monitoring, automate guidance, and parking reservation mechanism.

☞ Cities Smart Lighting for Roads

- It can help in saving energy.
- Smart lighting for roads allows lighting to be dynamically controlled and also adaptive to ambient conditions.

- Smart light connected to the Internet can be controlled remotely to configure lighting schedules and lighting intensity.
- Custom lighting configurations can be set for different situations such as a foggy day, a festival, etc.
- **Paper :** Smart Lighting solutions for Smart Cities [International Conference on Advance Information Networking and Applications Workshop, 2013]-> described the need for smart lighting system in smart cities, smart lighting features and how to develop interoperable smart lighting solutions.

☞ Cities Smart Roads

- Smart Roads provides information on driving conditions, travel time estimates and alerts in case of poor driving conditions, traffic congestions and accidents.
- Such information can help in making the roads safer and help in reducing traffic jams
- Information sensed from the roads can be communicated via internet to cloud-based applications and social media and disseminated to the drivers who subscribe to such applications.
- **Paper :** Sensor networks for smart roads [PerCom Workshop, 2006]-> proposed a distributed and autonomous system of sensor network nodes for improving driving safety on public roads, the system can provide the driver and passengers with a consistent view of the road situation a few hundred metes ahead of them or a few dozen miles away, so that they can react to potential dangers early enough.

☞ Cities Structural Health Monitoring

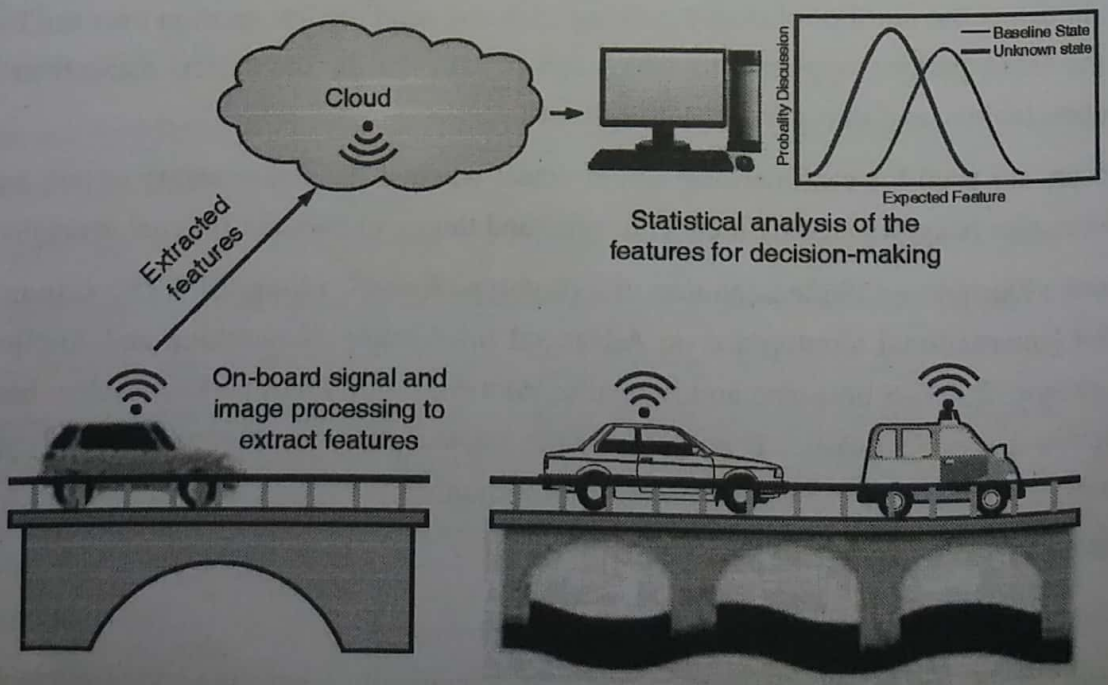


Fig. 5.2.2

- It uses a network of sensors to monitor the vibration levels in the structures such as bridges and buildings.
- The data collected from these sensors is analyzed to assess the health of the structures.
- By analyzing the data it is possible to detect cracks and mechanical breakdowns, locate the damages to a structure and also calculate the remaining life of the structure.
- Using such systems, advance warnings can be given in the case of imminent failure of the structure.
- **Paper :** Environmental Effect Removal Based Structural Health Monitoring in the Internet of Things [International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2013]-> proposed an environmental effect removal based structural health monitoring scheme in an IoT environment.
- Energy harvesting technologies for structural health monitoring applications [IEEE Conference on Technologies for Sustainability, 2013] -> Explored energy harvesting technologies of harvesting ambient energy, such as mechanical vibrations, sunlight, and wind.

☞ Cities Surveillance

Fig. 5.2.3

- Surveillance of infrastructure, public transport and events in cities is required to ensure safety and security.
- City wide surveillance infrastructure comprising of large number of distributed and Internet connected video surveillance cameras can be created.
- The video feeds from surveillance cameras can be aggregated in cloud-based scalable storage solutions.
- Cloud-based video analytics applications can be developed to search for patterns of specific events from the video feeds.

☞ Cities Emergency Response

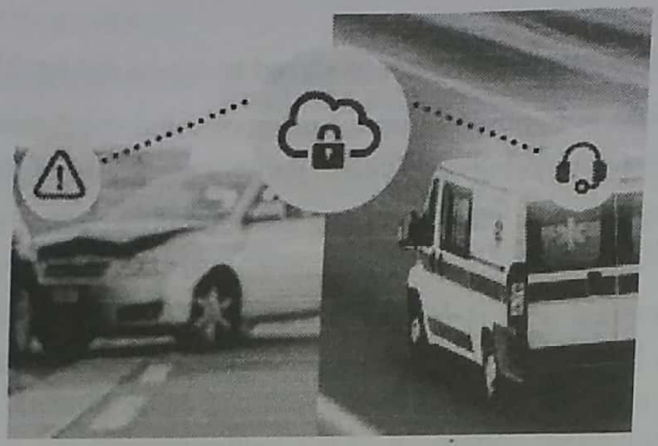


Fig. 5.2.4

- IoT systems can be used for monitoring the critical infrastructure cities such as buildings, gas, and water pipelines, public transport and power substations.
- IoT systems for critical infrastructure monitoring enable aggregation and sharing of information collected from lager number of sensors.
- Using cloud-based architectures, multi-modal information such as sensor data, audio, video feeds can be analyzed I near real-time to detect adverse events.
- The alert can be in the form :
  - Alerts sent to the public Re-rerouting of traffic
  - Evacuations of the affected areas

⏭ 5.3 ENVIRONMENT IOT APPLICATIONS FOR SMART ENVIRONMENTS:

GQ. Explain Environment IoT applications for smart environments. **(4 Marks)**

- Weather Monitoring
- Air Pollution Monitoring
- Noise Pollution Monitoring
- Forest Fire Detection
- River Flood Detection

☞ Environment Weather Monitoring

- It collects data from a number of sensor attached such as temperature, humidity, pressure, etc and send the data to cloud-based applications and store back-ends.
- The data collected in the cloud can then be analyzed and visualized by cloud-based applications.
- Weather alert can be sent to the subscribed users from such applications.
- AirPi is a weather and air quality monitoring kit capable of recording and uploading information about temperature, humidity, air pressure, light levels, UV levels, carbon monoxide, nitrogen dioxide and smoke level to the Internet.
- **Paper :** PeWeMoS – Pervasive Weather Monitoring System [ICPCA, 2008]-> Presented a pervasive weather monitoring system that is integrated with buses to measure weather variables like humidity, temperature, and air quality during the bus path

☞ Environment Air Pollution Monitoring

- IoT based air pollution monitoring system can monitor emission of harmful gases by factories and automobiles using gaseous and meteorological sensors.
- The collected data can be analyzed to make informed decisions on pollutions control approaches.
- **Paper :** Wireless sensor network for real-time air pollution monitorings [ICCSPA, 2013]-> Presented a real time air quality monitoring system that comprises of several distributed monitoring stations that communicate via wireless with a back- end server using machine-to machine communication.

☞ Environment Noise Pollution Monitoring

- Noise pollution monitoring can help in generating noise maps for cities.
- It can help the policy maker in making policies to control noise levels near residential areas, school and parks.
- It uses a number of noise monitoring stations that are deployed at different places in a city.
- The data on noise levels from the stations is collected on servers or in the cloud and then the collected data is aggregate to generate noise maps.
- **Papers :** Noise mapping in urban environments : Applications at Suez city center [ICCIE, 2009]Presented a noise mapping study for a city which revealed that the city suffered from serious noise pollution.

- SoundOfCity – Continuous noise monitoring for a health city [PerComW,2013]-> Designed a smartphone application that allows the users to continuously measure noise levels and send to a central server here all generated information is aggregated and mapped to a meaningful noise visualization map.

☞ Environment Forest Fire Detection

- IoT based forest fire detection system use a number of monitoring nodes deployed at different location in a forest.
- Each monitoring node collects measurements on ambient condition including temperature, humidity, light levels, etc.
- Early detection of forest fires can help in minimizing the damage.
- **Papers :** A novel accurate forest fire detection system using wireless sensor networks [International Conference on Mobile Ad- hoc and Sensor Networks, 2011]-> Presented a forest fire detection system based on wireless sensor network. The system uses multi-criteria detection which is implemented by the artificial neural network. The ANN fuses sensing data corresponding to ,multiple attributes of a forest fire such as temperature, humidity, infrared and visible light to detect forest fires.

☞ Environment River Flood Detection

- IoT based river flood monitoring system uses a number of sensor nodes that monitor the water level using ultrasonic sensors and flow rate using velocity sensors.
- Data from these sensors is aggregated in a server or in the cloud, monitoring applications raise alerts when rapid increase in water level and flow rate is detected.
- **Papers :** RFMS : Real time flood monitoring system with wireless sensor networks [MASS, 2008]-> Described a river flood monitoring system that measures river and weather conditions through wireless sensor nodes equipped with different sensors
- Urban Flash Flood Monitoring, Mapping and Forecasting via a Tailored Sensor Network System [ICNSC, 2006] -> Described a motes-based sensor network for river flood monitoring that includes a water level monitoring module, network video recorder module, and data processing module that provides floods information n the form of raw data, predict data, and video feed.

5.4 ENERGY IOT APPLICATIONS FOR SMART ENERGY SYSTEMS:

GQ. Explain Energy IoT applications for smart energy systems. **(4 Marks)**

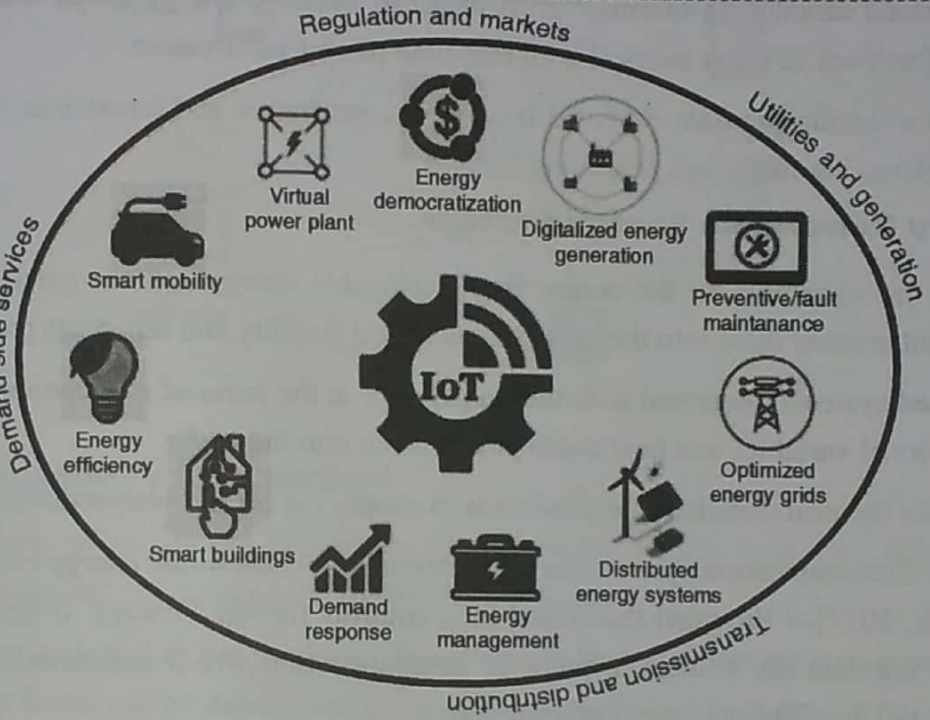


Fig. 5.4.1

- Smart Grid
- Renewable Energy Systems
- Prognostics

☞ Energy Smart Grids

- Smart grid technology provides predictive information and recommendation s to utilize, their suppliers, and their customers on how best to manage power.
- Smart grid collect the data regarding :
  - Electricity generation
  - Electricity consumption
  - Storage
  - Distribution and equipment health data
- By analyzing the data on power generation, transmission and consumption of smart grids can improve efficiency throughout the electric system.

- Storage collection and analysis of smarts grids data in the cloud can help in dynamic optimization of system operations, maintenance, and planning.
- Cloud-based monitoring of smart grids data can improve energy usage usage levels via energy feedback to users coupled with real-time pricing information.
- Condition monitoring data collected from power generation and transmission systems can help in detecting faults and predicting outages.

☞ Energy Renewable Energy System

- Due to the variability in the output from renewable energy sources (such as solar and wind), integrating them into the grid can cause grid stability and reliability problems.
- IoT based systems integrated with the transformer at the point of interconnection measure the electrical variables and how much power is fed into the grid
- To ensure the grid stability, one solution is to simply cut off the overproductions.
- **Paper :** Communication systems for grid integration of renewable energy resources [IEEE Network, 2011]-> Provided the closed-loop controls for wind energy system that can be used to regulate the voltage at point of interconnection which coordinate wind turbine outputs and provides reactive power support.

☞ Energy Prognostics

- IoT based prognostic real-time health management systems can predict performance of machines of energy systems by analyzing the extent of deviation of a system from its normal operating profiles.
- In the system such as power grids, real time information is collected using specialized electrical sensors called Phasor Measurement Units (PMU)
- Analyzing massive amounts of maintenance data collected from sensors in energy systems and equipment can provide predictions for impending failures.
- OpenPDC is a set of applications for processing of streaming time-series data collected from Phasor Measurements Units (PMUs) in real-time.

⏭ 5.5 RETAIL IOT APPLICATIONS IN SMART RETAIL SYSTEMS

GQ. Explain IOT smart retail application. **(4 Marks)**

- Inventory Management
- Smart Payments

- Smart Vending Machines

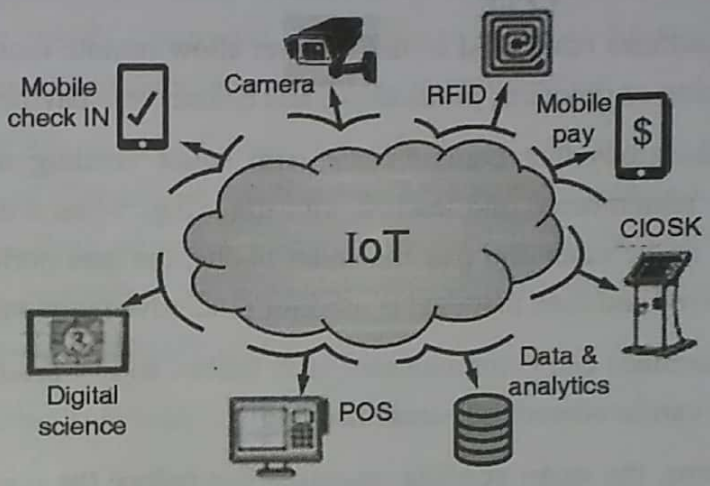


Fig. 5.5.1

☞ Retail Inventory Management

- IoT system using Radio Frequency Identification (RFID) tags can help inventory management and maintaining the right inventory levels.
- RFID tags attached to the products allow them to be tracked in the real-time so that the inventory levels can be determined accurately and products which are low on stock can be replenished.
- Tracking can be done using RFID readers attached to the retail store shelves or in the warehouse.
- **Paper :** RFID data-based inventory management of time-sensitive materials [IECON, 2005]-> described an RFID data-based inventory management system for time-sensitive materials

☞ Retail Smart Payments

- Smart payments solutions such as contact-less payments powered technologies such as Near field communication (NFC) and Bluetooth.
- NFC is a set of standards for smart-phones and other devices to communicate with each other by bringing them into proximity or by touching them
- Customer can store the credit card information in their NFC-enabled smart-phones and make payments by bringing the smart-phone near the point of sale terminals.
- NFC maybe used in combination with Bluetooth, where NFC initiates initial pairing of devices to establish a Bluetooth connection while the actual data transfer takes place over Bluetooth.

☞ Retail Smart Vending Machines

- Smart vending machines connected to the Internet allow remote monitoring of inventory levels, elastic pricing of products, promotions, and contact-less payments using NFC.
- Smart-phone applications that communicate with smart vending machines allow user preferences to be remembered and learned with time. E.g: when a user moves from one vending machine to the other and pair the smart-phone, the user preference and favourite product will be saved and then that data is used for predictive maintenance.
- Smart vending machines can communicated each others, so if a product out of stock in a machine, the user can be routed to nearest machine
- For perishable items, the smart vending machines can reduce the price as the expiry date nears.

⏭ 5.6 LOGISTIC IOT APPLICATIONS FOR SMART LOGISTIC SYSTEMS

GQ. Explain IOT logistic Application. **(4 Marks)**

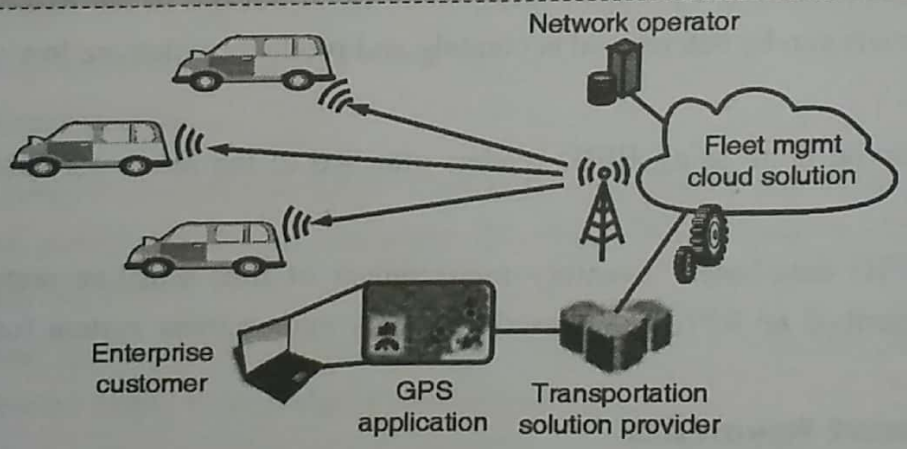


Fig. 5.6.1

- Fleet Tracking
- Shipment Monitoring
- Remote Vehicle Diagnostics

☞ Logistics Fleet Tracking

- Vehicle fleet tracking systems use GPS technology to track the locations of the vehicles in the real- time.
- Cloud-based fleet tracking systems can be scaled up on demand to handle large number of vehicles.

- The vehicle locations and routers data can be aggregated and analyzed for detecting bottlenecks I the supply chain such as traffic congestions on routes, assignments and generation of alternative routes, and supply chain optimization
- **Paper :** A Fleet Monitoring System for Advanced Tracking of commercial Vehicles [IEEE International Conference in Systems, Man and Cybernetics, 2006]-> provided a system that can analyze messages sent from the vehicles to identify unexpected incidents and discrepancies between actual and planned data, so that remedial actions can be taken.

☞ Logistics Shipment Monitoring

- Shipment monitoring solutions for transportation systems allow monitoring the conditions inside containers.
- E.g : Containers carrying fresh food produce can be monitored to prevent spoilage of food. IoT based shipment monitoring systems use sensors such as temperature, pressure, humidity, for instance, to monitor the conditions inside the containers and send the data to the cloud, where it can be analyzed to detect food spoilage.
- **Paper :**"On a Cloud-Based Information Technology Framework for Data Driven Intelligent Transportation System [Journal of Transportation Technologies, 2013]-> proposed a cloud based framework for real time fresh food supply tracking and monitoring
- Container Integrity and Condition Monitoring using RF Vibration Sensor Tags [IEEE International Conference on Automation Science and Engineering, 2007] ◊ Proposed a system that can monitor the vibrations patterns of a container and its contents to reveal information related to its operating environment and integrity during transport, handling, and storage.

☞ Logistics Remote Vehicle Diagnostics

- It can detect faults in the vehicles or warn of impending faults.
- These diagnostic systems use on-board IoT devices for collecting data on vehicle operation such as speed, engine RPM, coolent temperature, fault code number and status of various vehicle sub- system.
- Modern commercial vehicles support on-board diagnostic (OBD) standard such as OBD-II
- OBD systems provide real-time data on the status of vehicle sub-systems and diagnostic trouble codes which allow rapidly identifying the faults in the vehicle.
- IoT based vehicle diagnostic systems can send the vehicle data to centralized servers or the cloud where it can be analyzed to generate alerts and suggest remedial actions.

5.7 AGRICULTURE IOT APPLICATIONS FOR SMART AGRICULTURE

GQ. Explain Agriculture IoT applications for smart agriculture. **(4 Marks)**

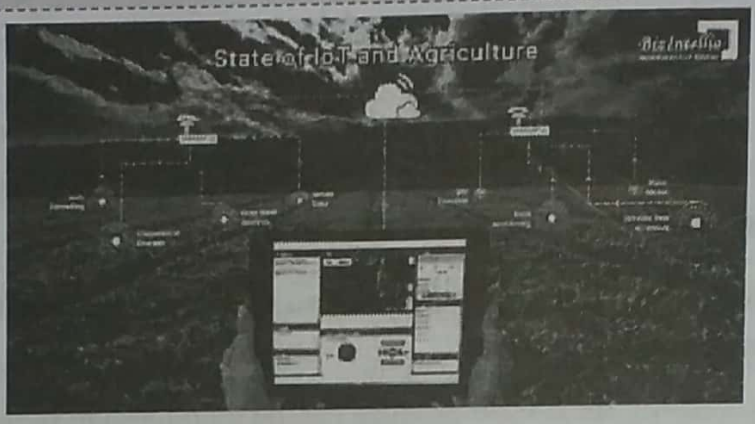


Fig. 5.7.1

- Smart Irrigation
- Green House Control

☞ Agriculture Smart Irrigation

- Smart irrigation system can improve crop yields while saving water.
- Smart irrigation systems use IoT devices with soil moisture sensors to determined the amount of moisture on the soil and release the flow of the water through the irrigation pipes only when the moisture levels go below a predefined threshold.
- It also collect moisture level measurements on the server on in the cloud where the collected data can be analyzed to plan watering schedules.
- Cultivar's RainCould is a device for smart irrigation that uses water valves, soil sensors, and a WiFi enabled programmable computer. [http://ecultivar.com/rain-cloud-product-project/]

☞ Agriculture Green House Control

- It controls temperature, humidity, soil, moisture, light, and carbon dioxide level that are monitored by sensors and climatological conditions that are controlled automatically using actuation devices.
- IoT systems play an importance role in green house control and help in improving productivity.

- The data collected from various sensors is stored on centralized servers or in the cloud where analysis is performed to optimize the control strategies and also correlate the productivity with different control strategies.
- **Paper :** Wireless sensing and control for precision Green house management [ICST, 2012]-> Provided a system that uses wireless sensor network to monitor and control the agricultural parameters like
- temperature and humidity in the real time for better management and maintenance of agricultural production.

5.8 INDUSTRY IOT APPLICATIONS IN SMART INDUSTRY

GQ. Explain Industry IOT application in smart Industry. **(4 Marks)**

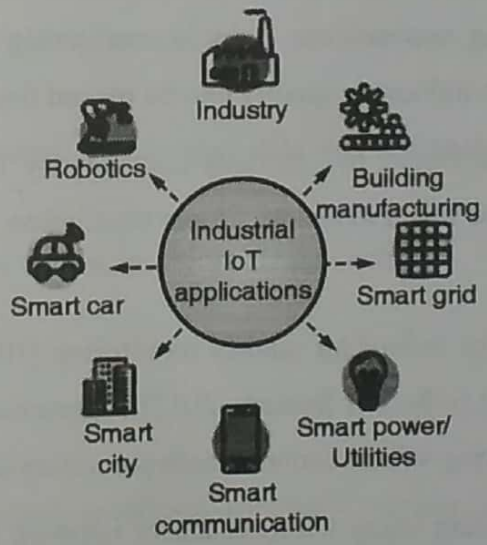


Fig. 5.8.1

- Machine Diagnosis & Prognosis
- Indoor Air Quality Monitoring

Industry Machine Diagnosis & Prognosis

- Machine prognosis refers to predicting the performance of machine by analyzing the data on the current operating conditions and how much deviations exist from the normal operating condition.
- Machine diagnosis refers to determining the cause of a machine fault.

- Sensors in machine can monitor the operating conditions such as temperature and vibration levels, sensor data measurements are done on timescales of few milliseconds to few seconds which leads to generation of massive amount of data.
- Case-based reasoning (CBR) is a commonly used method that finds solutions to new problems based on past experience.
- CBR is an effective technique for problem solving in the fields in which it is hard to establish a quantitative mathematical model, such as machine diagnosis and prognosis.

☞ **Industry Indoor Air Quality Monitoring**

- Harmful and toxic gases such as carbon monoxide (CO), nitrogen monoxide (NO), Nitrogen Dioxide, etc can cause serious health problem of the workers.
- IoT based gas monitoring systems can help in monitoring the indoor air quality using various gas sensors. - The indoor air quality can be placed for different locations
- Wireless sensor networks based IoT devices can identify the hazardous zones, so that corrective measures can be taken to ensure proper ventilation.

☞ **Papers**

- A hybrid sensor system for indoor air quality monitoring [IEEE International Conference on Distributed Computing in Sensor System, 2013]-> presented a hybrid sensor system for indoor air quality monitoring which contains both stationary sensor and mobile sensors.
- Indoor air quality monitoring using wireless sensor network [International Conference on Sensing Technology, 2012] -> provided a wireless solution for indoor air quality monitoring that measures the environmental parameters like temperature, humidity, gaseous pollutants , aerosol and particulate matter to determine the indoor air quality.◊

⏭ 5.9 HEALTH & LIFESTYLE IOT APPLICATIONS IN SMART HEALTH & LIFESTYLE

GQ. Explain Health & Health & Lifestyle IoT applications in smart health & lifestyle. **(4 Marks)**

- Health & Fitness Monitoring
- Wearable Electronics

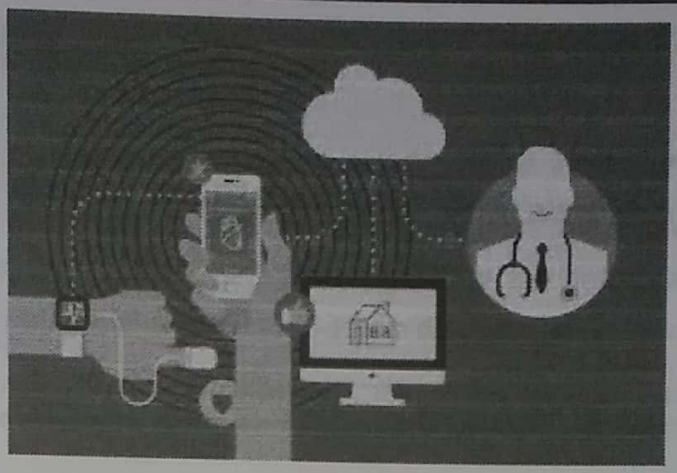


Fig. 5.9.1

☞ Fitness Monitoring

- Wearable IoT devices allow to continuous monitoring of physiological parameters such as blood pressure, heart rate, body temperature, etc than can help in continuous health and fitness monitoring.
- It can analyze the collected health-care data to determine any health conditions or anomalies.
- The wearable devices may can be in various form such as:
  (1) Belts
  (2) Wrist-bands
  (3) Papers
- Toward ubiquitous mobility solutions for body sensor network health care [IEEE Communications Magazine, 2012]-> Proposed an ubiquitous mobility approach for body sensor network in health-care
- A wireless sensor network compatible wearable u-healthcare monitoring system using integrated ECG, accelerometer and SpO2 [International Conference of the IEEE Engineering in Medicine and Biology Society, 2008]-> Health & Lifestyle Health & Designed a wearable ubiquitous health-care monitoring system that uses integrated electrocardiogram (ECG), accelerometer and oxygen saturation (SpO2) sensors.◊

☞ Health & Lifestyle Wearable Electronics

- Wearable electronics such as wearable gadgets (smart watch, smart glasses, wristbands, etc) provide various functions and features to assist us in our daily activities and making us lead healthy lifestyles.

- Using the smart watch, the users can search the internet, play audio/video files, make calls, play games, etc.
- Smart glasses allows users to tae photos and record videos, get map directions, check flight status or search internet using voice commands
- Smart shoes can monitor the walking or running speeds and jumps with the help of embedded sensors and be paired with smart-phone to visualize the data.
- Smart wristbands can tract the daily exercise and calories burnt.

Chapter Ends...

❑❑❑

MODULE 6

CHAPTER 6

Create your own IoT

Syllabus

IoT Hardware - Arduino, Raspberry Pi, ESP32, Cloudbit/Littlebits, Particle Photon, Beaglebone Black. IoT Software - languages for programming IoT hardware, for middleware applications and API development, for making front ends, REST and JSON-LD, A comparison of IoT boards and platforms in terms of computing, A comparison of IoT boards and platforms in terms of development environments and communication standards, A comparison of boards and platforms in terms of connectivity, A comparison of IoT software platforms.

6.1 IOT HARDWARE

When it comes to IoT hardware, one can think of mobile phones as IoT devices, since smartphones have sensors, dis-plays, and a unique address and are connected to the Inter-net. Regarding IoT devices, Paul Jacobs, former chief executive officer of Qualcomm, has said, "In the future, almost all things will be linked on the web, and mobile phones will act as hubs for IoT. So, IoT is nothing but the Internet linkage of smart objects and embedded systems other than mobile phones, with mobiles phones acting as access centers for IoT". The term smart objects referred to by Jacobs can be described as things or objects that are responsible for providing useful information on their interac-

6.1.1 ARDUINO

GQ. Explain features of Arduino. **(2 Marks)**

Introduction

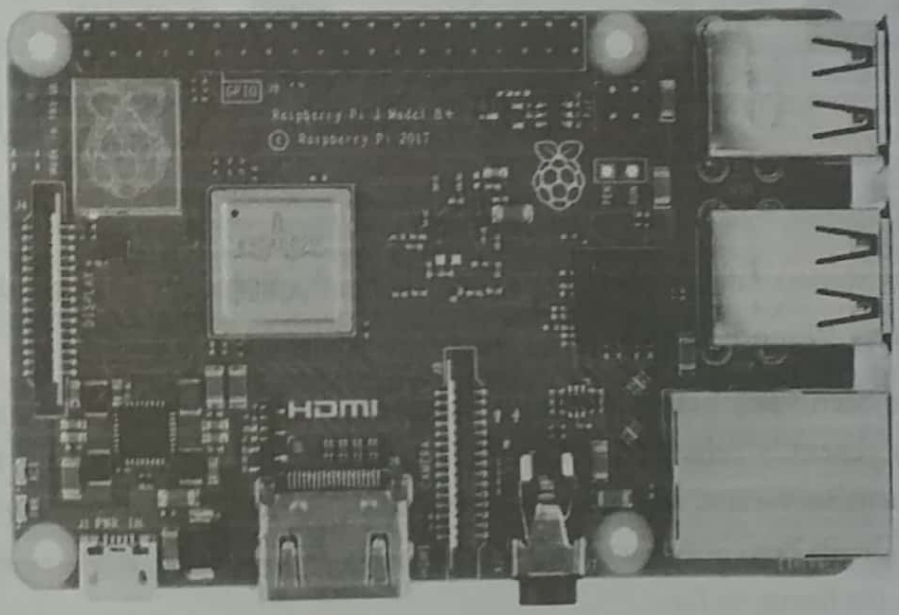
- Arduino is an open-source platform used for building electronics projects. Arduino consists of both a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or IDE (Integrated Development Environment) that runs on your computer, used to write and upload computer code to the physical board.

(1F1)**Fig. 6.1.1 : Arduino**

- The Arduino platform has become quite popular with people just starting out with electronics, and for good reason.
- Unlike most previous programmable circuit boards, the Arduino does not need a separate piece of hardware (called a programmer) in order to load new code onto the board -- you can simply use a USB cable. Additionally, the Arduino IDE uses a simplified version of C++, making it easier to learn to program.
- Finally, Arduino provides a standard form factor that breaks out the functions of the micro-controller into a more accessible package.

6.1.2 What is a Raspberry Pi?

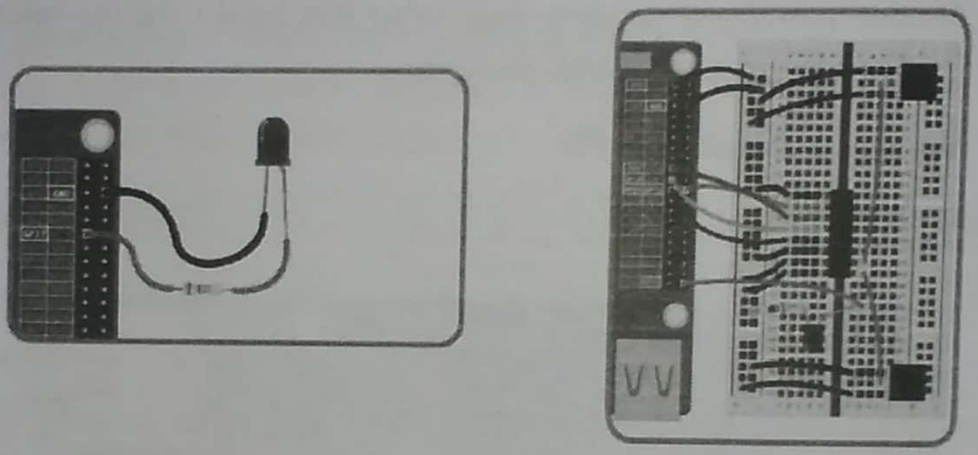
GQ. Explain Raspberry Pi. **(4 Marks)**



(1F2)**Fig. 6.1.2 : Raspberry Pi**

- Raspberry Pi is the name of a series of single-board computers made by the Raspberry Pi Foundation, a UK charity that aims to educate people in computing and create easier access to computing education.
- The Raspberry Pi launched in 2012, and there have been several iterations and variations released since then. The original Pi had a single-core 700MHz CPU and just 256MB RAM, and the latest model has a quad-core CPU clocking in at over 1.5GHz, and 4GB RAM. The price point for Raspberry Pi has always been under $100 (usually around $35 USD), most notably the Pi Zero, which costs just $5.

- All over the world, people use the Raspberry Pi to learn programming skills, build hardware projects, do home automation, implement Kubernetes clusters and Edge computing, and even use them in industrial applications.
- The Raspberry Pi is a very cheap computer that runs Linux, but it also provides a set of GPIO (general purpose input/output) pins, allowing you to control electronic components for physical computing and explore the Internet of Things (IoT).



(1F2)**Fig. 6.1.3 : GIO Pins**

See Getting started with Raspberry Pi and download the Raspberry Pi cheat sheet.

What Raspberry Pi models have been released?

There have been many generations of the Raspberry Pi line: from Pi 1 to 4, and even a Pi 400. There has generally been a Model A and a Model B of most generations. Model A has been a less expensive variant, and tends to have reduced RAM and fewer ports (such as USB and Ethernet). The Pi Zero is a spinoff of the original (Pi 1) generation, made even smaller and cheaper. Here's the lineup so far:

- Pi 1 Model B (2012)
- Pi 1 Model A (2013)
- Pi 1 Model B+ (2014)
- Pi 1 Model A+ (2014)
- Pi 2 Model B (2015)
- Pi Zero (2015)
- Pi 3 Model B (2016)
- Pi Zero W (2017)

- Pi 3 Model B+ (2018)
- Pi 3 Model A+ (2019)
- Pi 4 Model A (2019)
- Pi 4 Model B (2020)
- Pi 400 (2021)

6.1.3 ESP32

1.1 About

- ESP32 is a series of low cost, low power system on a chip microcontrollers with integrated Wi-Fi & dual-mode Bluetooth. The ESP32 series employs a Tensilica Xtensa LX6 microprocessor in both dual-core and single-core variations.
- ESP32 is created and developed by Espressif Systems, a Shanghai-based Chinese company, and is manufactured by TSMC using their 40 nm process. It is a successor to the ESP8266 micro controller.

6.2 FEATURES OF THE ESP32 INCLUDE THE FOLLOWING

GQ. Explain features of ESP 32.

- CPU: Xtensa Dual-Core 32-bit LX6 microprocessor, operating at 160 or 240 MHz and performing at up to 600 DMIPS
- Memory: 520 KiB SRAM
- Wireless connectivity:

  + Wi-Fi: 802.11 b/g/n/e/i

  + Bluetooth: v4.2 BR/EDR and BLE
- Peripheral interfaces:

  + 12-bit SAR ADC up to 18 channels

  + 2 × 8-bit DACs

  + 10 × touch sensors

  + Temperature sensor

  + 4 × SPI

  + 2 × I²S

+ 2 × I²C

+ 3 × UART

+ SD/SDIO/MMC host

+ Slave (SDIO/SPI)

+ Ethernet MAC interface with dedicated DMA and IEEE 1588 support

+ CAN bus 2.0

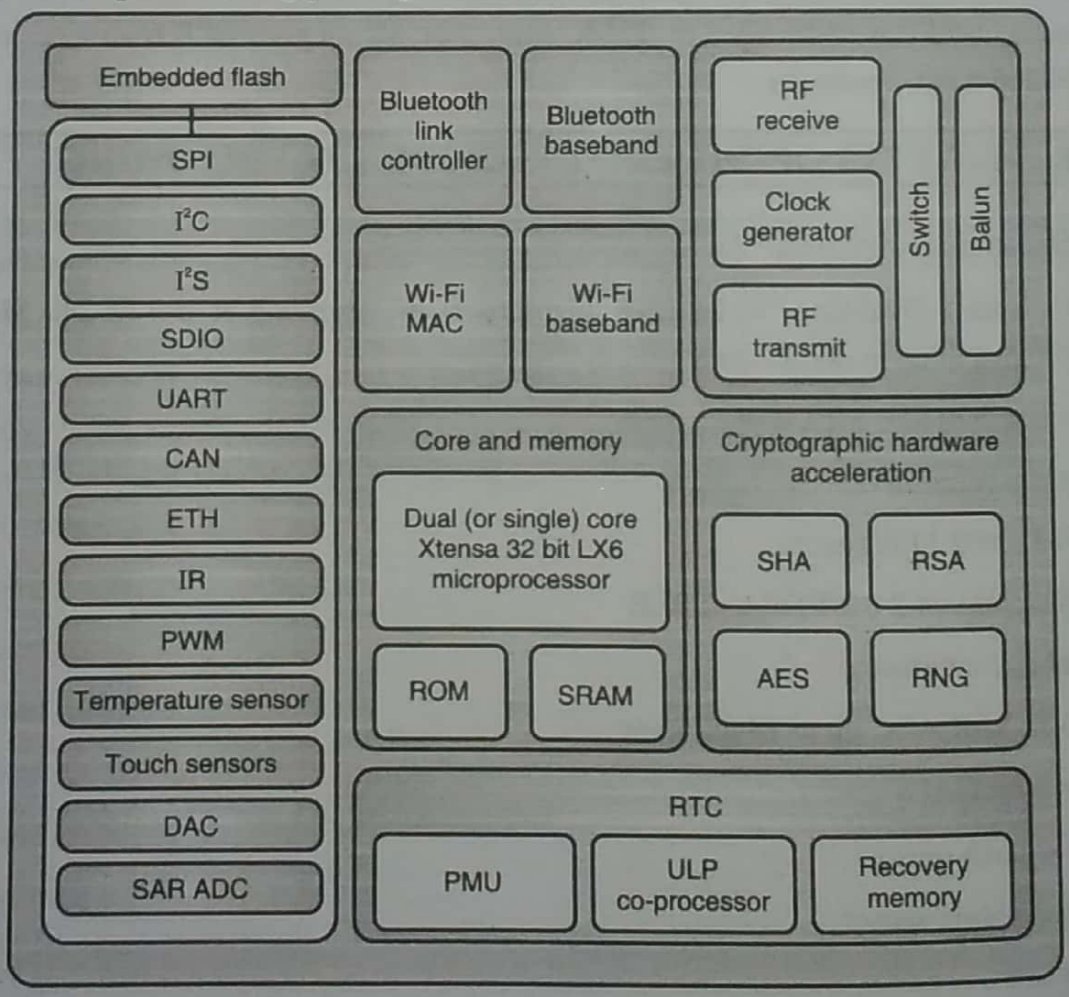
+ IR (TX/RX)

+ Motor PWM

+ LED PWM up to 16 channels

+ Hall effect sensor

+ Ultra low power analog pre-amplifier



(1F4)**Fig. 6.2.1 : ESP32 block diagram**

- Security:

  + IEEE 802.11 standard security features all supported, including WFA, WPA/WPA2 and WAPI

  + Secure boot

  + Flash encryption

  + 1024-bit OTP, up to 768-bit for customers

  + Cryptographic hardware acceleration: AES, SHA-2, RSA, elliptic curve cryptography (ECC), random number generator (RNG)

6.3 ESP8266 VS ESP32

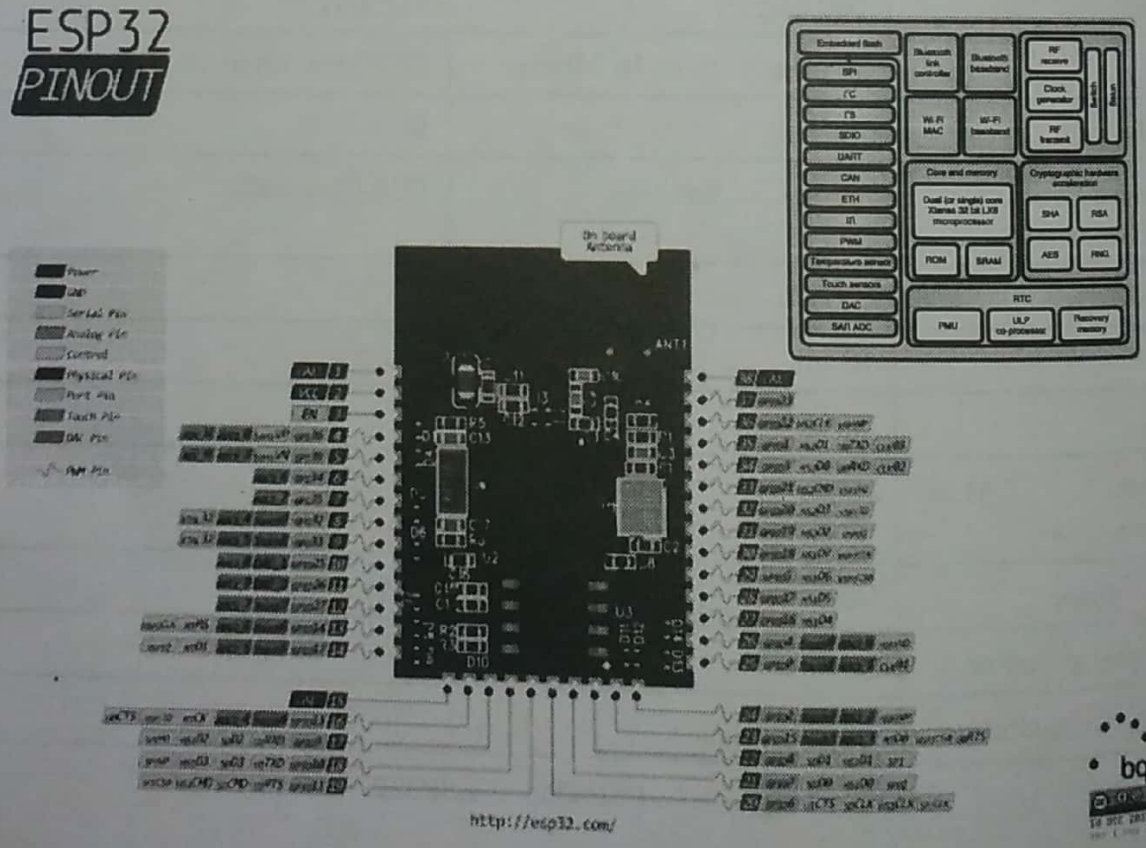
Specifications	ESP8266	ESP12
MCU	Xtensa@ Single-Core 32-bit L106	Xtensa@ Dual-Core 32-bit LX6 600 DMIPS
802.11 b/g/n Wi-Fi	Yes, HT20	Yes HT40
Bluetooth	None	Bluetooth 4.2 and below
Typical Frequency	80 MHz	160 MHz
SRAM	160 kBytes	512 kBytes
Flash	SPI flash. up to 16 Mbytes	SPI flash. up to 16 Mbytes
GINO	17	36
Hardware / Software PWM	None / 8 Channels	1/16 Channels
SPI/12C / 12S / UART	2/1/2/2	4/2/2/2
ADC	10 bit	12 bit
CAN	None	1
Ethernet MAC Interlace	None	1
Touch Sensor	None	Yes
Temperature Sensor	None	Yes
Working Temperature	– 40°C – 125°C	– 40°C – 125°C

Fig. 6.3.1 : ESP8266 vs ESP322

Module boards

ESP32 module boards are small PCBs which directly contain the ESP32 SoC and are designed to be easily used by other circuit boards. Meandered inverted-F antenna designs are used for the PCB trace antennas on the modules listed below. 2 popular module boards same features but different pinout and Vendor.

Vendor	Name	Antenna	Flash memory (DEB)	Description
Espressif	ESP-WR 00M-03	PCB trace	4	Limited distribution, pre7jai-odustiop module created by .Ew-essif for beta testing purposes; this module used the E5P31B, the beta resting chip for the ESP32 series
	ESP-ROOM-32	PCB trace	4	Flagship, public-release ESP32 module board created by Espressif.
Ai-Thinker	ESP-325	PCB trace	4	E5P32 module based On the farm factor of the Espressif ESP-WROOM-32 module. The ESP-325 module replaced the unreleased ESP3212 module

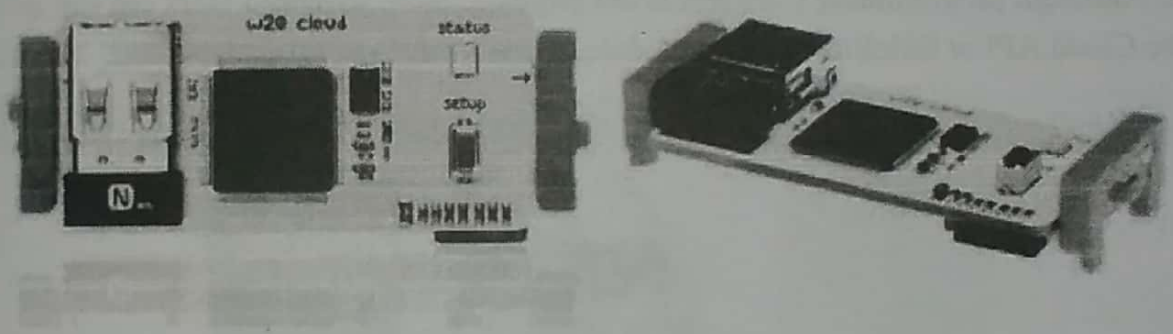


(1F5)**Fig. 6.3.2 : ESP32S module**

6.3.1 littleBits CloudBit Wi-Fi Module Simplifies DIY IoT Designs

GQ. Explain littleBits CloudBit Wi-Fi Module. **(4 Marks)**

- littleBits Electronics is a company selling tiny modules that snap together with tiny magnets for prototyping called littleBits. They do not require soldering, wiring, or programming, can be buttons, sensors, motors, etc., and are the electronics equivalent of LEGO, and are suitable to 8 years old and older kids.
- The company have recently launched a new product called CloudBit, a module based on Freescale i.MX233 with Wi-Fi connectivity meant to be used/snapped with existing littleBits.



(1F6)**Fig. 6.3.3 : little bits**

CloudBit hardware specifications

- Processor – Freescale i.MX233 ARM926EJ-S processor @ 454MHz
- System Memory – 64MB of RAM;
- Storage – microSD slot with included 4GB micro SD card pre-loaded with a customized Arch Linux ARM distribution
- Connectivity – 802.11b/g Wi-Fi via included USB dongle
- USB – micro USB port (for power only)
- Connectors – 2x BitSnap connectors for LittleBits connectivity using i.MX233 ADC/DAC signals
- Debugging – Pads for UART (3.3V, 8-N-1, 115,200 baud) to access the serial console (bottom of the board)
- Misc -Status LED, Setup button
- Power – via USB (power module, wall adapter, and cable included)

- Dimensions – 15 x 10 x 5mm
- Weight – 154 grams

CloudBit also includes a USB power module, and a wall adapter with cable. It runs Arch Linux ARM and leverages node.js technologies. The overall system diagram can be found here.

This little module allows you to connect virtually any device to the Internet, such as a thermostat that turns on when it's too hot or cold, a doorbell that send an SMS or an email, etc... All that "without programming, soldering or wiring required", the company claims. So how do you control it? You can use IFTTT "If this then that" app to connect to online services such as Facebook, Gmail and Twitter, as well as compatible hardware such as Nest and Philips HUE. Although programming CloudBit is not required, more advanced users can still do with via the Cloud API or littleBits Arduino module.

(1F7)**Fig. 6.3.4 : Cloud bits**

☞ Cloud Starter Bundle

- If you are new to littleBits, the CloudBit won't be useful by itself, and that's why the company also offers a Cloud Starter Bundle with CloudBit, the USB power module and wall adapter, but also several littleBits modules namely a "long" LED, a button, a servo, a sound trigger, as well as a mounting board, a sort of breadboard for the company's modules.

- The cloudBit and littleBits can interact with the web and each other in three ways :
  (1) **Bits to Web :** Using hardware to communicate with web services and software
  (2) **Web to Bits :** Communicating events in the web to the CloudBit, using for example, the company's Cloud Control or the third party IFTTT app.
  (3) **Bits to Bits :** Communicating from machine to machine
- The company features several demo projects with instructions including a chicken feed monitoring system, a remote fish/pet feeder, a baby monitor, an SMS doorbell, etc... and they also provide a few IFTTT samples, as tutorials.
- You can find all the documentation you need on CloudBit and Cloud Starter Bundles product pages, as well as purchase them respectively for $59 and $99, plus shipping.

6.3.2 Introduction To Particle

GQ. Write a short note on Particle. **(2 Marks)**

Fig. 6.3.5

Introduction

- Particle is an Internet of Things device platform which enables a developer to quickly and easily build, connect and manage their connected systems/applications.
- It provides ease for connecting things to the Internet/Web.
- Particle has come up with the different Internet of Things development kit which is mainly designed for creating IoT based applications.

- Particle's IoT based platform provides everything that is necessary to build a connected system/application like a smart home.
- All the Particle Devices come with free access to the Particle Cloud. The Cloud serves as the gateway between your devices and the web.
- The Particle Cloud has some great features for building connected projects, including Over-The-Air (OTA) firmware updates, an easy-to-use REST API, and firmware development supported by web and local IDEs.
- OTA (Over-The-Air) technique is useful for wirelessly updating firmware and configuration settings of Particle IoT devices remotely.
- Particle comes with access to a set of development tools - a Web IDE, Desktop IDE(Dev) and a CLI (Command Line Interface).

Why Particle?

- Particle provides many types of boards related to the Internet of Things (IoT) platforms which are useful for various applications.
- Particle provides its own web IDE, Dev IDE (Integrated Development Environment) and command line interface (CLI) which is free to download from Particle website and use.
- The main thing in Particle is you do not require a cable connection while flashing the code or programming, it can flash the code over the air (OTA).
- The program structure for Particle is built with Arduino compatible. This allows us to compile and run codes as it is from Arduino.
- The same libraries of Arduino can be useful for the particle photon. The functions implemented in these libraries can be used for quick development purposes.
- This is very useful for developers who are focused on building innovative applications and proof of concepts. The developers can spend more time on developing the applications rather than on developing the sub-modules used in building the applications.

Particle's Devices/Boards

Particle has designed various development boards which are useful for building IoT based systems/applications. The list of these boards is as follows,

☞ **Particle Photon (Wi-Fi)**

Particle Photon is a very small Wi-Fi development kit which is designed for creating connected projects and applications for the Internet of Things (IoT). It has a powerful 120Mhz ARM Cortex M3 microcontroller with an on-board Broadcom Wi-Fi chip.

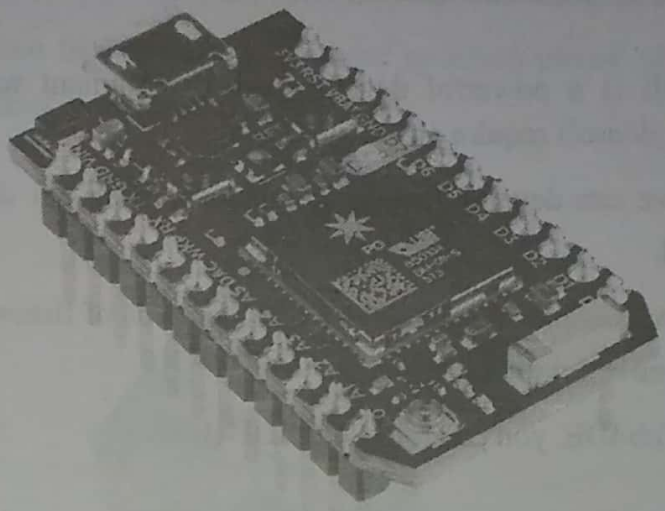


Fig. 6.3.6 particle Photon (Wi fi)

☞ **Particle Photon**

Particle Electron (Cellular)

- Particle Electron is a tiny Cellular(2G/3G) based development kit that can be used for creating connected projects and applications. It comes with a Particle SIM card with a data plan for low bandwidth applications.

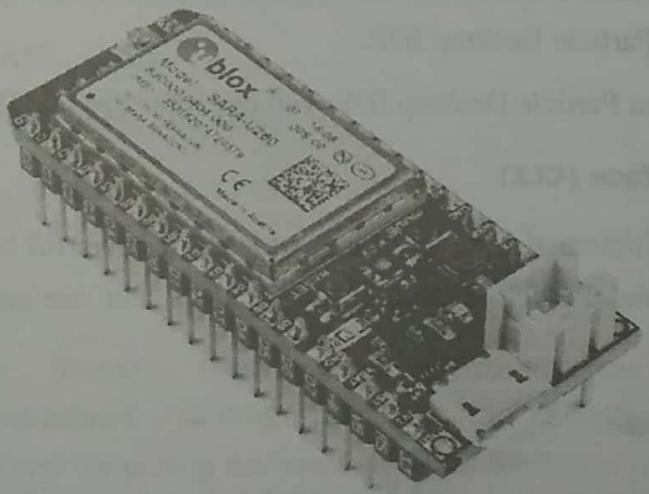


Fig. 6.3.7 Particle Electron (Cellular)

☞ **Particle Electron**

Particle's IDE

Particle has 3 different IDE platforms for developing applications.

Web IDE

- Particle's Web IDE is a powerful development environment which can run in your favorite browser. It doesn't require any setup to use.
- Using Web IDE, we can develop debug, compile and flash our devices from anywhere (OTA) in the world.
- We can access many sample code examples and hundreds of firmware libraries from any computer with an active Internet connection.

To know more about Web IDE, you can refer Web IDE (Build).

Desktop IDE (Dev)

- Particle's Desktop IDE is used as a local development environment. It is very easy to use the IDE.
- It provides advanced features that make managing large or complicated firmware projects fast, easy and efficient. But it requires internet access as the Desktop IDE is not an offline development tool. It uses the internet to push files to the cloud for compilation and returns binary.
- It is easy to download and install for Windows, Linux, and MacOS. To download Desktop IDE, you can visit Particle Desktop IDE.
- To know more about Particle Desktop IDE, you can refer Particle Desktop IDE.

Command Line Interface (CLI)

- Particle has CLI (Command Line Interface) which is a powerful tool for interacting with particle's devices and Particle Cloud. It uses node.js and can easily run on Windows, Linux, and MacOS.

6.3.3 BeagleBone

- BeagleBone is an "opensource hardware" which is having a credit card sized foam factor. It was the first in its kind, which becomes famous for its small size, but having high capability.
- Unlike its ancestors such as BeagleBoard or BeagleBoard-xM, it has plenty of input-output pins which can be used by hackers and hardware lovers for interfacing linux with their favorite sensors without any kernel level modifications.

- Moreover, its arduino like design can be used to attach plenty of capes, which will add wings to itscapabilities even further.

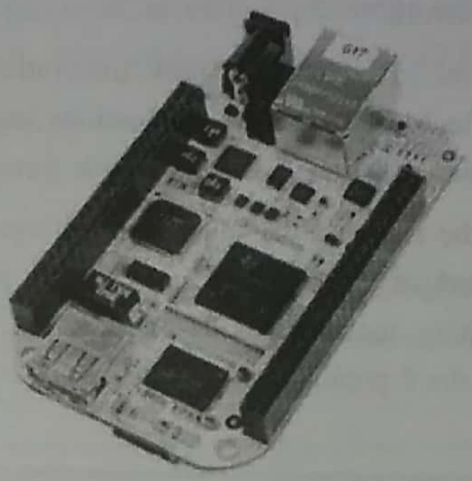


Fig. 6.3.8

- Major features are as follows
  (1) 256MB DDR2 RAM
  (2) 3D graphics accelerator
  (3) ARM Cortex-M3 for power management
  (4) 2x PRU 32-bit RISC CPUs
  (5) USB client: power, debug and device
  (6) USB host
  (7) Ethernet
  (8) 2x 46 pin headers
- Many opensource projects based on BeagleBone can be found under http://beagleboard.org/project. Getting Started page contains all the necessary informations and drivers for getting the board up out of the box in just few minutes.
- The SD Card which comes bundled with the pack contains Angstrom Linux Distribution, has all the necessary tools to begin development. This production version image can also be obtained from here. Apart from the Angstrom distribution users can easily switch to other distros like Ubuntu, ArchLinux or Android. More hacking tips on BeagleBone will be made available soon

- Internet of Things (IoT) concerned with the network of physical devices that are embedded with several technologies in order to connect, communicate and share the data with each other over the network.
- The major components of the IoT are connectivity, integration, cloud computing, sensing, & various others and the technology has its applications in multiple areas whether it be Smart IoT devices for Homes, Health Care, Automation, Retail, etc.
- There is no doubt about the fact that the Internet of Things is the next big thing in the Information Technology industry. Most of the developers and technical enthusiasts have already focused on learning the new skills required to pursue the career. In this whitepaper, we list down the 8 popular open source popular programming languages for IoT development.

6.4 IOT SOFTWARE - LANGUAGES FOR PROGRAMMING IOT HARDWARE

GQ. Explain different IOT software. **(4 Marks)**

1. JAVA

- When it comes to IoT Development, JAVA stands out among the most popular programming languages.
- One of the prominent features that make JAVA favorable for the Internet of Things (IoT) Development is Write Once, Run Anywhere concept which implies that the compiled JAVA code can run on any platform that supports the language without compiling it again.
- In general, the JAVA codes are compiled to byte code that can run on any JAVA Virtual Machine conveniently. Moreover, the object-oriented language allows you to build the applications compatible for both – Edge nodes as well as Cloud.
- Furthermore, the languages come up with various other renowned features such as an *extensive built-in library*, *highly interoperable*, etc. beneficial for the IoT Development.

2. Python

- Python is another most-recommended programming language compatible for the IoT Development. It is an interpreted language that supports the programming standards of object-oriented programming as well as functional and structured programming.

- The high-level programming language has an easier syntax and better code readability that makes it one of the most preferred languages for IoT by the developers.
- Also, the language can work on various platforms such as Windows, Linux, etc. and can be integrated with other languages such as *C++*, *Java*, etc. conveniently.
- Moreover, the language has *rich library support*, *large community support*, and various other features, and also it is much suitable for data-intensive applications.

3. **C**

- How can we forget this much-acclaimed programming language!! C can be considered as one of the most widely used programming languages in the Internet of Things (IoT) world.
- The middle-Level programming language allows you to understand the underlying architecture of programming that *provides the required flexibility to the IoT Developers*. Moreover, the language has several other prominent features also such as *portability*, *rich library*, and many more.
- Furthermore, the language is pretty much compatible with the micro-controllers required for the IoT devices. However, it requires more effort and time as well to learn C Language effectively due to its not-so-easy syntax and layered architecture.

4. **LUA**

- However, LUA is not one of the usual names in the computer programming word but when it comes to IoT Development, it has already made its strong presence among the developers.
- LUA is a *general-purpose, high-level programming languag*e that is specifically designed for embedded purposes. The extensible procedural language is aimed to support data description facilities and it is required to be embedded in a host client for successful functioning.
- Moreover, LUA comes up with its most preferred framework *Node.lua built on a lightweight LUA interpreter* that helps the developers to create IoT-based applications and various other enriching features such as better efficiency, portability, etc.

5. **Golang**

- Golang, sometimes referred to as Go, is also one of those best languages that can be taken into consideration for IoT Development. In general, Golang is an open-source statically typed programming language, developed by Robert Griesemer, Rob Pike, and Ken Thompson at Google.

- The language offers several prominent features such as inbuilt concurrency (goroutines & channels) and the ability for the maximum usage of the hardware that makes it more compatible and relevant for the IoT development.
- Furthermore, the language provides several other crucial features also such as the rich standard library, dynamic-typing capability, etc. that can also be considered by the developers.

6. PHPoC

- If you're familiar with PHP (Hypertext Preprocessor) Language then to relate with the PHPoC (PHP on Chip) is not a big deal for you!! Meanwhile, PHPoC (PHP on Chip) is a programming language (based on PHP Language) and an IoT hardware platform. Even the syntax of PHPoC is almost similar to the PHP language.
- However, it can be considered that PHPoC is not only a web development language but also a general-purpose programming language compatible and suitable for IoT.
- Moreover, apart from the core PHP functions, PHPoC also includes several *additional functions like SPI, UART, RTC,* and various others beneficial for the IoT Development.

7. Swift

- Last but not least – Swift!! If we talk about the language introduction – Swift is a *general-purpose, multi-paradigm programming language* that is specifically designed to create applications for iOS, iPadOS, macOS, watchOS, and tvOS.
- The language comes up with several prominent features such as *powerful error handling, functional programming patterns, fast & secure*, and many more.
- However, as mentioned above that Swift is particularly concerned with the development of applications for Apple's devices so if you're looking forward to doing IoT development for these particular platforms such as iOS, macOS, etc. then you're strongly recommended to opt for Swift otherwise you can go with other languages as well.
- So these are several programming languages that you can take into consideration to learn IoT Development. Meanwhile, you can opt for a language (from the above-mentioned list or other than that) based on your own preferences, *for example – if you're looking for a language for IoT development with the easier syntax you can go with Python or if want to learn IoT for iOs & macOS devices you can opt for Swift, and so on.*

- However, whichever language you'd choose, you're required to do hard work with all the dedication and consistency to accomplish your goals!!

☞ Open-source Middleware Software Solutions

Open-source middleware application development tools are free to use and thus, they significantly reduce the overall project costs. Many of these platforms are used by a large number of small-to-medium enterprises as well as fortune 500 companies. Below are some examples of the most sought-after open-source middleware platforms that are also effective at building IoT middleware software solutions.

#1 Talend

- Talend, a market leader in cloud data integration, provides open-source middleware software solutions for enterprises to strengthen their software infrastructure.
- Talend's middleware application development platform enables enterprises to bridge the gap between disparate software components and heterogeneous enterprise IoT applications.
- Besides, it renders complete support to address a wide range of data integration and implementation requirements through middleware application development.
- Talend provides a unified software application suite that provides dedicated tools for diverse middleware project requirements. Other features include built-in data quality and data governance capabilities.
- Most importantly, developers don't need additional tools or switch between different software environments since they have all the required tools at their disposal.

#2 Apache Camel

- Apache Camel is a Java-based software integration framework that provides message-oriented middleware software solutions for varied business needs.
- It is an open-source framework with a rule-based routing and mediation engine that enables developers to implement enterprise integration patterns using custom APIs. In doing so, they can easily configure the given routing and mediation rules.
- Apache Camel supports several functions including Bean Binding (for Java objects) and JavaBeans. As a result, it makes it easy for developers to integrate many heterogeneous applications regardless of their software model or underlying technologies.

- Apache Camel is quite often used with several other software platforms like Apache ServiceMix, Apache CXF, and Apache ActiveMQ to address different project requirements.

#3 MuleSoft ESB

- Mule ESB (enterprise service bus) is an open-source software platform that incorporates Java-based programming for middleware application development.
- It is a lightweight integration platform by MuleSoft Inc. that enables developers to interconnect various applications, software components, and distributed systems regardless of their heterogeneity. Mule ESB is effective at handling a diverse range of applications built on top of the technologies like HTTP, JMS, JDBC, web services, and many others.
- Developers can deploy the ESB anywhere to integrate or orchestrate various events in several batches. Mule ESB offers universal connectivity and can also be deployed in real-time for software integration and orchestration.

☞ **Zetta**

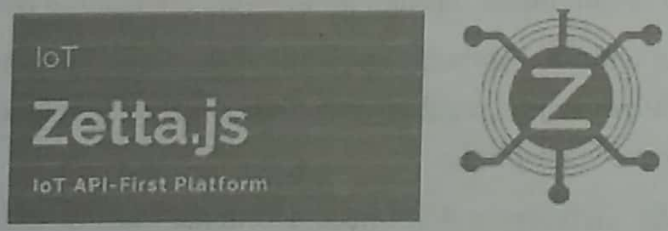


Fig. 6.4.1

Zetta is API based IoT platform based on Node.js. It is considered as a complete toolkit to make HTTP APIs for devices. Zetta combines REST APIs, WebSockets to make data-intensive and real-time applications. The following are some notable features.

- It can run on the cloud, or a PC, or even modest development boards.
- Easy interface and necessary programming to control sensors, actuators, and controllers.
- Allows developers to assemble smartphone apps, device apps, and cloud apps.
- It is developed for data-intensive and real-time applications.
- Turns any machine into an API.

☞ **Arduino**

Fig. 6.4.2

- If you are seeking to make a computer that can perceive and exercise stronger control over the real world when related to your ordinary stand-alone computer, then Arduino can be your wise preference.
- Offering an appropriate blend of IoT hardware and software, Arduino is a simple-to-use IoT platform. It operates through an array of hardware specifications that can be given to interactive electronics. The software of Arduino comes in the plan of the Arduino programming language and Integrated Development Environment (IDE).

☞ **OpenRemote**

OpenRemote has introduced a new open-source IoT platform to create professional energy management, crowd management, or more generic asset management applications.

Summing up the most important features:

- Generic asset and attribute model with different assèt types
- Protocol agents like HTTP REST or MQTT to connect your IoT devices, gateways, or data services or build a missing vendor-specific API.
- Flow editor for data processing, and a WHEN-THEN and a Groovy UI for event-based rules.
- Standard Dashboard for provisioning, automating, controlling, and monitoring your application as well as Web UI components to build project-specific apps.
- Android and iOS consoles which allow you to connect to your phone services, e.g., geofences, and push notifications.

- Edge Gateway solution to connect multiple instances with a central management instance.
- Multi-realms multi-tenant solution, combined with account management and identity service.

☞ **Node-RED**

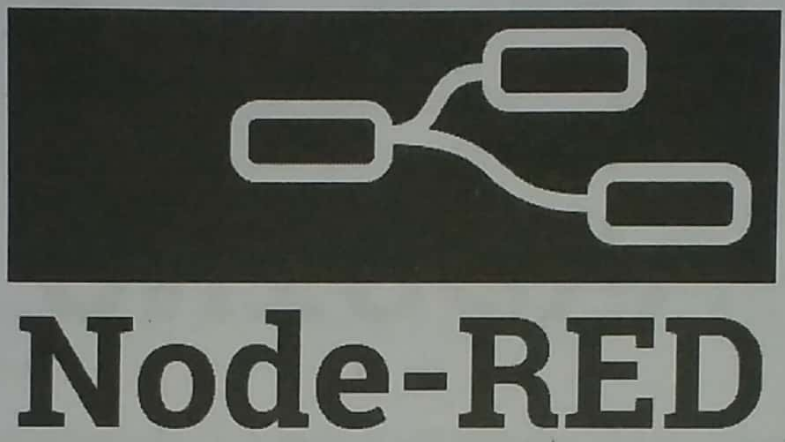


Fig. 6.4.3

- Node-RED is a visual tool for lining the Internet of Things, i.e., wiring together hardware devices, APIs, and online services in new ways. Built on Node.js, Node-RED describes itself as "a visual means for wiring the Internet of Things."
- It provides developers to connect devices, services, and APIs using a browser-based flow editor. It can run on Raspberry Pi, and further 60,000 modules are accessible to increase its facilities.

☞ **Flutter**

Fig. 6.4.4

- Flutter is a programmable processor core for electronics projects, designed for students, and engineers. Flutter's take to glory is it's long-range. This Arduino-based board includes a wireless transmitter that can show up to more than a half-mile. Plus, you don't require a router; flutter boards can interact with each other quickly.

- It consists of 256-bit AES encryption, and it's simple to use. Some of the other features are below.
  - Fast Performance
  - Expressive and Flexible UI
  - Native Performance
  - Visual finish and functionality of existing widgets.

M2MLabs Mainspring

- M2MLabs Mainspring is an application framework for developing a machine to machines (M2M) applications such as remote control, fleet administration, or smart terminal. Its facilities include flexible design of devices, device structure, connection between machines and applications, validation and normalization of data, long-term data repository, and data retrieval functions.
- It's based on Java and the Apache Cassandra NoSQL database. M2M applications can be modeled in hours rather than weeks and subsequently passed on to a high-performance execution environment made on top of a standard J2EE server and the highly-scalable Apache Cassandra database.

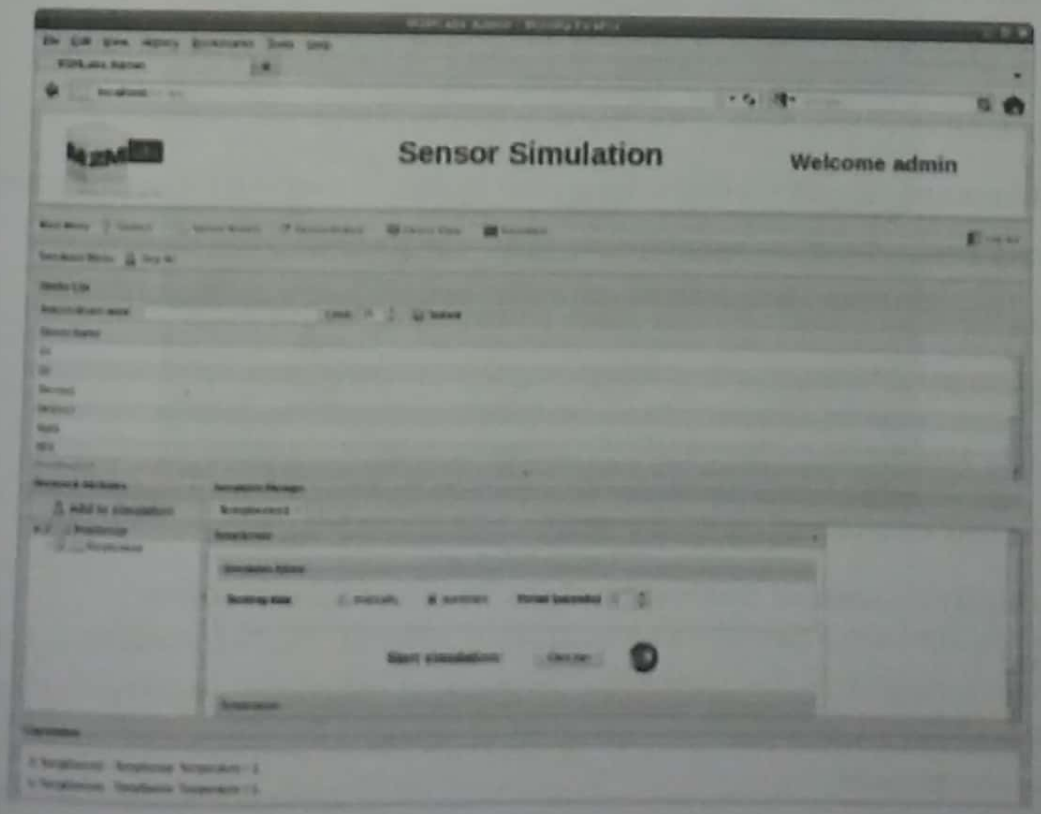


Fig. 6.4.5 M2MLabs

☞ **ThingsBoard**

ThingsBoard

Fig. 6.4.6

ThingsBoard is for data collection, processing, visualization, and device management. It upholds all standard IoT protocols like CoAP, MQTT, and HTTP as quickly as cloud and on-premise deployments. It builds workflows based on design life cycle events, REST API events, RPC requests.

Let's take a look at the following ThigsBoard features.

- A stable platform that is combining scalability, production, and fault-tolerance.
- Easy control of all connected devices in an exceptionally secure system
- Transforms and normalizes device inputs and facilitates alarms for generating alerts on all telemetry events, restores, and inactivity.
- Enables use-state specific features using customizable rule groups.
- Handles millions of devices at the same time.
- No single moment of failure, as every node in the bundle is exact.
- Multi-tenant installations out-of-the-wrap.
- Thirty highly customized dashboard widgets for successful user access.

☞ **Kinoma**

- Kinoma, a Marvell Semiconductor hardware prototyping platform, involves three different open source projects.
- Kinoma Create is a DIY construction kit for prototyping electronic devices.

Kinoma

Fig. 6.4.7

- Kinoma Studio is the development environment that functions with Set up and the Kinoma Platform Runtime.
- Kinoma Connect is a free iOS and Android app that links smartphones and stands with IoT devices.

☞ **Kaa IoT Platform**

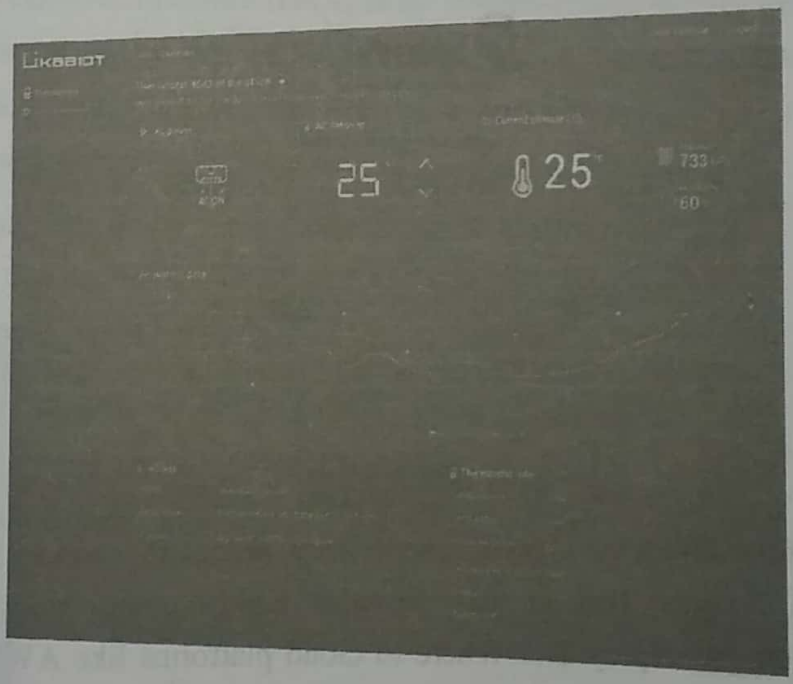


Fig. 6.4.8 Kaa IOT

Kaa is a production-ready, flexible, multi-purpose middleware platform for establishing end-to-end IoT solutions, connected applications, and smart devices. It gives a comprehensive way of carrying out effective communication, deals with, and interoperation capabilities in connected and intelligent devices.

It mounts from tiny startups to a great enterprise and holds advanced deployment models for multi-cloud IoT solutions. It is primarily based on flexible microservices and readily conforms to virtually any need and application some other features as below.

- Facilitates cross-device interoperability.
- Performs real-time device control, remote device provisioning, and structure.
- Create cloud services for smart products
- Consists of topic-based warning systems to provide end-users to deliver messages of any predefined format to subscribed endpoints.
- Perform real-time device monitoring
- Manage an infinite quantity of connected devices
- Collect and analyze sensor data

☞ **SiteWhere**

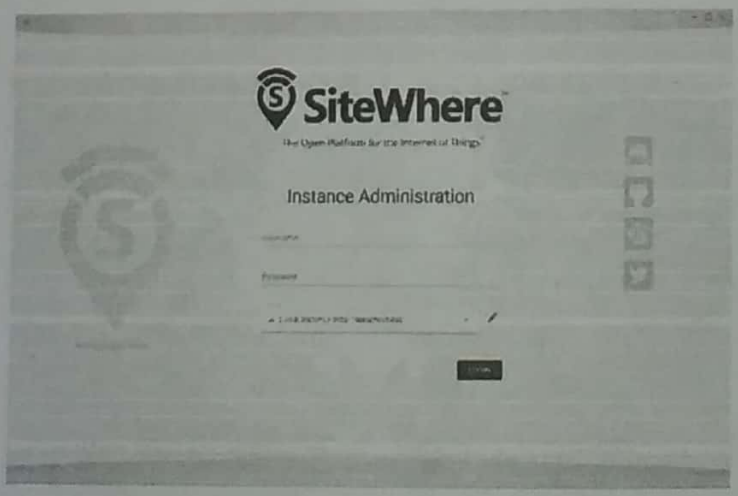


Fig. 6.4.9

SiteWhere platform offers the ingestion, repository, processing, and assimilation of device inputs. It runs on Apache Tomcat and provides highly tuned MongoDB and HBase implementations. You can deploy Site Where to cloud platforms like AWS, Azure, GCP, or on-premises. It also supports Kubernetes cluster provisioning.

The following are some of the other features.

- Run any estimate of IoT applications on a single SiteWhere instance
- Spring brings the root configuration framework.
- Add widgets through self-registration, REST services, or in batches.
- InfluxDB for event data storage

- Connect devices with MQTT, Stomp, AMQP and other protocols
- Integrates third-party integration frameworks
- Eclipse Californium for CoAP messaging
- HBase for the non-relational datastore
- Grafana to visualize SiteWhere data

☞ **DSA**

- Distributed Services Architecture (DSA) is for implementing inter-device communication, logic, and efforts at every turn of the IoT infrastructure. It allows cooperation between devices in a distributed manner and sets up a network engineer to share functionality between discrete computing systems.
- You can manage node attributes, permission, and links from DSLinks.

☞ **Thinger**

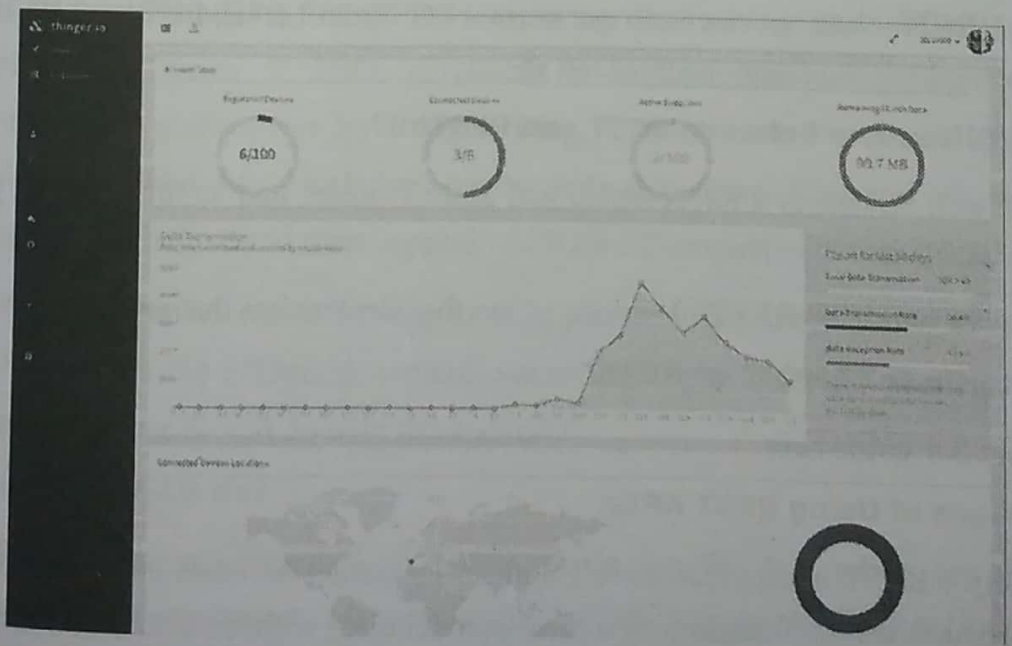


Fig. 6.4.10 Thinger

- Thinger.io provides a scalable cloud base for connecting devices. You can deal with them quickly by running the admin console or combine them into your project logic using their REST API. It supports all types of hackers boards such as Raspberry Pi, Intel Edison, ESP8266.
- Thinger can be integrated with IFTT, and it provides real-time data on a beautiful dashboard.

6.4.1 For Making front ends, REST and JSON-LD

What is REST API?

- REST stands for Representational State Transfer. It's an architectural style for developing web services. A lot of people believe that there is a REST protocol in IoT. However, REST itself is a concept, not an IoT protocol.
- REST is the basis for the most widely used form of API and is designed to be used over any protocol. However, it typically uses HTTP or COAP to work with components in a particular IoT device, such as:
  - Files
  - Objects
  - Media
- Web services are defined on the principles of REST and can be defined as a RESTful web service. RESTful web services can use normal POST, DELETE, PUT, and HTTP verbs of GET for working the components listed above.

What's the Difference between REST and RESTful?

A REST web service is a Representational State Transfer and an architectural pattern for creating web services.

On the other hand, the RESTful service is one that implements that pattern.

What's better in IoT? MQTT or REST?

Check out our guide here

Advantages of Using REST APIs

1. **Scalability :** REST means that there's a clear separation between client and server. As a result, products can be scaled up by a development team without much difficulty.

2. **Familiarity and Usability :** REST APIs use constructs that are familiar to anyone who has used HTTP – i.e. the internet. Unless you're completely off the grid, you'll have used the internet before.

   On top of that, most IoT developers are already familiar with the REST architecture, such as SSL and TLS. This makes REST APIs the most easy-to-use API out there.

3. **Language-independent :** Developers can use any language that uses HTTP to make web-based requests. This is another reason why REST APIs are so popular with developers. They give you the power to program using a language you're comfortable and familiar with to develop your IoT app.

☞ **Disadvantages of Using REST APIs**

1. **Limited Architecture :** While the simple architecture of REST is a great entry point for budding IoT developers, those who want to do more or work with REST frequently may encounter limitations due to its architecture.

6.4.2 What is JSON-LD?

- JSON-LD stands for *JavaScript Object Notation for Linked Data*, which consists of multi-dimensional arrays (think: list of attribute-value pairs).
- It is an implementation format for structuring data analogous to Microdata and RDFa. Typically, in terms of SEO, JSON-LD is implemented leveraging the Schema.org vocabulary, a joint effort by Google, Bing, Yahoo!, and Yandex in 2011 to create a unified structured data vocabulary for the web. (However, Bing and other search engines have not officially stated their support of JSON-LD implementations of Schema.org.)
- JSON-LD is considered to be simpler to implement, due to the ability to simply paste the markup within the HTML document, versus having to wrap the markup around HTML elements (as one would do with Microdata).

What does JSON-LD do?

JSON-LD annotates elements on a page, structuring the data, which can then be used by search engines to disambiguate elements and establish facts surrounding entities, which is then associated with creating a more organized, better web overall.

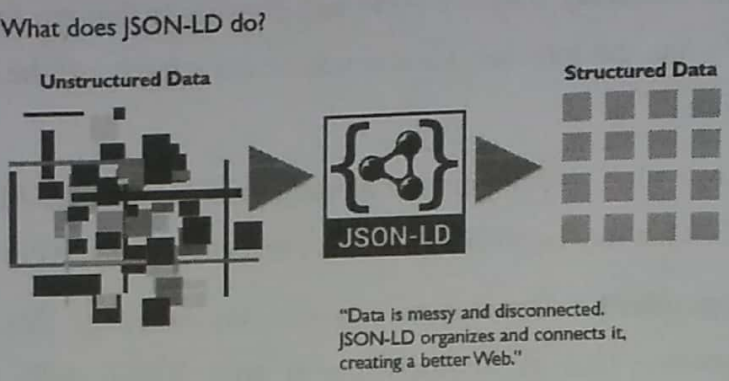


Fig. 6.4.11 : A conceptual visualization of JSON-LD taking the unstructured content on the web, annotating, and structuring the content to create an organized, structured result.

6.5 COMPARISON OF IOT BOARDS AND PLATFORMS

A comparison of IoT boards and platforms in terms of computing, IDE, Connectivity

Parameter	RASPBERRY PI	BEAGLEBONE BLACK
Model Tested	It uses Model B version.	It uses Rev A5 version.
Processor Type	It uses ARM11 processor.	It uses ARM Cortex-A8 processor.
RAM	For the functioning of raspberry pi, 512 MB SDRAM is used.	For the functioning of beaglebone black, 512 MB DDR3L is used.
Processor Speed	It uses 700 MHz for processing.	It uses 1 GHz for its processing.
Flash	It has dedicated SD Card socket for loading operating system.	It uses 4GB (micro SD) for loading OS and data storage.
Min Power	It requires a power supply of 700mA (3.5W).	It requires min power of 210mA (1.05W) for its functioning.
GPIO Pins	It has 12 GPIO pins.	It has 69 GPIO pins.
Dev IDE	It uses IDLE, Scratch, Squeak/Linux to perform tasks.	It uses Python, Scratch, Squeak, Cloud9/Linux to perform a particular task.

Parameter	RASPBERRY PI	BEAGLEBONE BLACK
USB Master	It has 2 USB 2.0 on board.	It has 1 USB 2.0 on its board.
Audio Output	Supports HDMI, Analog audio output	It uses Analog output for audio.
Video Output	It supports HDMI, Composite output for video.	No such specific video output.
UART	It uses 1 UART to transmit and receive serial data.	It uses 5 UART to transmit and receive serial data.
No. of I/O pins	It has 8 Digital, 0 Analog pins.	It has 65 Digital, 7 Analog pins.

6.6 A COMPARISON OF BOARDS AND PLATFORMS IN TERMS OF CONNECTIVITY

Platform	Connectivity	Microcontroller	Cost
Arduino Yun	WiFi & Ethernet	ATmega32u4 & AtherosAR9331	S75
Raspberry Pi	WiFin BLE & Ethernet	64 bit ARM Cortex-A53 Quad Core	S40
ESP8266	WiFi	Tensilica L106 32-bit	S3
Beaglebone Black	WiFi & BLE	OSD 3358ARM 1 GHz Cortex-AS	S70
Particle Photon	WiFi	STM32F205 120 MHz ARM Cortex M3	S20
Arduino Nano	Nil	ATmega328	S3

Arduino

- Arduino will be one of the first IoT hardware to come in mind when thinking about building a simple connected device. Arduino microcontrollers are open-source hardware which means that basically anyone can build it. There's a wide range of Arduino versions including the most popular Arduino Uno, Arduino YUN with enabled WiFi connectivity and Arduino MKR family that offers multiple wireless connectivity options such as WiFi, Bluetooth, LoRa, SigFox and Narrowband IoT.

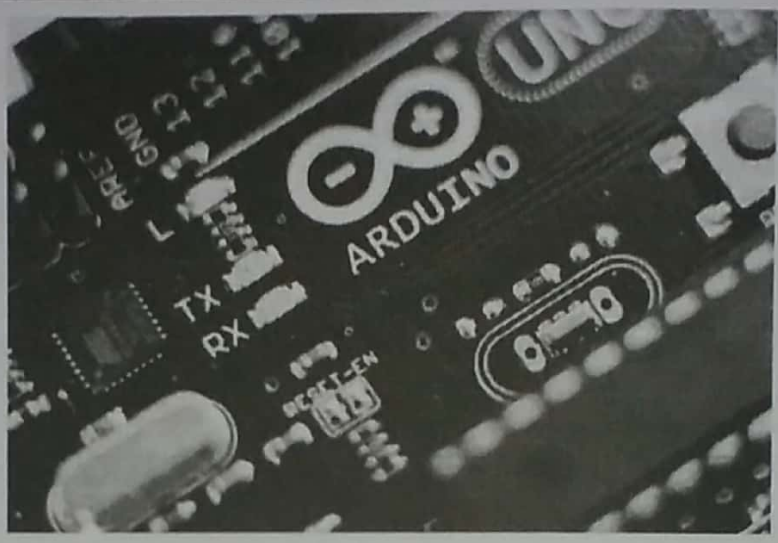


Fig. 6.6.1 : Arduino

- Apart from hardware, Arduino offers IDE (integrated development environment) and recently released Pro IDE for easier and faster coding. The platform has a well-established community, online software tools, various development kits, Arduino IoT Cloud and other resources for building connected devices.
- To learn more about Arduino hardware, check this article.

Why choose Arduino as an IoT hardware platform?

- Arduino hardware is an affordable and easy to set up option for building a basic IoT device that is supposed to perform one action, for example, read humidity sensor data.
- Arduino community is one of the oldest in this domain, so there won't be a lack of support or resources. On top of that, Arduino's functionality is easily expandable with on-top shields and multiple digital and analog general-purpose input/output pins.

☞ **Raspberry Pi**

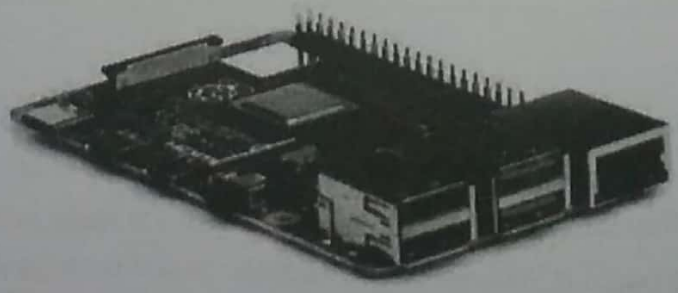


Fig. 6.6.2 : Raspberry Pi

- Raspberry Pi is another story. Pis are originally small fully-fledged computers with a range of connectivity options, a processor and up to 8GB of memory storage. It's much more powerful and speedy than other IoT boards and can handle complex functionality including data-heavy audio and video streaming.
- Just like Arduino, Raspberry Pi has its own community, accessory set, set-up and troubleshooting guides and multiple resources for developers. However, Raspberry Pi is closed-source hardware, so to build a Pi-based application, you'll need to use the boards, accessories and kits offered by the producer.

Why choose Raspberry Pi as an IoT hardware platform?

- Raspberry Pi is the best choice for data-heavy connected devices like hubs, gateways, datum collectors or personal cloud servers, however, it will also be a good fit for simpler IoT applications.
- There're several generations and various models of Pis with different componentry and price range starting from $5. Original models already have connectivity options, inputs and outputs on-board, so no on-top modules or soldering are needed for setting up basic functionality. As a rule, Pi-based solutions are low-powered, however, they require more power than Arduino considering higher processing capabilities.

☞ **Particle**

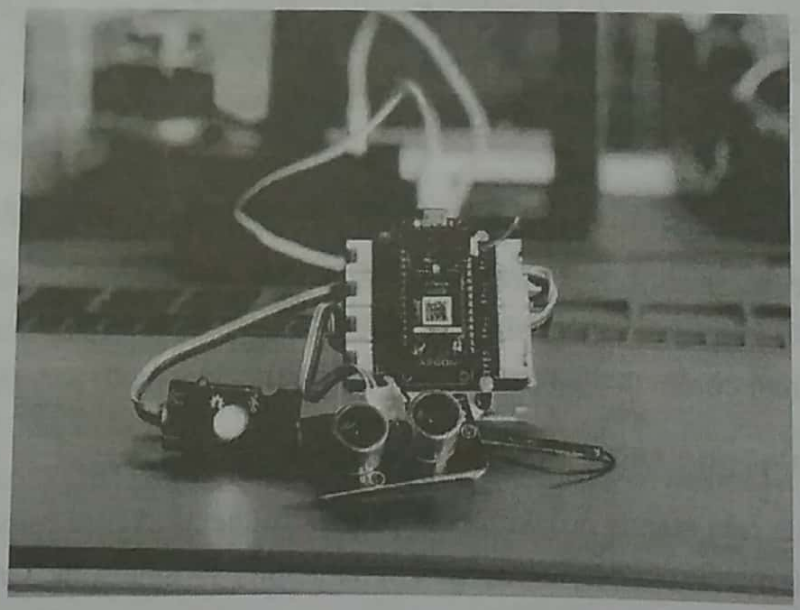


Fig. 6.6.3 : Particle application

- Particle is, probably, the most complete IoT hardware platform which offers Internet of Things hardware, connectivity, cloud and drag-and-drop IoT application builder. Apart from that, Particle has a serious developer community, its own IDE, developer tools, SDKs and numerous kits for different purposes and IoT projects.

- In terms of hardware, Particle provides boards with different types of connectivity, for example, Boron with cellular and mesh, Photon with WiFi or Xenon with mesh only. Additionally, there's a wide range of accessories, sensors and other add-ons with detailed specifications and instructions.

Why choose Particle as an IoT hardware platform?

- Particle is an all-inclusive platform that covers all bases not only for IoT prototyping but also for building a fleet of ready-to-go IoT devices. Basically, you have everything you need in one place hardware, development environment and tools, cloud and robust support from the community. Another benefit of the Particle platform is the mesh-ready hardware and connectivity which is getting more and more popular among IoT connectivity options.

☞ **BeagleBone**

- BeagleBone is an IoT hardware platform with open-source hardware, various daughter boards or capes to add functionality to main IoT development boards, strong Beagle community of developers and enthusiasts who promote open software and hardware in embedded computing.

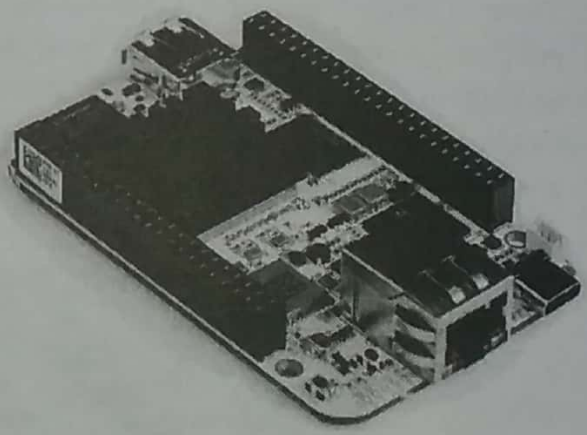


Fig. 6.6.4 : Begal bone black

- BeagleBone Linux-based boards are very diverse. They come in different sizes and feature sets, from the most basic PocketBeagle to AI-enabled BeagleBone AI with 1GB RAM and 16GB of flash memory, embedded vision engines and common connectivity options WiFi, Bluetooth and gigabit Ethernet.

Why choose BeagleBone as an IoT hardware platform?

- BeagleBone platform stands out with pretty powerful yet uncomplicated boards and great compatibility and connectivity options. For example, BeagleBone Green has 2 sets of 46 pin headers. This is a lot of I/O pins to connect to, so you can add multiple sensors and modules to your original board. Unlike Arduino or Particle, BeagleBone doesn't offer IDE but works with an open-source Cloud9 programming platform.

Let's discuss your project.

☞ **Adafruit**

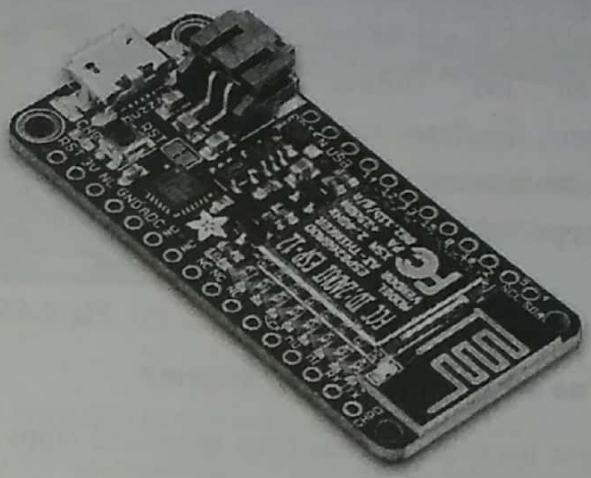


Fig. 6.6.5 : Adafruit

- Adafruit is a hardware platform and marketplace that has a huge community and can become the best place for the newbies in electronics and embedded computing.
- The platform both provides its own hardware and accessories and sells boards by other vendors like Raspberry Pi and Arduino.
- Adafruit Feather boards and extensions (wings) are extremely flexible extensions can work with any board. To connect devices to the Internet and handle all the data they create, Adafruit offers Adafruit IO cloud service that works both with Adafruit and Arduino hardware.

Why choose Adafruit as an IoT hardware platform?

- Adafruit may not have its own IDE or IoT software platform, but has one of the strongest communities, support and knowledgebase for building an IoT project and connecting physical objects to the Internet. Adafruit's hardware also has a competitive advantage. Feather boards are extremely light and simple, so they will become a great start of a small and uncomplicated IoT device like a soil sensor or a tracking wearable.
- *Read: What's hot on Internet of Things wearable technology market?*

☞ **Espressif**

- Espressif may not be the first in the IoT platform list, but can be the first option for an industrial IoT development. The thing is, one of the most catchy features of Espressif's hardware is longevity and robustness, which is a great perk for IoT devices that need to endure extreme conditions or be placed in remote locations. The most popular board series - ESP8266 and ESP32 have 12 years longevity guarantee, for example.

- Apart from reliable hardware and versatile development kits, Espressif IoT platform offers an IoT software development ecosystem, developer space for support and communication and multiple tools and apps for building an IoT prototype.

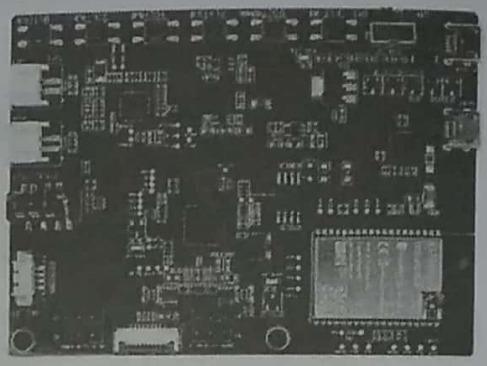


Fig. 6.6.6 Espressif

Why choose Espressif as an IoT hardware platform?

- Espressif offers diverse hardware options from coin-sized chips to full development kits for rapid prototyping and easy setup. Adafruit, for example, uses ESP microcontroller in its Feather development boards.
- As mentioned earlier, ESP boards are designed to withstand extreme conditions and can address the needs of a certain type of IoT projects. In terms of IoT connectivity, platform hardware works with WiFi, Bluetooth and mesh networks.

Chapter Ends...

❑❑❑