**UNIT 1**

**QUE 1 :-What is IOT ?**

**ANS:-** There are different definition given by different people for IOT.

**Definition of IOT**

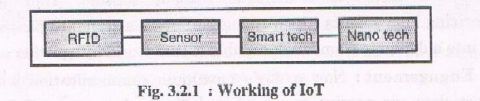
1. The Internet of things (IOT) is the network of physical objects embedded with electronic, software, sensors, and network connectivity that enable these objects to collect and exchange data. OR
2. The internet of things (IOT) is a wireless network between objects or things. OR
3. By embedding short-run mobile handsets into a wide exhibit of extra device and regular things, empowering new type of correspondence amongst individuals and things, and between things themselves. OR
4. The term “internet of things” has come to depict various advances and research teaches that empower the internet of connect into this present reality of physical items. OR
5. “Things having identities and virtual identities working in shrewd spaces utilizing smart interfaces to associate and convey inside social, natural, and client settings ”.

In the IOT objects are sensed and controlled remotely across existing network infrastructure, making open doors for more direct integration between the physical world and computer-based systems, and bringing about enhanced productivity, accuracy and economic benefit.

“Things,” in the IOT to the broad variety of devices as follows:

* Heart monitoring implants
* Biochip transponders on farm animals
* Electric clams in 7coastal waters
* Automobiles with built-in sensors
* DNA analysis devices for environmental/food/pathogen monitoring or
* Field operation devices that assist fire-fighters in search and rescue operations.

These devices assembles useful data with the help of various existing technologies and then autonomously flow the data between other devices.

****

* As shown in figure the RFID identifies and track the data. Sensors are used to collect and process the data to detect the changes in the physical status of things.
* The smart technology is then used to enhance the power of the network by devolving processing capabilities to different part of the network.
* The nano technology is used to make the smaller things to connect and interact.

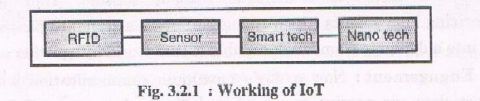
There are few capabilities which helps to bridge the between the virtual and physical world.

* Communication and cooperation
* Embedded information processing
* Localization
* Addressability
* Identification
* Sensing
* Actuation
* User interfaces

**QUE 2:- Explain how IOT works.**

**ANS:- Definition of IOT**

1. The Internet of things (IOT) is the network of physical objects embedded with electronic, software, sensors, and network connectivity that enable these objects to collect and exchange data. OR
2. The internet of things (IOT) is a wireless network between objects or things. OR
3. By embedding short-run mobile handsets into a wide exhibit of extra device and regular things, empowering new type of correspondence amongst individuals and things, and between things themselves. OR
4. The term “internet of things” has come to depict various advances and research teaches that empower the internet of connect into this present reality of physical items. OR
5. “Things having identities and virtual identities working in shrewd spaces utilizing smart interfaces to associate and convey inside social, natural, and client settings ”.

****

* As shown in figure the RFID identifies and track the data. Sensors are used to collect and process the data to detect the changes in the physical status of things.
* The smart technology is then used to enhance the power of the network by devolving processing capabilities to different part of the network.
* The nano technology is used to make the smaller things to connect and interact.

There are few capabilities which helps to bridge the between the virtual and physical world.

* Communication and cooperation
* Embedded information processing
* Localization
* Addressability
* Identification
* Sensing
* Actuation
* User interfaces

**QUE 3:- Explain features of IOT.**

**ANS:-** **Definition of IOT**

1. The Internet of things (IOT) is the network of physical objects embedded with electronic, software, sensors, and network connectivity that enable these objects to collect and exchange data. OR
2. The internet of things (IOT) is a wireless network between objects or things. OR
3. By embedding short-run mobile handsets into a wide exhibit of extra device and regular things, empowering new type of correspondence amongst individuals and things, and between things themselves. OR
4. The term “internet of things” has come to depict various advances and research teaches that empower the internet of connect into this present reality of physical items. OR
5. “Things having identities and virtual identities working in shrewd spaces utilizing smart interfaces to associate and convey inside social, natural, and client settings ”.

In the IOT objects are sensed and controlled remotely across existing network infrastructure, making open doors for more direct integration between the physical world and computer-based systems, and bringing about enhanced productivity, accuracy and economic benefit.

“Things,” in the IOT to the broad variety of devices as follows:

* Heart monitoring implants
* Biochip transponders on farm animals
* Electric clams in 7coastal waters
* Automobiles with built-in sensors
* DNA analysis devices for environmental/food/pathogen monitoring or
* Field operation devices that assist fire-fighters in search and rescue operations.

following are the features of IOT:

1. **Artificial intelligence:** IOT makes anything smart virtually; it is done with the help of data collection and artificial intelligence algorithms and networks.

For example: detecting the level of milk in the refrigerator and when it will become low then place an order to the milk dairy.

1. **Connectivity:** as per the advance in new technology you can now connect the smaller devices to the network.
2. **Sensors:** IOT loses its refinement without sensors. They go about as characterizing instruments which change IOT from a standard passive network of devices into a dynamic framework capable of real-world integration.
3. **Active Engagement:** now a day’s maximum communication with connected technology done via passive engagement. IOT introduces a new model for active content, product, or service engagement.
4. **Small Devices :** small devices have become cheaper and more powerful over time. IOT abuses reason fabricated little devices to convey it’s accuracy, adaptability, and flexibility.

QUE 4:- Explain application of IOT.

ANS:-following are the application of IOT:-

1. Wearables

Wearable technology is the hallmark of IoT applications and one of the earliest industries to deploy IoT. We have fit bits, heart rate monitors and smartwatches these days.

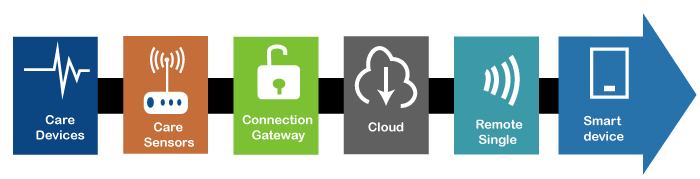
Guardian glucose monitoring device has been developed to help people with diabetes. It detects glucose levels in our body, uses a small electrode called the glucose sensor under the skin, and relates it to a radiofrequency monitoring device.

2. Smart Home Applications

The smart home is probably the first thing when we talk about the IoT application. The example we see the AI home automation is employed by **Mark Zuckerberg. Alan Pan's** home automation system, where a string of musical notes uses in-house functions.

3. Health care

IoT applications can transform reactive medical-based systems into active wellness-based systems. Resources that are used in current medical research lack important real-world information. It uses controlled environments, leftover data, and volunteers for clinical trials. The **Internet of Things** improves the device's **power, precision** and **availability**. IoT focuses on building systems rather than just tools. Here's how the IoT-enabled care device works.



4. Smart Cities

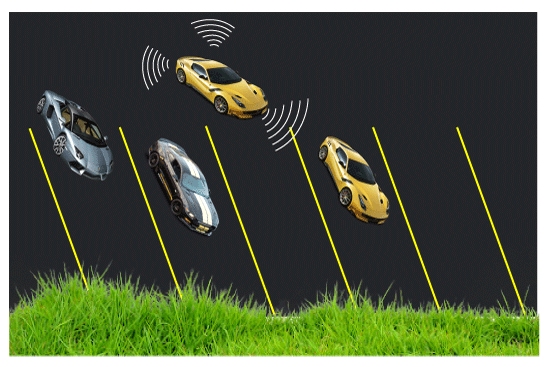
Most of you have heard about the term smart city. Smart city uses technology to provide services. The smart city includes improving transportation and social services, promoting stability and giving voice to their citizens.

The problems faced by Mumbai are very different from Delhi. Even global issues, such as clean drinking water, declining air quality, and increasing urban density, occur in varying intensity cities. Therefore, they affect every city.

Governments and engineers use the Internet of Things to analyze the complex factors of town and each city. IoT applications help in the area of water management, waste control and emergencies.

**Example of a smart city - Palo Alto.**

Palo Alto, San Francisco, is the first city to acquire the traffic approach. He realized that most cars roam around the same block on the streets in search of parking spots. It is the primary cause of traffic congestion in the city. Thus, the sensors were installed at all parking areas in the city. These sensors pass occupancy status to the cloud of each spot.



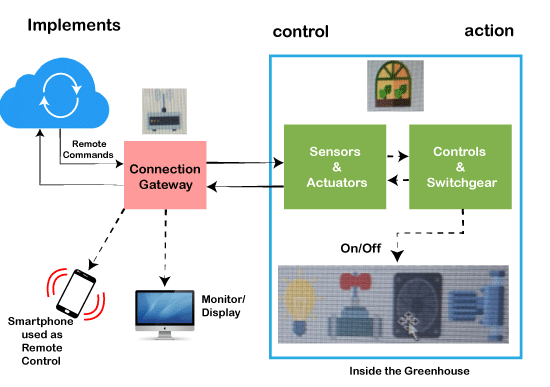
This solution involves the use of sensor *arrays* that collects data and uses it for many purposes.

5. Agriculture

By the year **2050**, the world's growing population is estimated to have reached about 10 billion. To feed such a large population, agriculture needs to marry technology and get the best results. There are many possibilities in this area. One of them is Smart Greenhouse.

Farming techniques grow crops by **environmental parameters**. However, manual handling results in production losses, energy losses and labor costs, making it less effective.

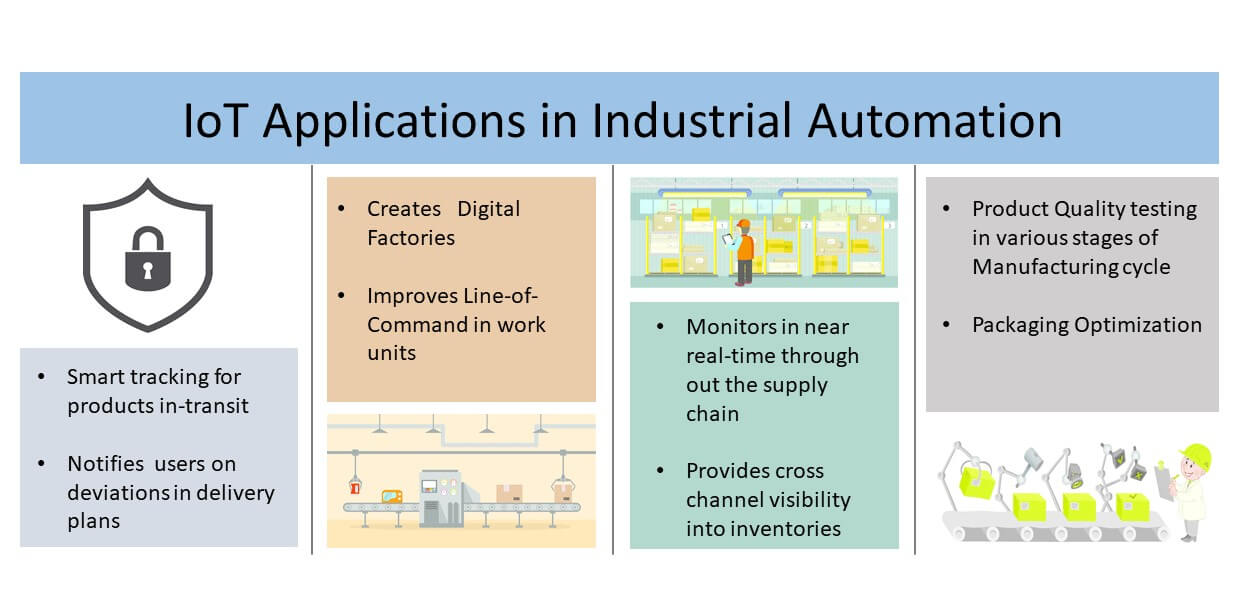
The greenhouse makes it easy to monitor and enables to control the climate inside it.



6. Industrial Automation

It is one of the areas where the quality of products is an essential factor for a more significant investment return. Anyone can **re-engineer** products and their packaging to provide superior performance in **cost** and **customer experience** with IoT applications. IoT will prove as a game-changer. In industrial automation, IoT is used in the following areas:

* **Product flow monitoring**
* **Factory digitization**
* **Inventory management**
* **Safety and security**
* **Logistics and Supply Chain Optimization**
* **Quality control**
* **Packaging customization**



7. Hacked Car

A connected car is a technology-driven car with Internet access and a WAN network. The technology offers the user some benefits such as in-car infotainment, advanced navigation and fuel efficiency.

8. Healthcare

Healthcare do real-time monitoring with the help of smart devices. It gathers and transfers health data such as blood pressure, blood sugar levels, weight, oxygen, and ECG. The patient can contact the doctor by the smart mobile application in case of any emergency.

9. Smart Retail

IoT applications in retail give shoppers a new experience. Customers do not have to stand in long queues as the checkout system can read the tags of the products and deduct the total amount from the customer's payment app with IoT applications' help.

10. Smart Supply Chain

Customers automate the delivery and shipping with a smart supply chain. It also provides details of real-time conditions and supply networks.

11. Smart Farming

Farmers can minimize waste and increase productivity. The system allows the monitoring of fields with the help of sensors. Farmers can monitor the status of the area.

Internet-connected devices go from 5 million to billions in just one year. Business Insider Intelligence estimates 24 billion IoT devices will install and generate more than 300 billion in revenue in the future.

**QUE 5:-** write advantages and disadvantages of IOT.

**ANS:-** advantages of IOT:-

internet of things facilitates several advantages in our daily lives. Some of its advantages are given below:

1. **Minimize human effort:** As IoT devices interact and communicate with each other, they can automate the tasks helping to improve the quality of a business’s services and reducing the need for human intervention.
2. **Save time:** By reducing the human effort, it saves a lot of our time. Saving time is one of the primary advantages of using the IoT platform.
3. **Enhanced data collection:**Information is easily accessible, even if we are far away from our actual location, and it is updated frequently in real-time. Hence these devices can access information from anywhere at any time on any device.
4. **Improved security:** If we have an interconnected system, it can assist in the smarter control of homes and cities through mobile phones. It enhances security and offers personal protection.
5. **Efficient resource utilization:**We can increase resource utilization and monitor natural resources by knowing the functionality and how each device works.
6. **Reduced use of other electronic equipment:** Electric devices are directly connected and can communicate with a controller computer, such as a mobile phone, resulting in efficient electricity use. Hence, there will be no unnecessary use of electrical equipment.
   1. **Use in traffic systems:** Asset tracking, delivery, surveillance, traffic or transportation tracking, inventory control, individual order tracking, and customer management can be more cost-effective with the right tracking system using IoT technology.
   2. **Use in traffic systems:** Asset tracking, delivery, surveillance, traffic or transportation tracking, inventory control, individual order tracking, and customer management can be more cost-effective with the right tracking system using IoT technology. **Useful for safety concerns:**It is helpful for safety because it senses any potential danger and warns users. For example, GM OnStar is an integrated device that identifies a car crash or accident on the road. It immediately makes a call if an accident or crash is found.
   3. **Useful in the healthcare industry:**Patient care can be performed more effectively in real-time without needing a doctor’s visit. It gives them the ability to make choices as well as provide evidence-based care.

**disadvantages of IOT:-**

as the Internet of things facilitates advantages, it also creates a significant set of drawbacks. Some of the IoT disadvantages are given below:

1. **Security issues:**IoT systems are interconnected and communicate over networks. So, the system offers little control despite any security measures, and it can lead to various kinds of network attacks.
2. **Privacy concern:** The IoT system provides critical personal data in full detail without the user’s active participation.
3. **Increased unemployment:**Unskilled workers or even the skilled ones are at a high risk of losing their jobs, leading to high unemployment rates. Smart surveillance cameras, robots, smart ironing systems, smart washing machines, and other facilities are replacing the humans who would earlier do these works.
4. **The complexity of the system:** The designing, developing, maintaining, and enabling the extensive technology to IoT system is quite complicated.
5. **High chances of the entire system getting corrupted:** If there is a bug in the system, it is possible that every connected device will become corrupted.
6. **Lack of international standardizations:** As there is no international standard of compatibility for IoT, it is problematic for devices from different manufacturers to communicate with each other.
7. **High dependency on the internet:** They rely heavily on the internet and cannot function effectively without it.
8. **Reduced mental and physical activity:**Overuse of the internet and technology makes people ignorant because they rely on smart devices instead of doing physical work, causing them to become lethargic and inactive.

**QUE 6:-** explain real time examples of IOT .

### ANS:- following are some real time examples of IOT:-

### Smart thermostats:

Imagine that you can control the temperature of your home from anywhere, with just a simple touch on your smart phone or tablet, and you get the desired temperature before getting home so that you don’t need to wait. [Nest Learning Thermostat](https://nest.com/thermostat/meet-nest-thermostat/) is the most popular Thermostat in this ‘Smart’ category, this company has been bought by **Google**. Nest thermostat not only controlled from anywhere but also it learns by itself by following your daily routing and change the temperature of your home without bothering you, Like if you have set low temperature at night continuously for 7 days, then this device learns that and automatically lowers the temperature at night. This is very helpful device for saving the energy.

1. **Apple Watch and HomeKit:**

And the most talked company of gadgets and devices. Apple has changed the world with its inventive and ultra-modern devices. Be it phones, laptops or any other electronic device, Apple has itself strongly established. The **Apple watch** is the example of how advanced the technology is at Apple. Apart from time and date, the Apple watch enables you to keep a track record of your health and daily activities. Also the voice activation allows you to get notifications in instant. View maps, listen to music and take care of your calls just by a single watch. Surprised at what a watch can do? Well, it’s has lot more features for you to explore and make life easier.

Apart from Apple watch, Apple has also released **Apple HomeKit Framework**, which enables Siri (voice assistant in Apple’s iOS) to communicate with the devices and accessories at your home, so that they can be controlled remotely.

1. **Smart Refrigerator:**

Have you ever experienced a situation when you have some friends at home and you opened the fridge for some cold drinks and there were no cold drinks in the refrigerator! In that situation you must have wished that, someone would have informed you about the cold drinks and you had bought them before. But don’t worry, now this is possible with IoT, **Smart refrigerators** are there, which not only inform you about the consumed items or empty bottles in the fridge but also order them online before they runs out. These refrigerators can do much more than this although the production has not started at big scale yet.

1. **Smart Phones:**

Everybody knows about the smart phones now, and **Smart Phones** are the most common example of IoT or we can say Smart Phone is one of the first few “Things” in the ‘Internet of Things’. All the devices explained above can be controlled using your smart phone and smart phone is become the center of this network like the stick of the magician. Like a magician do the magic by moving his stick, Smart Phone can do the “Real magic” by just few touches.

1. **Smart cars:**

The automotive companies like Ford, Tesla has already stepped into the world where Car would also the part of IoT. **Tesla car** is really a big achievement in this field. Imagine that a car automatically opens the garage door before you arrive at home and you can remotely control the temperature, lights, charging of the car. Tesla car have all these feature, it also have a App framework where you can build your own app to control the car and know its speed, location, battery status from anywhere. The car can upgrade itself automatically by downloading and installing the latest firmware and software. It has 18 sensors to automate the things, and it can fix a service schedule at the car service station by itself.

1. **Microchips:**

We are hearing about microchips for a long time and have their applications in some of the sensitive and dangerous fields like defense. But now one of the most integrated circuit have found its way to our day-to-day life. Microchips are generally used in the forms of tracer as the radar detectors can detect data about various things. Now with ioT, you can fit a microchip on collars of pet or attach it to them to keep a track of their movement without being physically looking for them. There is more freedom to your pets now and this also enables you to keep a record of their health too.

1. Google Glass:

We are talking about innovation and how can we forget to mention the company that defines innovation and internet the best. Google has always come up with things that have made our life easy always and with **Google glass** it is more like repeating history for the company. A headset designed with optical-head display, if only you knew eyeglasses could be this much efficient. You can now wear it and together with voice activation you can interact, see, surf the net, click pictures and do many others things in a Smartphone-like-hands-free form. This Google glass is the result of ‘Project Glass’ from Google.

The internet of Things has many other innovative devices to introduce to the world which will simply leave you amazed and thrilled. We are talking about technology that a decade from now will be marvelous amazement of science playing a yet another important role in our lives.

**QUE 7:-** Explain architecture of IOT.

## **ANS:- Architecture of IoT**

There are different phases in the architecture of IoT but they can vary according to the situations but generally, there are these four phases in the architecture of IoT −

### Networked Devices

These are the physical devices which include sensors, actuators, and transducers. These are the actual devices that collect and send the data for processing. They are capable of receiving real-time data and they can convert the physical quantities into electrical signals which can be sent through a network.

### Data Aggregation

It is a very important stage as it includes converting the raw data collected by sensors into meaningful data which can be used to take actions. It also includes Data Acquisition Systems and Internet Gateways. It converts the Analog signals provided by sensors into digital signals.

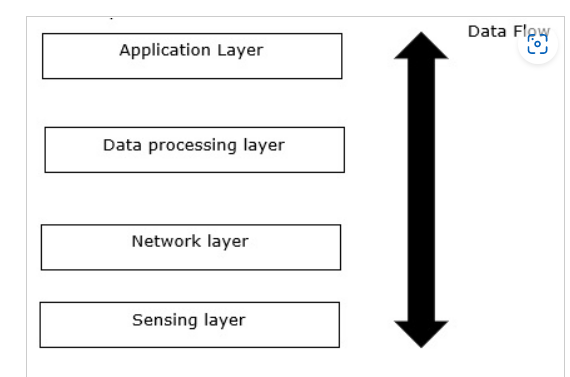
### Final Analysis

This is a stage that includes edge IT analytics and the processing of data to make it more efficient and fully capable of execution. It also includes managing and locating all the devices correctly

### Cloud Analysis

The final data is received here and analysed closely and precisely in data centres. They process and clean the data to make it free from any kind of errors and missing values. After this stage, data is ready to be sent back and executed to perform operations.

**Now let us see the basic fundamental architecture of IoT which consists of four stages as shown in the diagram given below**−



* **Sensing Layer**− The first stage of IoT includes sensors, devices, actuators etc. which collect data from the physical environment, processes it and then sends it over the network.
* **Network Layer**− The second stage of the IoT consists of Network Gateways and Data Acquisition Systems. DAS converts the analogue data (collected from Sensors) into Digital Data. It also performs malware detection and data management.
* **Data Processing Layer**− The third stage of IoT is the most important stage. Here, data is pre-processed on its variety and separated accordingly. After this, it is sent to Data Centres. Here Edge IT comes into use.
* **Application Layer**− The fourth stage of IoT consists of Cloud/Data Centres where data is managed and used by applications like agriculture, defence, health care etc.

**QUE 8:-**Explain History of IoT.

**ANS:-** **Definition of IOT**

1. The Internet of things (IOT) is the network of physical objects embedded with electronic, software, sensors, and network connectivity that enable these objects to collect and exchange data. OR
2. The internet of things (IOT) is a wireless network between objects or things. OR
3. By embedding short-run mobile handsets into a wide exhibit of extra device and regular things, empowering new type of correspondence amongst individuals and things, and between things themselves. OR
4. The term “internet of things” has come to depict various advances and research teaches that empower the internet of connect into this present reality of physical items. OR
5. “Things having identities and virtual identities working in shrewd spaces utilizing smart interfaces to associate and convey inside social, natural, and client settings ”.

In the IOT objects are sensed and controlled remotely across existing network infrastructure, making open doors for more direct integration between the physical world and computer-based systems, and bringing about enhanced productivity, accuracy and economic benefit.

“Things,” in the IOT to the broad variety of devices as follows:

* Heart monitoring implants
* Biochip transponders on farm animals
* Electric clams in 7coastal waters
* Automobiles with built-in sensors
* DNA analysis devices for environmental/food/pathogen monitoring or
* Field operation devices that assist fire-fighters in search and rescue operations.

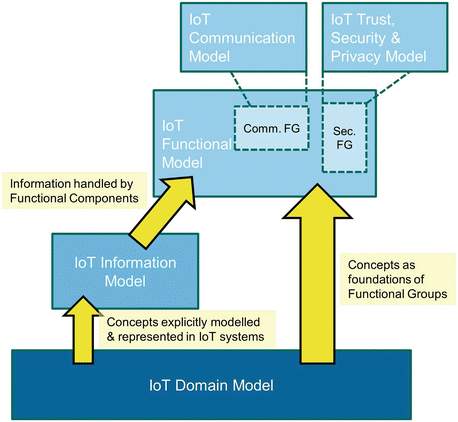
## History of IoT

* 1970- The actual idea of connected devices was proposed
* 1990- John Romkey created a toaster which could be turned on/off over the Internet
* 1995- Siemens introduced the first cellular module built for M2M
* 1999- The term “Internet of Things” was used by Kevin Ashton during his work at P&G which became widely accepted
* 2004 – The term was mentioned in famous publications like the Guardian, Boston Globe, and Scientific American
* 2005-UN’s International Telecommunications Union (ITU) published its first report on this topic.
* 2008- The Internet of Things was born
* 2011- Gartner, the market research company, include “The Internet of Things” technology in their research

**QUE 9:-**Explain reference model of IoT.

**ANS:-** The first major contribution of the *IoT Architectural Reference Model* (IoT ARM) is the IoT Reference Model itself. Besides models, the IoT Reference Model provides the concepts and definitions on which IoT architectures can be built. The Reference Model consists of several sub-models that set the scope for the IoT design space and that address architectural views. The IoT Reference Model aims at establishing a common grounding and a common language for IoT architectures and IoT systems. It consists of the sub-models shown in Fig. [7.1](https://link.springer.com/chapter/10.1007/978-3-642-40403-0_7#Fig1), which we explain below. The yellow arrows show how concepts and aspects of one model are used as the basis for another.

**Fig. 7.1**

[](https://link.springer.com/chapter/10.1007/978-3-642-40403-0_7/figures/1)

Interaction of all sub-models in the IoT Reference Model. The sub-models are explained in the text body

The foundation of the IoT Reference Model is the IoT Domain Model, which introduces the main concepts of the Internet of Things like Devices, IoT Services and *Virtual Entities* (VE), and it also introduces relations between these concepts. The abstraction level of the IoT Domain Model has been chosen in such a way that its concepts are independent of specific technologies and use-cases. The idea is that these concepts are not expected to change much over the next decades or longer.

**QUE 10:-**Explain use of Internet in IoT

**ANS:-** use of internet in IOT:-

Connectivity

The IoT devices will most definitely need connectivity to the controllers that will be controlling the devices. The connectivity to the network could be wired or wireless. There are several protocol options in this space like zigbee, bluetooth, z-wave, 6LowPAN, WiFi, Cellular, NFC, Sigfix etc. The network will need to evolve to support these protocols that are common in the IoT world.

Power

Power over Ethernet is one of the significant innovations in the last decade that has powered devices like phones and access points, enabling innovations like VoIP. More recently, PoE is being leveraged to power lights in the enterprise. This has several advantages:  
• It reduces the installation costs in the enterprise significantly, because deployment of traditional electrical conduits is expensive.  
• It is safer compared to traditional electrical infrastructure.  
• It is more efficient – Network powered lighting is expected to increase the power efficiency by 38%.  
• Converging the building and IT infrastructure will also help reduce the customers’ operational expenses.  
• With UPoE, even laptops can be charged through the network, eliminating the electrical conduit at the cubicles.  
Moving forward, more devices in the enterprise like HVACs and badge readers will start leveraging PoE.

Security

Securing the IoT infrastructure is critical given the verticals it will be deployed in. The recent attack on the Dyn DNS servers, which brought down Netflix, Amazon and Twitter among others, originated from cameras that were infected with the Mirai botnet. The network will need to evolve to be able to secure these devices – it needs to protect the devices from being infected by malware, but will also need to protect the network and application servers from attacks originating from the infected IoT devices. The devices connecting to the network would have to be authenticated, which is something that the network would play a major role in.

In some verticals, IoT devices will require a secure connectivity to the application running in the server. As an example, a video camera can originate traffic that needs to be securely transported to the control room. This would require a secure tunnel to be created from the camera to the server.

Compute

The network has compute than can be leveraged in the IoT deployments to process events that cannot afford latency in processing. The IoT devices themselves are highly cost optimised, which will limit the compute available in those devices. The network, as a result, would have to support an application hosting environment, that would allow the IoT vendors to host their software locally. Extending on the example given above in the context of video surveillance, the compute on the network elements could be leveraged to run image processing software that can help detect events. Local detection of events will help in scenarios where the priority that the network provides for this traffic has to be dynamically increased.

Policy

IoT devices, in many cases, would require specific SLAs from the network – such as latency and reliability. Based on the type of the device and the requirements for the traffic generated, the network can provision the required end-to-end policies that would help realise these requirements. The controller will, in this case, help in the provisioning of the required configurations on the devices in the traffic path.

Manageability

Managing the IoT devices at scale is a major challenge in the enterprise. While every IoT vendor would most often have their own controller to manage their IoT devices, the network can help host this software stack in the compute that is part of the networking infrastructure. It will help deliver the critical messages from the controller to the devices with high reliability. It will also help automate the provisioning of the network for supporting IoT deployments.

In summary, the network will play a role that is front and centre in the IoT revolution – it’ll help rolling out these high scale deployments in quick time. There has NEVER BEEN A BETTER TIME TO ROLL OUT IoT.

**QUE 11:-**Explain What is System on chip?

**ANS:-** a system on chip(Soc) is an integrated circuit(also known as an ”IC”)that integrates all component of a computer or any other electric systems. On a single substrate it contains digital, analog, mixed-singal, as well as radio-frequency functions.

System on chips consumes low power and therefore they are mostly available. In the area of embedded systems socs are widely used. Socs are not only integrates microprocessor/microcontroller but also integrates many advanced peripherals like coprocessor, GPU (graphics processing unit), wi-fi module, etc. soc does not necessarily contain built- in memory.

There can be three categories of socs:

1. Soc built around a microcontroller
2. Soc built around a microprocessor
3. Soc built for specific application

Basically , a system on chip (soc) is a microchip with all parts of electronic circuits for a particular system such as wearable computer, smartphone on a single chip.

Example of soc for a specific application is like sound detecting device which includes ADC (An analog-to-digital converter), an audio receiver, microprocessor, memory and input/output logic controller which is on single chip. These types of systems are much more powerful.

A typical SoC consists of:

* A microcontroller, microprocessor or DSP core(s). Some SoCs—called *multiprocessor system on chip* (MPSoC)—include more than one processor core.
* Memory blocks including a selection of ROM, RAM, EEPROM and flash memory.
* Timing sources including oscillators and phase-locked loops.
* Peripherals including counter-timers, real-time timers and power-on reset generators.
* External interfaces including industry standards such as USB, FireWire, Ethernet, USART, SPI.
* Analog interfaces including ADCs and DACs.
* Voltage regulators and power management circuits.

These blocks are connected by either a proprietary or industry-standard bus such as the AMBA bus from ARM Holdings. DMA controllers route data directly between external interfaces and memory, bypassing the processor core and thereby increasing the data throughput of the SoC.

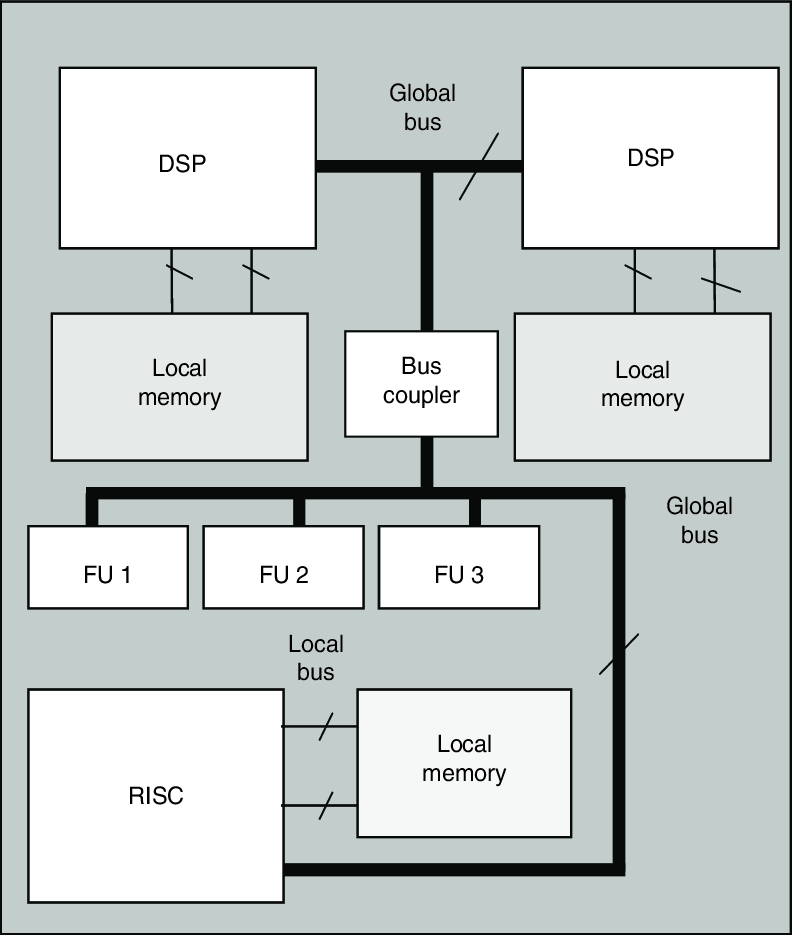
**QUE 12 :-**Explain Structure of System on Chip.

**ANS:-** A typical SoC consists of:

* A microcontroller, microprocessor or DSP core(s). Some SoCs—called *multiprocessor system on chip* (MPSoC)—include more than one processor core.
* Memory blocks including a selection of ROM, RAM, EEPROM and flash memory.
* Timing sources including oscillators and phase-locked loops.
* Peripherals including counter-timers, real-time timers and power-on reset generators.
* External interfaces including industry standards such as USB, FireWire, Ethernet, USART, SPI.
* Analog interfaces including ADCs and DACs.
* Voltage regulators and power management circuits.

These blocks are connected by either a proprietary or industry-standard bus such as the AMBA bus from ARM Holdings. DMA controllers route data directly between external interfaces and memory, bypassing the processor core and thereby increasing the data throughput of the SoC.

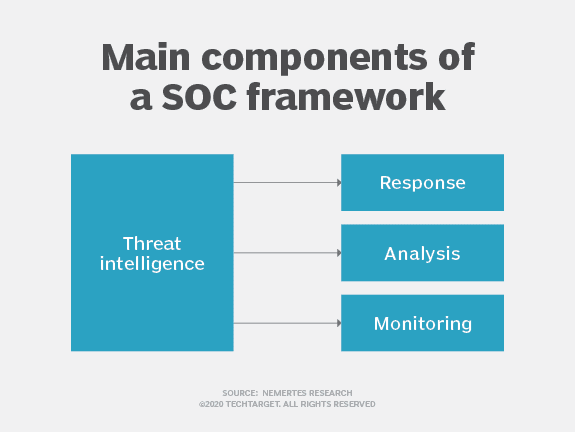
A **system on a chip** or **system on chip** (**SoC** or **SOC**) is an integrated circuit (**IC**) that integrates all components of a computer or other electronic system into a single chip. It may contain digital, analog, mixed-signal, and often radio-frequency functions—all on a single chip substrate. A typical application is in the area of embedded systems.



**QUE 13:-** Explain SoC Elements

**ANS:-** As a business owner, you need to protect your business where you need to manage the threat lifecycle. In this case, the SOC framework can apply few things to help you to establish and provide you a mature approach. Here you can see the SOC elements which will help you to grow your business.

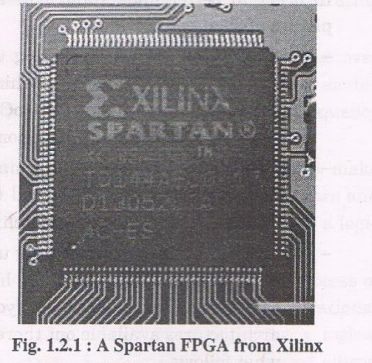
* **Identify:** As a businessman, you need to earn the trust of your people and need to have a complete understanding between you both. You also need to identify the risk and vulnerabilities, digital and physical assets, defense systems, and much more.
* **Protect:** You need to establish a diverse and layered approach to defend the business while they will be ready to reply to any attack.
* **Detect:** You need to implement the technology and do the practice to quickly detect the security data.
* **Respond:** You can react calmly to any incident, and you need to be in a severe breach.
* **Recover:** This is when you need to return the organisation to its original state by doing proper planning. It also does preventative measures to safeguard your business against a repeat attack.



**QUE 14:-**Explain FPGA.

**ANS:-** FPGA means the field programmable gate array. It is an integrated circuit which is configured the end customer or a designer after process of manufacturing and therefore the name is field-programmable. Using a hardware description language (HDL)FPGA configuration is generally specified. It is as similar as that used for an application specific integrated circuit(ASIC).

The following fig. is a example of FPGSA chip.



FPGAs contain an array of programmable logic blocks. They also contain a hierarchy of reconfigurable blocks that interconnects together, like many logic gates that can be inter-wired in different type of configurations. These logic blocks are configured to perform complex combinational functions, or simple logic gates like OR, AND,NOT,NAND and NOR. In most FPGAs, logic blocks also include memory elements, which are similar to flip flips.

Contemporary field-programmable gate arrays(FPGAs)have large resources of logic gates and RAM blocks to implement complex digital computations.

As FPGA designs employ very fast I/O and bidirectional data buses, it becomes a challenge to verify correct timing of valid data within setup time and hold time.

Floor planning enables resources allocation within FPGAs to meet these time constraints FPGAs can be used to implement any logical function that an ASIC could perform .

The ability to update the functionality after shipping, partial re-configuration of a portion of the design and the low non-recurring engineering costs relative to an ASIC design(notwithstanding the generally higher unit cost), offer advantages for many applications.

**QUE 15:-**Explain GPU

**ANS:-** GPU stands for the Graphics Processing Unit. A different name of graphics processing unit (GPU) is visual processing unit(VPU) . it is designed to manipulate and after memory of images in a frame buffer rapidly.

GPUs are generally being used In mobile phones, embedded system, personal computers and games. For image processing purpose, GPU can be very much useful for manipulating.

These types of algorithms for processing of large blocks of data are worked in parallel. In today’s home computers, a GPU is present on a video card, or it can be embedded on the motherboard.

GPUs are generally being used in mobile phones, embedded system, personal computers and games.

These type of algorithms for processing of large blocks of data are worked in parallel.

In today’s home computer, a GPU is present on a video card, or it can be embedded on the motherboard.

There are basically two forms of graphics processing unit (GPU):-

1. Dedicated graphics card- it is also called as discrete.
2. Integrated graphics – it is also called as shared graphics solutions, integrated graphics processors(IGP),or unified memory architecture(UMA).

Dedicated graphics card:-

A dedicated or discrete, GPU is an independent source of video memory apart from RAM in a system. Dedicated cards are perfect for purely gaming or totally graphic designer.

However there are a few drawbacks to having a dedicated card. These video cards will heat up quickly. These card are also power hungry, therefore a laptop with dedicated graphics card will tend to decrease the battery life.

Integrated graphics

Instead of using separate memory, an integrated graphics processing unit(GPU) uses it’s system’s memory. So, if the system has 4GB of RAM, the video card may use between one and five precent of the available memory for graphics processing. Of course, this percentage varies depending on the size of task specially multitask (gaming purpose).

**QUE 16:-** Explain APU

**ANS:-** An accelerated processing unit (APU) is a microprocessor that combines the central processing unit (CPU) with the graphics processing unit (GPU) on a single computer chip. It makes a computer a bit faster than if the processors were set far apart from each other because, in that case, it would take more time for them to communicate.

You can compare an APU to a pencil with an eraser at the other end. There’s no need to drop the pencil and grab an eraser, erase the mistake, and then exchange the eraser back. Instead, you can easily and quickly make corrections to your work with a single tool. The APU works like that for today’s powerful gaming computers.

APU stands for accelerated processing unit. The Central Processing Unit (CPU) is the brain of the computer, handling most of the processing. However, one area where it doesn't excel is graphics.

To compensate for this, Graphics Processing Units (GPU) deal exclusively with visual output tasks. However, designing and manufacturing two units to handle this data is inefficient. The Accelerated Processing Unit is designed to combine the two separate units onto a single die. In this case, a die is a small segment of semiconducting material, containing a copy of a mass-produced circuit.

Although placing two circuits onto a single die doesn't sound that forward-thinking, it is the manufacturing and design decisions that dictate the performance of your computer.

Reducing the footprint of the processing units brings down the cost, allows more room for other hardware, and is more efficient. Keeping the components close together increases the data transfer rates and reduces power consumption, too.

If you haven't heard of APU technology before, there may be a reason; the term is almost exclusively used by a single manufacturer, AMD.

When considering upgrading your CPU or GPU, things can quickly become overwhelming. There are many products out there, with similar numerical names, and tall marketing claims. Each new release is touted as a vast improvement over the last, even if this isn't strictly borne out in benchmarking tests.

Of course, it's natural that a company should want to sell their product, so you'd be right to be skeptical of APUs, too. However, there are some real benefits to using the technology. The most immediate transformation is in system performance.

If your computer previously used just a single CPU and integrated graphics, then you'll see a noticeable bump in performance. Tasks will be quicker, videos will run smoother, and speeds will generally increase. In the long-term, you'll also see a reduction in power usage.

**QUE 17:-**Explain Compute Units

**ANS:-** A compute unit is a stream multiprocessor in a Nvidia who is a GPU vendor or a SIMD(single instruction, multiple data)engine in an AMD GPU.

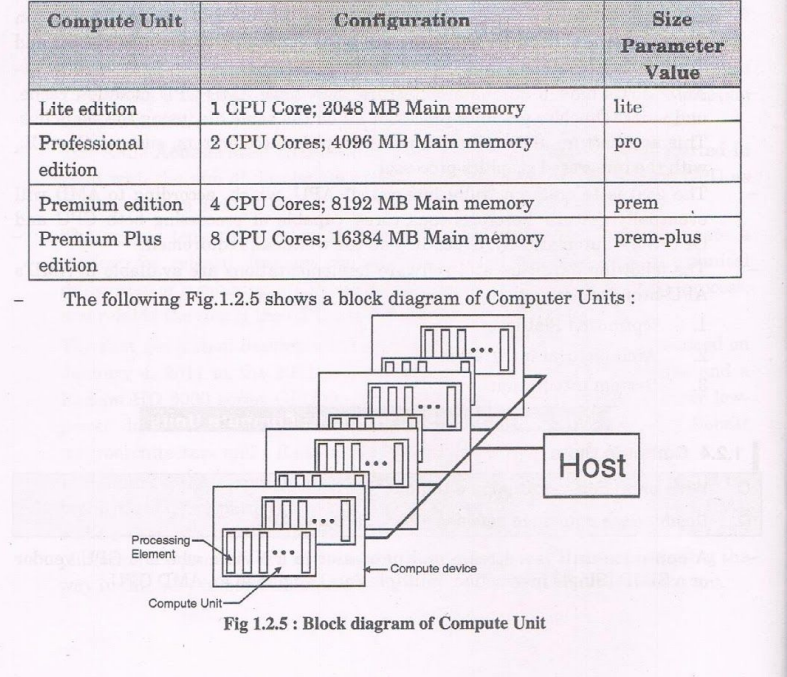
Each compute unit has several processing element like arithmetic logic unit/ stream processor. For example, a compute unit of a HD 5000 series GPU has 80o processing elements (16 processing cores with 5 ALUs per processing core).

A compute unit is the smallest organization of register and instructions capable of working at once.

A stream processor is a programming paradigm where only a single instruction is applied to all the record in a stream of data. An example of such records would be the pixels of an image.

A compute unit is the virtualized hardware resources used by an SAP cloud platform application. After being deployed to the cloud, the application is hosted on a compute unit with certain central processing unit(CPU), main memory disk space, and an installed OS, compute unit sizes.

SAP cloud platform offers four standard sizes of compute units according to the providing resources.

Depending on their needs, customers can choose from the following compute unit configurations:

**QUE 18:-** Explain Introduction to Raspberry Pi.

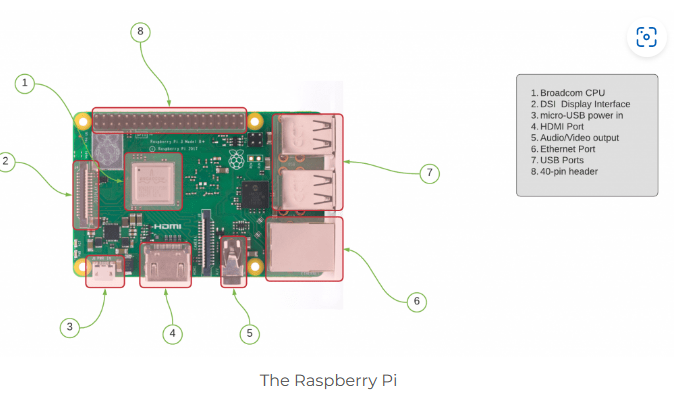
**ANS:-** The [Raspberry Pi](https://www.amazon.com/Raspberry-Pi-Computer-Suitable-Workstation/dp/B0899VXM8F?keywords=Raspberry+Pi+4+Model+B&qid=1636845883&sr=8-4&linkCode=ll1&tag=circbasi-20&linkId=fa08c0dbd273d4ca54acbe204154e563&language=en_US&ref_=as_li_ss_tl) is probably the most popular electronics prototyping platform ever. Its creators, the Raspberry Pi Foundation, wanted to create a single-board computer that could be used to teach computer science and programming to high school students in developing countries.

The Raspberry Pi was first released to the public in February of 2012. Soon after, people around the world began to realize how useful the Raspberry Pi could be for a wide variety of DIY electronics projects.

The Raspberry Pi is a credit card sized computer that can connect to a huge variety of sensors and other modules like [LCD displays](https://www.amazon.com/HiLetgo-Display-Backlight-Controller-Character/dp/B00HJ6AFW6?dchild=1&keywords=16x2+lcd&qid=1594793937&sr=8-3&linkCode=ll1&tag=circbasi-20&linkId=7ef3bd45b3cb673222665ee02a40623c&language=en_US&ref_=as_li_ss_tl), [servos](https://www.amazon.com/Dorhea-Arduino-Helicopter-Airplane-Walking/dp/B07Q6JGWNV?keywords=arduino+servo&qid=1637085948&sr=8-5&linkCode=ll1&tag=circbasi-20&linkId=b46a3e0827e5374d6f145fe2e3ee0981&language=en_US&ref_=as_li_ss_tl), and [motors](https://www.amazon.com/EUDAX-Electric-Magnetic-Connector-Propeller/dp/B07GDP2FCL?keywords=dc+motor+assortment&qid=1638070693&sr=8-3&linkCode=ll1&tag=circbasi-20&linkId=104ae6a798a93a121e91955ef3c7357b&language=en_US&ref_=as_li_ss_tl).

The Raspberry Pi is a low-cost, low power consumption, credit-card-sized single-board computer. After some initial setup, you can connect it to a computer or TV monitor and start using it.

Aside from a monitor, the Raspberry Pi will also need a [mouse and keyboard](https://www.amazon.com/Verbatim-Slimline-Keyboard-Mouse-Accessibility/dp/B017M4J1BU?keywords=usb+keyboard+and+mouse&qid=1637775468&sr=8-8&linkCode=ll1&tag=circbasi-20&linkId=4a6495558ef20aad94e61478fa6c82c6&language=en_US&ref_=as_li_ss_tl), unless you decide to set it up in [headless mode](https://www.circuitbasics.com/raspberry-pi-basics-setup-without-monitor-keyboard-headless-mode/). In headless mode you only need a computer and a USB cable to use the Raspberry Pi.



The Raspberry Pi has 40 GPIO pins to connect external peripherals or sensors. The abundance of GPIO pins allows the Raspberry Pi to be used as a control center for more complex projects like robots and autonomous vehicles.

Finally, the Raspberry Pi relies on a Broadcom BCM2835 System on a Chip (SoC). An SoC is an integrated circuit that has all the components necessary to power a computer. On the Raspberry Pi, the Broadcom chip contains a 700MHz ARM processor and a video core 4 GPU.

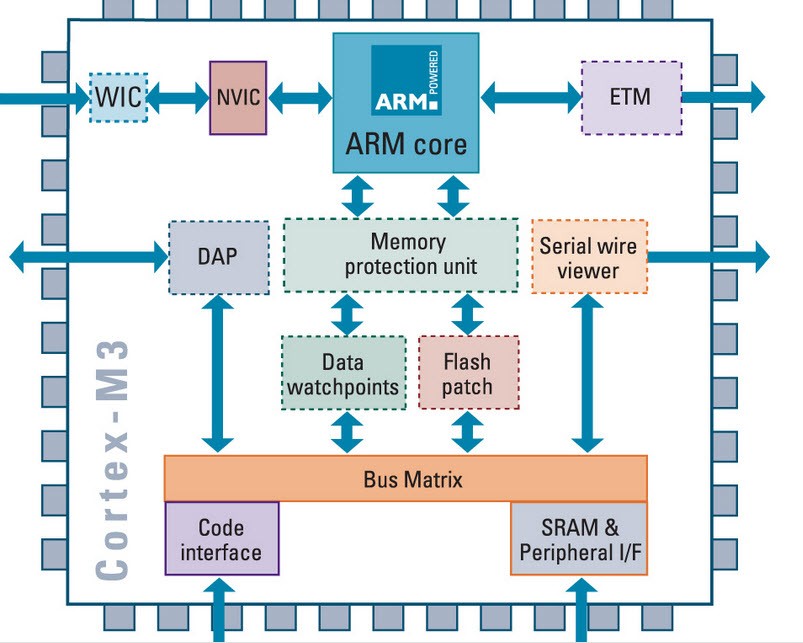
## USES OF RASPBERRY PI

There are so many things you can make with a Raspberry Pi. And due to its extreme popularity, the number of third-party sensors, modules, and code libraries has grown to epic proportions. This has greatly expanded the possible applications for the Raspberry Pi. The applications really are endless, but here are some common ones:

* Web servers
* Local network hubs for IoT
* Sensor control
* Robotics control
* Industrial equipment control
* Automated control systems
* Data processing

**QUE 19:-** Explain Introduction to SoC-ARM Architecture

**ANS:-** The ARM architecture processor is an advanced reduced instruction set computing [RISC] machine and it’s a 32bit reduced instruction set computer (RISC) microcontroller. It was introduced by the Acron computer organization in 1987. This ARM is a family of microcontroller developed by makers like ST Microelectronics,Motorola, and so on. The ARM architecture comes with totally different versions like ARMv1, ARMv2, etc., and, each one has its own advantage and disadvantages.



**ARM Architecture**

The ARM cortex is a complicated microcontroller within the ARM family that has ARMv7 design. There are 3 subfamilies within the ARM cortex family :

* ARM Cortex Ax-series
* ARM-Cortex Rx-series
* ARM-Cortex Mx-series

### The ARM Architecture

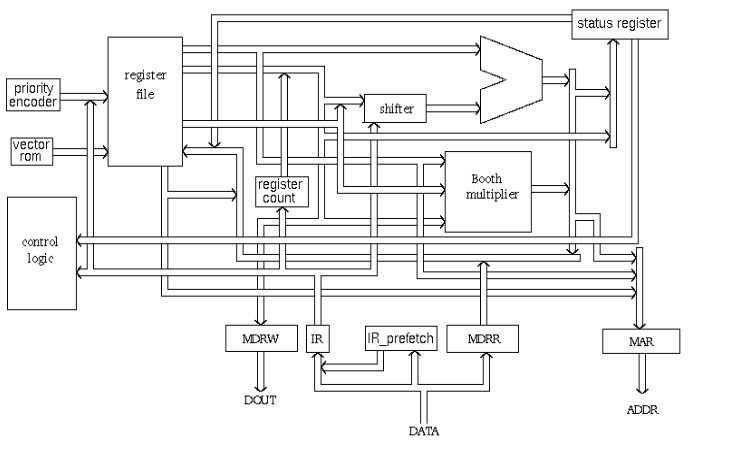
* Arithmetic Logic Unit
* Booth multiplier
* Barrel shifter
* Control unit
* Register file

This article covers the below mentioned components.

The ARM processor conjointly has other components like the Program status register, which contains the processor flags (Z, S, V and C). The modes bits conjointly exist within the program standing register, in addition to  the interrupt and quick interrupt disable bits; Some special  registers:  Some  registers are  used  like  the  instruction, memory data read and write registers and memory address register.

Priority encoder: The encoder  is  used  in  the  multiple  load  and  store instruction to point which register within the register file to be loaded or kept .

Multiplexers: several multiplexers are accustomed to the management operation  of  the processor buses. Because of the restricted project time, we tend to implement these components in a very behavioral model. Each component is described with an entity. Every entity has its own architecture, which can be optimized for certain necessities depending on its application. This creates the design easier to construct and maintain.



**ARM Block Diagram**

#### Arithmetic Logic Unit (ALU)

The ALU has two 32-bits inputs. The primary comes from the register file, whereas the other comes from the shifter. Status registers flags modified by the ALU outputs. The V-bit output goes to the V flag as well as the Count goes to the C flag. Whereas the foremost significant bit really  represents  the S  flag,  the  ALU  output  operation is  done by NORed to  get  the  Z  flag. The ALU has a 4-bit function bus that permits up to 16 opcode to be implemented.

#### Booth Multiplier Factor

The multiplier factor has 3 32-bit inputs and the inputs return from the register file. The multiplier output is barely  32-Least Significant  Bits of the merchandise. The entity representation of the multiplier factor is shown in the above block diagram. The multiplication starts  whenever  the  beginning 04 input goes active. Fin of  the output goes high when finishing.

#### Booth Algorithm

Booth algorithm is a noteworthy multiplication algorithmic rule for 2’s complement numbers. This treats positive and negative numbers uniformly. Moreover, the runs of 0’s or 1’s within the multiplier factor are skipped over without any addition or subtraction being performed, thereby creating possible quicker multiplication.  The figure shows the simulation   results   for   the multiplier test bench. It’s clear that the multiplication finishes only in16 clock cycle.

#### Barrel Shifter

The barrel shifter features a 32-bit input to be shifted.  This input is coming back from the register file or it might be immediate data.  The shifter has different control inputs coming back from the instruction register. The Shift field within the instruction controls the operation of the barrel shifter.  This  field indicates the kind  of  shift  to  be  performed  (logical  left  or  right, arithmetic right or rotate right). The quantity by which the register ought to be shifted is contained in an immediate field within the instruction or it might be the lower 6 bits of a register within the register file.

The shift\_val input bus is 6-bits, permitting up to 32 bit shift. The shifttype indicates the needed shift sort of  00, 01, 10, 11 are corresponding to shift left, shift right, an arithmetic shift right and rotate right, respectively. The barrel shifter is especially created with multiplexers.

#### Control Unit

For any microprocessor, control unit is the heart of the whole process and it is responsible for the system operation,so the control unit design is the most important part within the whole design. The control unit is sometimes a pure combinational circuit design. Here, the control unit is implemented by easy state machine. The processor timing is additionally included within the control unit. Signals from the control unit are connected to each component within the processor to supervise its operation.

**QUE 20:-**Explain characteristics of IoT

**ANS:-** Characteristics of the Internet of Things :  
There are the following characteristics of IoT as follows. Let’s discuss it one by one.

Connectivity –  
Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times. For example, connection between people through internet devices like mobile phones ,and other gadgets, also connection between Internet devices such as routers, gateways, sensors, etc.

Intelligence and Identity –   
The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.

Scalability –   
The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.

Dynamic and Self-Adapting (Complexity) –  
IoT devices should dynamically adapt themselves to the changing contexts and scenarios.  Assume a camera meant for the surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon, night).

Architecture –   
IoT architecture cannot be homogeneous in nature. It should be hybrid, supporting different manufacturers ‘ products to function in the IoT network. IoT is not owned by anyone engineering branch. IoT is a reality when multiple domains come together.

Safety –   
There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet. This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge. IoT networks may also be at the risk. Therefore, equipment safety is also critical.

Self Configuring – This is one of the most important characteristics of IoT. IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.

**QUE 21:-** Explain Raspberry pi.

**ANS:-** The raspberry pi is like a PC and can be plugged into a TV or monitor as it is credit card shaped and it is used along with the general purpose input output(GPIO)pins to control all equipments.

Raspberry pi has capability of playing videos, electronics projects and programming. The raspberry pi is slower then a modern laptop or desktop but is still a complete Linux computer and can provide all the expected ability that implies, at a low-power consumption level.

Raspberry is the desired operating system for the raspberry pi.

In order to download and install the operating system onto our raspberry pi; you will need the following:

1. Download both Raspbian and win32DistImager and save somewhere easily accessible
2. Plug the USB memory card reader into your computer
3. Open win32DistImager
4. Find the location of the image of the file and the memory card
5. Click “write”

Now it is time to turn on our raspberry pi.

When the memory card, HDMI lead, ethernet cable, mouse and keyboard are plugged in, plug in the power lead. As soon as you do this. Your screen should be raspberry pi. Wait until your screen reads ”raspberrypi login :”

Username=pi [ENTER], password= raspberry pi [ENTER]

Prepared to check for updates after your raspberry pi reboots.

Open the terminal again by pressing the terminal icon on the top bar.

And then write “sudo apt-get update” and “ENTER.” The system package list will be updated.

Once that has finished, write “sudo apt-get dist-upgrade” and “ENTER.”

The packages installed will be with never versions.

**QUE 22:-** Explain all hardware which use in Raspberry pi.

**ANS :-** Here are the various hardware on the Raspberry Pi board:

ARM CPU/GPU -- This is a Broadcom BCM2835 System on a Chip (SoC) that's made up of an ARM central processing unit (CPU) and a Videocore 4 graphics processing unit (GPU). The CPU handles all the computations that make a computer work (taking input, doing calculations and producing output), and the GPU handles graphics output.

GPIO -- These are exposed general-purpose input/output connection points that will allow the real hardware hobbyists the opportunity to tinker.

RCA -- An RCA jack allows connection of analog TVs and other similar output devices.

Audio out -- This is a standard 3.55-millimeter jack for connection of audio output devices such as headphones or speakers. There is no audio in.

LEDs -- Light-emitting diodes, for all of your indicator light needs.

USB -- This is a common connection port for peripheral devices of all types (including your mouse and keyboard). Model A has one, and Model B has two. You can use a USB hub to expand the number of ports or plug your mouse into your keyboard if it has its own USB port.

HDMI -- This connector allows you to hook up a high-definition television or other compatible device using an HDMI cable.

Power -- This is a 5v Micro USB power connector into which you can plug your compatible power supply.

SD cardslot -- This is a full-sized SD card slot. An SD card with an operating system (OS) installed is required for booting the device. They are available for purchase from the manufacturers, but you can also download an OS and save it to the card yourself if you have a Linux machine and the wherewithal.

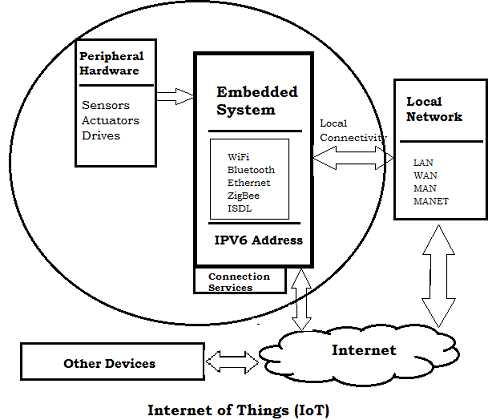
Ethernet -- This connector allows for wired network access and is only available on the Model B.

**QUE 23:-** explain embedded technology used in IoT

**ANS:-** Embedded Devices (System) in (IoT)

It is essential to know about the embedded devices while learning the IoT or building the projects on IoT. The embedded devices are the objects that build the unique computing system. These systems may or may not connect to the Internet.

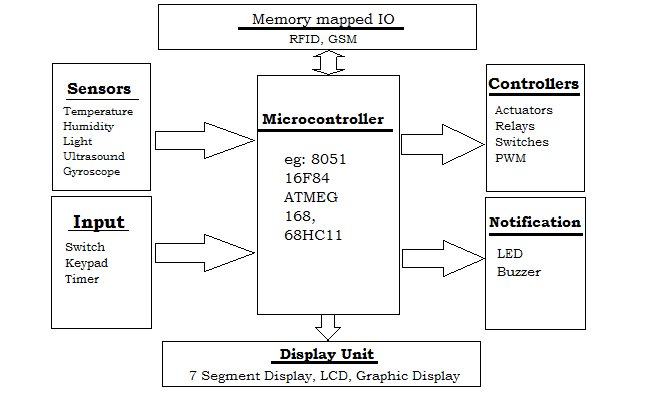
An embedded device system generally runs as a single application. However, these devices can connect through the internet connection, and able communicate through other network devices.



Embedded System Hardware

The embedded system can be of type microcontroller or type microprocessor. Both of these types contain an integrated circuit (IC).

The essential component of the embedded system is a RISC family microcontroller like Motorola 68HC11, PIC 16F84, Atmel 8051 and many more. The most important factor that differentiates these microcontrollers with the microprocessor like 8085 is their internal read and writable memory. The essential embedded device components and system architecture are specified below.



**Fig: Basic Embedded System**

Embedded System Software

The embedded system that uses the devices for the operating system is based on the language platform, mainly where the real-time operation would be performed. Manufacturers build embedded software in electronics, e.g., cars, telephones, modems, appliances, etc. The embedded system software can be as simple as lighting controls running using an 8-bit microcontroller. It can also be complicated software for missiles, process control systems, airplanes etc.

**QUE 24:-** explain physical and logical architecture of IoT.

**ANS :-**

## Physical Design of IoT

A physical design of an IoT system refers to the individual node devices and their protocols that are utilised to create a functional IoT ecosystem.

Each node device can perform tasks such as remote sensing, actuating, monitoring, etc., by relying on physically connected devices. It may also be capable of transmitting information through different types of wireless or wired connections.

The things/devices in the IoT system are used for:

* Building connections
* Data processing
* Providing storage
* Providing interfaces
* Providing graphical interfaces

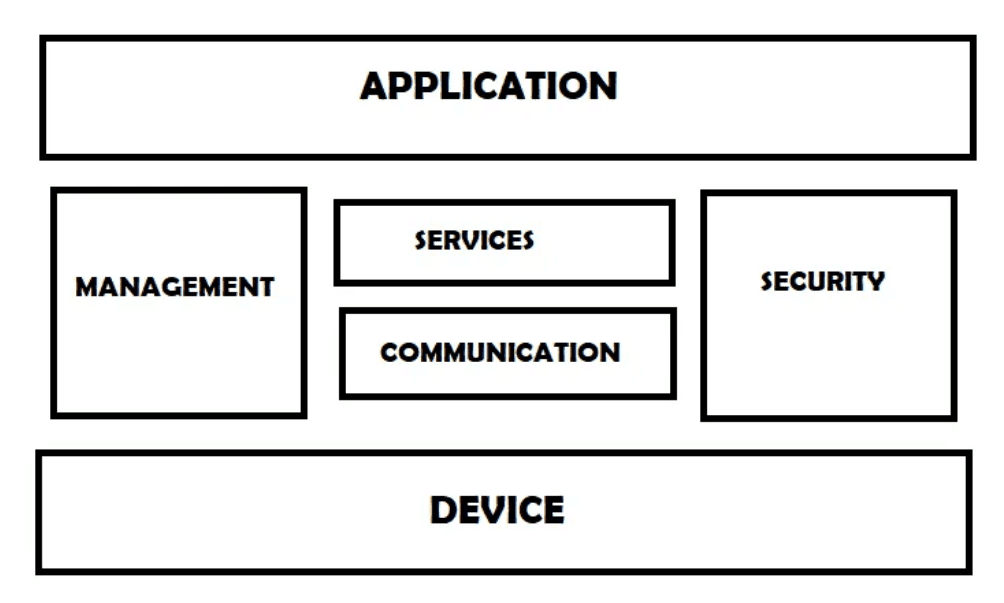
The devices generate data, and the data is used to perform analysis and do operations for improving the system. For instance, a moisture sensor is used to obtain the moisture data from a location, and the system analyses it to give an output.

## Logical Design of IoT

A logical design for an IoT system is the actual design of how its components (computers, sensors, and actuators) should be arranged to complete a particular function. It doesn’t go into the depth of describing how each component will be built with low-level programming specifics.

IoT logical design includes:

### IoT functional blocks:

IoT systems include several functional blocks such as Devices, communication, security, services, and application. The functional blocks provide sensing, identification, actuation, management, and communication capability.These functional blocks consist of devices that handle the communication between the server and the host, enable monitoring control functions, manage the data transfer, secure the IoT system using authentication and different functions, and provide an interface for controlling and monitoring various terms.

### IoT communications models

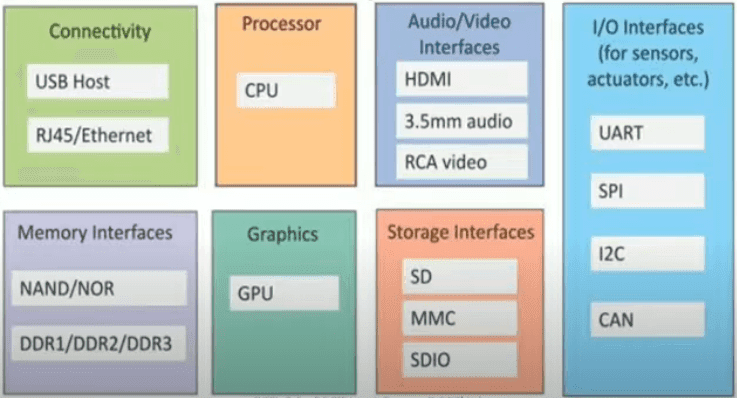
There are multiple kinds of models available in an Internet of Things system that is used for communicating between the system and server, such as:

* + Request-response model
  + Push-pull model
  + Publish-subscribe model
  + Exclusive pair model

### IoT communication APIs

APIs are used to communicate between the server and system in IoT. Some API’s include:

* + REST-based communication APIs
  + Client-server
  + Stateless
  + Cacheable
  + Websocket based communication API



##### Generic Block Diagram of an IoT Device

|  |  |
| --- | --- |
| **Physical Design** | **Logical Design** |
| Physical design is highly detailed. | Logical design is a high-level design and doesn’t provide any detail. |
| Physical design is more graphical than textual; however, it can comprise both. | Logical design can be textual, graphic, or both. |
| A physical design focuses on specific solutions explaining how they are assembled or configured. | A logical design focuses on satisfying the design factors, including risks, requirements, constraints, and assumptions. |

# IOT UNIT 2

# 1.Explain IOT security with http protocol.

* IOT primarily makes use of standard protocol and networking technologies. on the other hand ,the technologies and protocol of IOT are RFID, NFC, low-energy radio protocol ,LTE-A, and Wi Fi-Direct. These technologies support the specific networking functionality required in an IOT system in contract to a standard consistent network of common system.
* Hypertext Transfer Protocol(http) is a stateless request Protocol in HTTP client request information from a server and the server response to these request accordingly
* A request is mainaly made up od a three digit status code ,some headers and some optional content .
* Each resource is consider as a collection of Hypertext document or HTML document . HTML document are identify by a Uniform Resource Locator(URL)
* Client use the GET method to request a resource from the corresponding server.in the structure of the URL presented next the resource is identified by the path and the server by the authority portion of the URl
* To upload and remove the content from the server PUT and DELETE method are used.
* The POST method permit them to send data to a resource on the server, for example ,in a web form .URL structure
* HTTP defines a set of headers the header can be used to attach meta information about the request and response sent response sent over the network
* The headers are human readable key value text pairs and it contain information about how content are encoded, how long they are valid what type of content is preferred

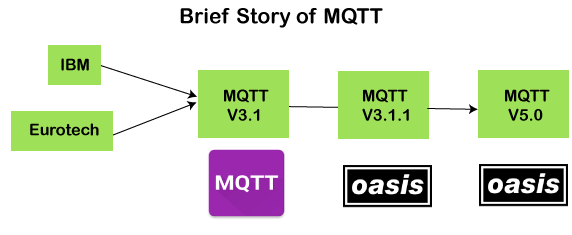
2. write a short note on UPnp.

* UPnP is a common protocol. It is used by all network enabled consumer electronics products utilized in your home or office. UNpn is avery important part of Digital Living Network Alliance(DLNA)
* UPnP forum (upnp.org) is the standard body for UPnP is mainaly based on an HTTP application in which both client and server are participants.HTTP is extended so that it can be used over TCP and UDP.
* TCP and UDP both uses unicast addressing (HTTPU) and multicast addressing (HTTPMU).simple service Discovery Protocol (SSDP) is used to do the discovery of device in the network ; it is based on HTTP over UDP.
* General Event Notification Architecture (GENA) is used for event subsciptions and notification . both SSDP and GENA bring in novel HTTP method to search, notify and subscribe to and unsubscribe from an event.
* Devices use multicast addressing and the available services to find each other by notifying the network of their existence. On the other hand , devices also search for the network using multicast addressing for certain type of devices or services. Action on services are called utilizing SOAP web service calls.

3.wtite a short note on CoAp.

* HTTP is a enormously popular protocol . the UpnP protocol has benefits of simplifying HTTP and using it over UDp instead of TCP.
* But for small resource constrained device that communicates over resource constrained Ip network HTTPU is not a practical option because it needs too many resources and in excess of bandwidth.
* Thise is particularly the case when the fundamental network limit the size of datagrams , which is the case when you use IPv6 Low Power wireless Personal Area Networks (6loWPAN),a radio networking protocol based on the latest version of Internet Protocol Version 6(IPv6).Constrained Application Protocol (CoAP)is used to try solved thise problem.
* The major difference between CoAP and HTTPU is that text headers. used by the HTTPU are replace by the CoAP with more compact binary headers . it also reduce the number of option available in the header .it makes CoAP much easier to reduce and parse CoAP messages.
* CoAP also reduce the set of methods that can be used . it offers four methods :CET,POST,PUT and DELETE.
* CoAP perform the method calls by using confirmable and non confirmable message , then the receiver always return an acknowledgement message after a time period.
* CoAP also reduce the number of response code to makes the implementation simple.
* CoAP also provides a few new features such as with HTTPU, CoAP supports multicasting .it is used to detect devices or communicate through firewel
* CoAP also offers a set of helpful extensions. One of these extension offers a block transfer algorithm permits you to transfer bigger amounts of data.
* One more extension permits you to have an event subscription and notification architecture where observable resources, which produce notification when events occur, can be subscribed to.
* CoAP support encryption in the unicast case via the use of Datagram Transport Layer Security(DTLS).
* As CoAP is comparatively new. So the availability of development tools for thise protocol is a bit restricted . in the firefox add ons are exist , they allow you to view and interest with CoAP resources

4.write a short note on MQTT.

* MQTT stands for **Message Queuing Telemetry Transport**. MQTT is a machine to machine internet of things connectivity protocol. It is an extremely lightweight and publish-subscribe messaging transport protocol.
* This protocol is useful for the connection with the remote location where the bandwidth is a premium. These characteristics make it useful in various situations, including constant environment such as for communication machine to machine and internet of things contexts.
* It is a publish and subscribe system where we can publish and receive the messages as a client. It makes it easy for communication between multiple devices. It is a simple messaging protocol designed for the constrained devices and with low bandwidth, so it's a perfect solution for the internet of things applications
* **Characteristics of MQTT**
* The MQTT has some unique features which are hardly found in other protocols. Some of the features of an MQTT are given below:
* It is a machine to machine protocol, i.e., it provides communication between the devices.
* It is designed as a simple and lightweight messaging protocol that uses a publish/subscribe system to exchange the information between the client and the server.
* It does not require that both the client and the server establish a connection at the same time
* It provides faster data transmission, like how WhatsApp/messenger provides a faster delivery. It's a real-time messaging protocol
* It allows the clients to subscribe to the narrow selection of topics so that they can receive the information they are looking for.
* features that make the code in place.
* The MQTT was developed by Dr. Andy Stanford-Clark, [IBM](https://www.javatpoint.com/ibm-full-form), and Arlen Nipper. The previous versions of protocol 3.1 and 3.1.1 were made available under MQTT ORG.
* In 2014, the MQTT was officially published by OASIS. The OASIS becomes a new home for the development of the MQTT. Then, the OASIS started the further development of the MQTT.
* Version 3.1.1 is backward comfortable with a 3.1 and brought only minor changes such as changes to the connect message and clarification of the 3.1 version. The recent version of MQTT is 5.0, which is a successor of the 3.1.1 version.
* Version 5.0 is not backward, comfortable like version 3.1.1. According to the specifications, version 5.0 has a significant number of features that make the code in place.
* **components of the MQTT.**
* **Message**
* **Client**
* **Server or Broker**
* **TOPIC**

5.write a short note on XMPP.

* The MQTT protocol is limited for a single communication pattern the is the publish/subscribe pattern.
* It is in cases where a things only publishes data has many consumers of its data and where data is homogenous and most reported data item are actually used.
* If individually tailored momentary values, or real-time, bidirectional communication is important and if data is rarely used compared to the frequency with which it is updated , new communication pattern would be more suitable .
* Extensible Messaging and Presence Protocol(XMPP) protocol uses message brokers to bypass firewall barriers. It support publish/subscribe pattern as well as other communication pattern , like point-to-point request/response and asynchronous messaging that permit you to have a richer communication experience
* XMPP was initially designed for use in instant messaging application for example chat. XMPP is an open protocol and it is standardized by Internet Engineering Task Force (IETF),as are HTTP and CoAP.
* As it was design for chat application , it provides itself very well to other application for , example , for IOT , because of its flexibility and richness of communication pattern.
* The XMPP architecture builds on the great success and universal scalability of the Simple Transfer Protocol (SMTP).
* The XMPP is design for real-time instant messaging applications, where smaller messages are sent with as little latency as possible and without any diligence.
* XMPP server offer an authenticated identity to each client . if the server is a public server in universal federated network of XMPP server then it is a global identity.
* When the client connects to the server the server ensure that the clients authenticate themselves by giving their corresponding client credentials like username and password.
* This authentication is performed securely using an extensible architecture based on Simple Authentication and Security Layer(SASL).
* The connection can also be switched over to Transport Layer Security (TLS) through negotiation between the client and the server, encrypting the communication between them.
* The client identity is often called XMPP address or Jabber ID(JID). Each connection is also bound to a particular resource , which is usually a random string.
* Together, the username, domain name , and resource make up the full JID of a connection , while only the username make up the JID of an account.
* A rich set of communication pattern is supported by the XMPP. It provides 3 communication primitive , they are known as stanza , the first is presence stanza it is used to sent the information about oneself to the authorized and interested parties.
* Second is the message stanza and it is used to asynchronous messages to a given receiver.
* Third is the IQ (information Query) stanza . it is used to offer a request/response communication pattern . a request is send to the receiver and the receiver sends the reply or an error
* The XMPP standards foundation(XSF) publishes a set of extensions which anyone can used . these extensions are known as XMPP Extension Protocols(XEPs).
* To promote the interoperability XSF publishes such extension . anyone can become a member of it and promote the development of new existing extension.
* The first stage is experimental where extension is recognized as a factor that would give a solution for an important use case but still under discussion and can go through important changes in the process.
* Second stage is draff , where the extension has go through wide discussion and technical review.
* Any alteration made to an extension in this stage should always be made in a backward-compatible manner if possible . the last stage is the final stage where changes are no longer made.

6. write short note on different modes of attack.

* The Internet of Things (IoT) has given us loads of valuable new devices, but it’s also created a new kind of security risk for organizations. Many people don’t see the danger posed by something as simple as a smart thermostat or lightbulb. So how does the issue of cybersecurity relate to the Internet of Things? Most of these devices have poor security requirements and serve as a platform for criminals to access the wider network.
* Fortunately, while the industry adapts to IoT risks and challenges, there’s plenty you can do to prevent cybersecurity issues from IoT devices.
* Common Types of IoT Cyber Attacks First, let’s take a look at the types of cyberattacks we’re working with. Common IoT attacks include:
* **Distributed denial of service (DDoS):** A DDoS attack occurs when a [botnet](https://agio.com/the-rise-of-iot-botnet-attacks/) — a network of computers — consistently and simultaneously requests services from a business. This extreme demand shuts the system down as it tries to serve the requests.
* **Firmware exploits:** Many cybercriminals use known vulnerabilities. Often, these vulnerabilities have patches available from the developer, but the user hasn’t downloaded them, leaving them open to the hack.
* **Man-in-the-middle:** In this type of IoT attack, the hacker intercepts the communication between two connected systems. The victim may believe they’re legitimately communicating with someone, but they’re actually leaking information to the hacker.
* **Data interception:**Since many IoT devices are not encrypted, attackers can snag information, such as login credentials, without needing to decrypt it.
* **Physical attacks:**Simply plugging a USB into an IoT device can
* be enough to spread malware to a network or spy on the communications.
* **Brute force attacks:**Just as passwords can be brute-forced, many IoT devices can be hacked with a system that generates password guesses until it gets through.
* **Unauthorized access:**With so many interconnected IoT devices, intrusion can lead to serious physical breaches. An IoT-enabled door lock may sound incredibly convenient until it lacks sufficient security and leads to an office break-in.
* **Ransomware:**Ransomware blocks access to a system until the hacker is paid. IoT devices can grant access to the larger system or be locked themselves.
* **Radio frequency jamming:**By interfering with radio signals, hackers can prevent IoT devices from communicat.

**7.Explain IOT protocol**..

* IOT primarily makes use of standard protocol and networking technologies. on the other hand ,the technologies and protocol of IOT are RFID, NFC, low-energy radio protocol ,LTE-A, and Wi Fi-Direct. These technologies support the specific networking functionality required in an IOT system in contract to a standard consistent network of common systems.

NFC and RFID

* RFID (ratio -frequency identification ) and NFC(near-field communication ) offer simple , low energy, and flexible option for identity and access tokens, connection bootstrapping , and payments.
* RFID technology employs two-way ratio transmitter-receivers to identity and track tag connected with object.
* NFC consist of communication protocol for electronic devices , normally a mobile device and a standard devices.

Low Energy Bluetooth

* Low energy Bluetooth supports the low power ,long use need of IOT function while exploiting a standard technology with native support across systems.

Low-Energy Wireless

* Low level wireless technology replace the most power keen aspect of an IOT system.
* Though sensors and other element can power down over long periods, communication links( I . e, wireless)must remain in listening mode.
* Low-energy wireless not only reduce consumption , but also extends the life of the devices through less use.

Radio Protocol

* The radio protocol are ZigBee ,z-wave and thread are used for creating low-rate private area network.
* These technology are low-power, but provide high throughput unlike many option . this increases the power of small local devices network without the typical costs.

LTE-A

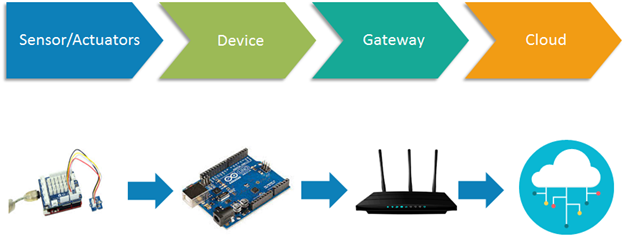
* LTE-A or LTE advanced , deliver an important upgrade to LTE technology by increasing not only its coverage , but also reducing its latency and raising its throughput.
* It gives IOT a tremendous power through expanding its range , with its most significant application being vehicle, UAV , and similar communication

WiFi-Direct

* Wi Fi Direct removes the need for an access point .it permits peer-to-peer (P2P)connection with the speed of Wi Fi , but with lower latency.
* Wi Fi Direct removes an element of a network that often bogs it down and it does not compromise on speed or throughput.

8)Explain Architecture of IOT.

* There is not such a unique or standard consensus on the Internet of Things (IoT) architecture which is universally defined.
* The IoT architecture differs from their functional area and their solutions. However, the IoT architecture technology mainly consists of four major components:
* **Components of IoT Architecture**
* Sensors/Devices
* Gateways and Networks
* Cloud/Management Service Layer
* Application Layer

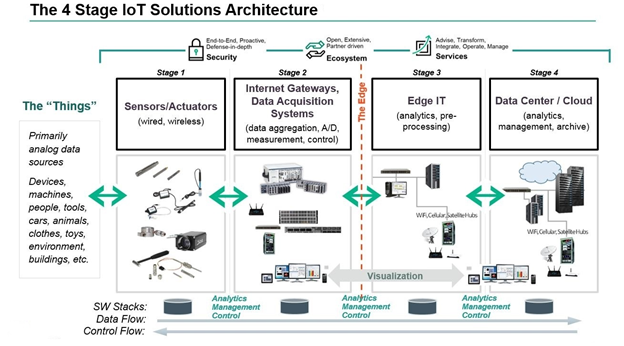


## **Stages of IoT Solutions Architecture**

## There are several layers of IoT built upon the capability and performance of IoT elements that provides the optimal solution to the business enterprises and end-users. The IoT architecture is a fundamental way to design the various elements of IoT, so that it can deliver services over the networks and serve the needs for the future.

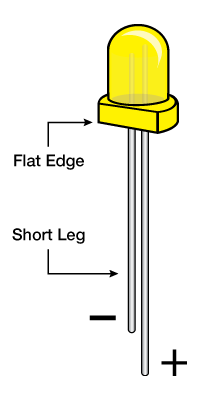
## Following are the primary stages (layers) of IoT that provides the solution for IoT architecture.

1. **Sensors/Actuators:** Sensors or Actuators are the devices that are able to emit, accept and process data over the network. These sensors or actuators may be connected either through wired or wireless. This contains GPS, Electrochemical, Gyroscope, RFID, etc. Most of the sensors need connectivity through sensors gateways. The connection of sensors or actuators can be through a Local Area Network (LAN) or Personal Area Network.
2. **Gateways and Data Acquisition:** As the large numbers of data are produced by this sensors and actuators need the high-speed Gateways and Networks to transfer the data. This network can be of type Local Area Network (LAN such as WiFi, Ethernet, etc.), Wide Area Network (WAN such as GSM, 5G, etc.).
3. **Edge IT:** Edge in the IoT Architecture is the hardware and software gateways that analyze and pre-process the data before transferring it to the cloud. If the data read from the sensors and gateways are not changed from its previous reading value then it does not transfer over the cloud, this saves the data used.
4. **Data center/ Cloud:** The Data Center or Cloud comes under the Management Services which process the information through analytics, management of device and security controls. Beside this security controls and device management the cloud transfer the data to the end users application such as Retail, Healthcare, Emergency, Environment, and Energy, etc.

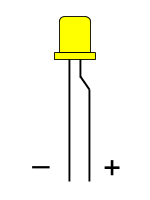


**9)Write short note on IOT LED.**

* LEDs (light-emitting diodes) are small, bright, power-efficient lights commonly used in electronic products.An LED light is a [polarized](https://learn.sparkfun.com/tutorials/polarity) part, meaning it has to be connected to a circuit in a certain way to work properly. Specifically, each LED has a positive leg and a negative leg. These can be identified visually by length: the negative leg has been made shorter.



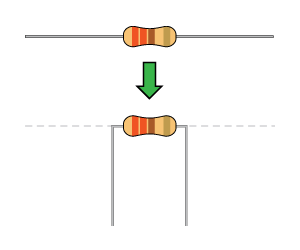
* To make it easier to insert the LED into a breadboard, you can carefully bend the positive leg as shown, so both legs become the same length. You can still identify them visually: the straight leg is negative, and the bent leg is positive.



* The negative leg of the LED has to be connected to GND (-). The positive leg is connected to any I/O pin, which will serve as the voltage source (+).

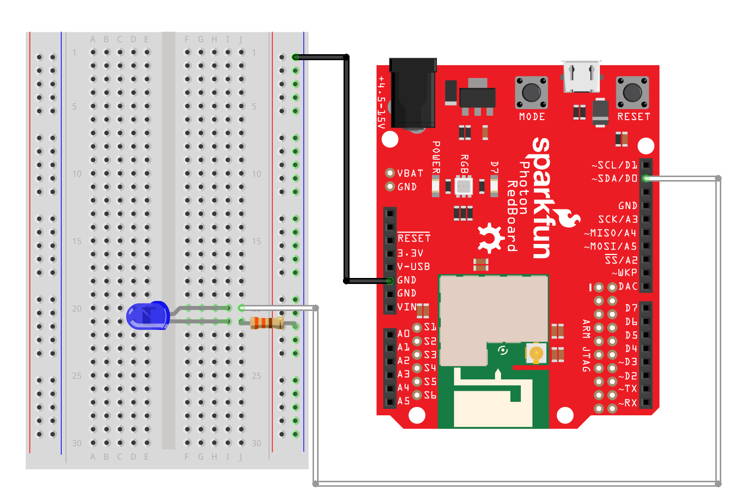
### Resistor

* An LED can be easily burned out if it receives too much power. Therefore, a [resistor](https://learn.sparkfun.com/tutorials/resistors) **must** be used to help limit the amount of current flowing through the LED.In order to use a resistor, you will need to bend both ends into 90° angles, so the resistor can be inserted into the holes on a breadboard.



* The resistor is typically used in place of a jumper wire to connect the negative leg of the LED to GND (-).

|  |  |
| --- | --- |
| LED Light | Photon Pin |
| Positive leg (long) = Power | any I/O pin |
| Negative leg (short) = Ground | GND using resistor |
|  |  |



## Code for LED Light

### Library

The LED does **not** require any special code library.

### Global Variables

In the global variables, you should declare a variable to represent the specific pin on the Photon board that the LED is connected to. This will make it easier to understand your code (and easier to modify the code if you change which pin the LED is connected to). The example below declares a variable called "led" (but you could use a different variable name).

// if necessary, change pin number to match your wiring

int led = D0;

If you are using **multiple** LED lights, then be sure to give each LED a unique variable name. Use variable names that will make sense when someone reads your code.

// global variables

int redLed = D0;

int blueLed = D1;

### setup( ) function

Within the setup() function, you have to include a statement to set the pin mode for the LED pin variable:

pinMode(led, OUTPUT);

If you are using multiple LED lights, be sure to set the pin mode for each LED's pin variable.

* **IMPORTANT:** If you want an LED light to be **off** when your device first starts, then be sure to include code to do this within the setup() function (after setting the pin mode). Otherwise, the LED light might be on (at a low brightness) when the device starts, depending on which I/O pin the LED is connected to.

10.write a short note on IOT buttons.

* Nowadays, IoT technologies are penetrating many industries and companies that aim to find new ways for automating and extending their business processes. According to Impact,**more than 60% of organizations currently use IoT solutions**. Impact also states that 83% of businesses that have implemented IoT technologies have increased their efficiency.
* At the same time, a certain stereotype exists that only big enterprises with significant budgets can use modern IoT solutions. However, there are also devices available on the market that can help small and medium businesses carry-out different actions in several easy steps. One of such IoT devices is the IoT button that is relatively low-cost and programmable. But it can provide endless possibilities and benefits from the touch-of-a-button functionality
* The IoT button is a programmable, handheld input device that allows automating actions by pushing a button on a specific wireless dongle. It can work through Wi-Fi or other communication protocols such as Zigbee and Z-Wave. The device has three types of modes: single-click, double-click, and long-press. You can configure IoT button clicks logic, which allows sending associated notifications wirelessly and triggering actions depending on the press type. Also, the IoT button can transmit its status due to various LED colors or blinking patterns.
* When choosing the appropriate IoT button to implement in your company, there is a wide range of brands to consider. Among the most popular ones, you can find the AWS IoT Button, Flic, Azure IoT Button, goButton.
* Thus, we have prepared for you a few cases of implementing the IoT button that can be helpful for your business.
* Implementing the IoT button can help your company create new services for clients, offer new features for current ones, and automate operations to increase operational efficiency. This technology can enhance client engagement, expand applications, and provide innovations to customers as it simplifies the user experience. By using the power of IoT, companies can respond to client demand for products or services in real-time and maintain a direct line of communication with clients, all via the IoT button.
* For businesses, there can be many use cases that will benefit from implementing the IoT button solution. Here you can find some ideas:
* capture product amounts for managing inventory systems efficiently;
* enhance reordering services and custom products like screws, nuts, or washers;
* allow customers to request a callback from a client service agent;
* provide a call-for-assistance button in cafes or stores to improve retail operations;
* promote healthcare applications for the disabled or elderly patients;
* integrate with smart systems for turning on/off different devices in the office;
* improve check-in/check-out systems for guests.

11.write a short note on IOT camera.

A **smart camera (sensor)** or **intelligent camera (sensor)** or **(smart) vision sensor** or **intelligent vision sensor** or **smart optical sensor** or **intelligent optical sensor** or **smart visual sensor** or **intelligent visual sensor** is a [machine vision](https://en.wikipedia.org/wiki/Machine_vision) system which, in addition to image capture circuitry, is capable of extracting application-specific information from the captured images, along with generating event descriptions or making decisions that are used in an intelligent and automated system.[[1]](https://en.wikipedia.org/wiki/Smart_camera#cite_note-1)[[2]](https://en.wikipedia.org/wiki/Smart_camera#cite_note-2) A smart camera is a self-contained, standalone vision system with built-in [image sensor](https://en.wikipedia.org/wiki/Image_sensor) in the housing of an industrial video camera. The vision system and the image sensor can be integrated into one single piece of hardware known as **intelligent image sensor** or **smart image sensor**. It contains all necessary communication interfaces, *e.g.* Ethernet, as well as industry-proof 24V I/O lines for connection to a [PLC](https://en.wikipedia.org/wiki/Programmable_logic_controller), actuators, relays or pneumatic valves, and can be either static or mobile.[[3]](https://en.wikipedia.org/wiki/Smart_camera#cite_note-3) It is not necessarily larger than an industrial or [surveillance camera](https://en.wikipedia.org/wiki/Surveillance_camera). A capability in [machine vision](https://en.wikipedia.org/wiki/Machine_vision) generally means a degree of development such that these capabilities are ready for use on individual applications. This architecture has the advantage of a more compact volume compared to PC-based vision systems and often achieves lower cost, at the expense of a somewhat simpler (or omitted) [user interface](https://en.wikipedia.org/wiki/User_interface). Smart cameras are also referred to by the more general term **smart sensors**

## **Components[**[**edit**](https://en.wikipedia.org/w/index.php?title=Smart_camera&action=edit&section=2)**]**

A smart camera usually consists of several (but not necessarily all) of the following components:

* Image sensor (matrix or linear, [CCD](https://en.wikipedia.org/wiki/Charge-coupled_device)- or [CMOS](https://en.wikipedia.org/wiki/CMOS))
* Image [digitization](https://en.wikipedia.org/wiki/Digitize) circuitry
* Image memory
* [processor](https://en.wikipedia.org/wiki/Central_processing_unit) (often a [DSP](https://en.wikipedia.org/wiki/Digital_signal_processor) or suitably powerful processor)
* program- and data memory (RAM, nonvolatile FLASH)
* Communication interface ([RS-232](https://en.wikipedia.org/wiki/RS-232), [Ethernet](https://en.wikipedia.org/wiki/Ethernet))
* [I/O](https://en.wikipedia.org/wiki/Input/output) lines (often opto-isolated)
* Lens holder or built in lens (usually C, CS or M-mount)
* Built in illumination device (usually [LED](https://en.wikipedia.org/wiki/LED))
* Purpose developed real-time operating system (For example VCRT)
* Optional video output (e.g. [VGA](https://en.wikipedia.org/wiki/VGA) or [SVGA](https://en.wikipedia.org/wiki/SVGA))
* Energy supply by e.g. [energy harvesting](https://en.wikipedia.org/wiki/Energy_harvesting)

## **Fields of application[**[**edit**](https://en.wikipedia.org/w/index.php?title=Smart_camera&action=edit&section=3)**]**

Having a dedicated processor in each unit, smart cameras are especially suited for applications where several cameras must operate independently and often asynchronously, or when distributed vision is required (multiple inspection or surveillance points along a production line or within an assembly machine). In general smart cameras can be used for the same kind of applications where more complex vision systems are used, and can additionally be applied in some applications where volume, pricing or reliability constraints forbid use of bulkier devices and PC's.

Typical fields of application are:

* [automated inspection](https://en.wikipedia.org/wiki/Automated_inspection) for [quality assurance](https://en.wikipedia.org/wiki/Quality_assurance) (detection of defects, flaws, missing parts...)
* non contact measurements.
* part sorting and identification.
* code reading and verification ([barcode](https://en.wikipedia.org/wiki/Barcode), [Data Matrix](https://en.wikipedia.org/wiki/Data_Matrix), [alphanumeric](https://en.wikipedia.org/wiki/Optical_character_recognition) etc.)
* web inspection (inspection of continuously flowing materials such as coils, tubes, wires, extruded plastic) for defect detection and dimensional gauging.
* detection of position and rotation of parts for [robot](https://en.wikipedia.org/wiki/Robot) guidance and automated picking
* unattended [surveillance](https://en.wikipedia.org/wiki/Surveillance) (detection of intruders, fire or smoke detection)
* [biometric](https://en.wikipedia.org/wiki/Biometrics) recognition and access control ([face](https://en.wikipedia.org/wiki/Facial_recognition_system), [fingerprint](https://en.wikipedia.org/wiki/Fingerprint), [iris](https://en.wikipedia.org/wiki/Iris_scan) recognition)
* [visual sensor networks](https://en.wikipedia.org/wiki/Visual_sensor_network) and [smartdust](https://en.wikipedia.org/wiki/Smartdust" \o "Smartdust)
* [robot](https://en.wikipedia.org/wiki/Robot) guidance
* nearly any [machine vision](https://en.wikipedia.org/wiki/Machine_vision) application

Developers can purchase smart cameras and develop their own programs for special, custom made applications, or they can purchase ready made [application software](https://en.wikipedia.org/wiki/Application_software) from the camera manufacturer or from [third party](https://en.wikipedia.org/wiki/Third-party_source) sources. Custom programs can be developed by programming in various languages (typically [C](https://en.wikipedia.org/wiki/C_programming_language) or [C++](https://en.wikipedia.org/wiki/C%2B%2B)) or by using more intuitive, albeit somewhat less flexible, [visual development tools](https://en.wikipedia.org/wiki/Visual_programming_language) where existing functionalities (often called tool or blocks) can be connected in a list (a sequence or a bi-dimensional flowchart) that describes the desired [flow of operations](https://en.wikipedia.org/wiki/Dataflow) without any need to write program code. The main advantage of the visual approach versus programming is the shorter and somewhat easier development process, available also to non-programmers. Other development tools are available with relatively few but comparatively high level functionalities, which can be configured and deployed with very limited effort.

12. write a short note on IOT motor.

## **What is Servo Motor?**

Servo motor is a [rotary actuator](https://en.wikipedia.org/wiki/Rotary_actuator) or [linear actuator](https://en.wikipedia.org/wiki/Linear_actuator) . It allows for precise control of angular or linear position, velocity and acceleration. It consists of a suitable motor coupled to a sensor for position feedback. It also requires a relatively sophisticated controller. Often a dedicated module designed specifically for use with servo motors.

[](https://robu.in/wp-content/uploads/2020/04/tower-pro-mg995-13kg013s-60g-standard-servo-768x768-1.jpg)

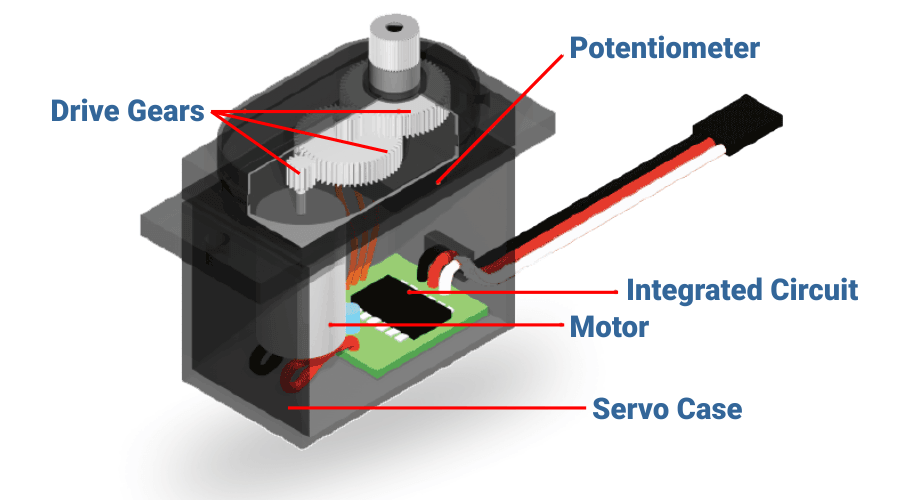
It is an electrical device which can push or rotate an object with great precision. If you want to rotate an object at some specific angles or distance, then you have to use servo motor. It is just a simple motor which run through **servo mechanism**.

If the motor uses the DC power as supply then it is the DC servo motor. If the motor uses an AC power as supply then it is an AC servo motor. We can get a very high torque servo motor in a small and light weight packages. Due to these features they uses in many applications like toy car, RC helicopters and planes, Robotics, Machines etc

**MUST READ BLOG POSTS ON SERVO MOTOR:**

* [What are the types of servo motor?](https://robu.in/types-of-servo-motor/)
* [Servo Motor Working Principle](https://robu.in/servo-motor-working/)
* [Interfacing servo motor using Arduino](https://robu.in/interfacing-servo-motors-controllers-sc08a-sc16a-using-arduino/)

## **Construction of Servo Motor**

[](https://robu.in/wp-content/uploads/2020/04/Servo-motor-constructons.png)

This motor is a closed-loop mechanism that incorporates positional feedback in order to control the rotational or linear speed and position.

This motor is actually an assembly of four things:

* Normal DC motor- That is in charge of generating the motion through its shaft.
* Gear reduction unit/gear box
* Potentiometer
* Control circuit

The [DC motor](https://robu.in/product-category/motors-drivers-actuators/dc-motor/) connects with a gear mechanism which provides feedback to a position sensor which is mostly a potentiometer.

It is connected to the central shaft, and informs at all times the angle in which the motor’s shaft is available

From the gear box or gear reduction unit, the output of the motor delivers via servo spline to the servo arm.  the gear box is formed by gears which may increase or decrease the speed and torque.

The standard servo motor uses the plastic gear whereas the high power servo motor uses the metal gear.

A control circuit allows for control over the motor’s motion by sending electric pulses

Motor consists of three wires- a black wire connected to ground. A white/yellow wire connected to control unit. And a red wire connected to power supply.

## **Advantages of Servo Motor**

* If a heavy load places on the motor, the driver will increase the current to the motor coil as it attempts to rotate the motor. Basically, there is no out-of-step condition.
* High-speed operation is possible.

## **Disadvantages of Servo Motor**

* Since the motor tries to rotate according to the command pulses, but lags behind. it is not suitable for precision control of rotation.
* Higher cost.
* When stopped, the motor’s rotor continues to move back and forth one pulse. So that, it is not suitable if you need to prevent vibration

## **Applications of Servo Motor**

It uses in the applications requiring rapid variations in speed without the motor getting overheated.

[](https://robu.in/wp-content/uploads/2020/04/applications.png)

* Industries, they uses in the machine tools, packaging, factory automation, material handling, printing converting, assembly lines. In many other demanding applications robotics, CNC machinery or automated manufacturing.
* uses in radio controlled airplanes to control the positioning and movement of elevators.
* In robots because of their smooth switching on and off and accurate positioning.
* In the aerospace industry to maintain hydraulic fluid in their hydraulic systems.
* uses in many radio controlled toys.
* used in electronic devices such as DVDs or Blue ray Disc players to extend or replay the disc trays.
* used in automobiles to maintain the speed of vehicles

13.explain type of sensor.

### 1. Temperature Sensors

Temperature sensors measure the amount of heat energy in a source, allowing them to detect temperature changes and convert these changes to data. Machinery used in [manufacturing](https://behrtechnologies.com/solutions/manufacturing/) often requires environmental and device temperatures to be at specific levels. Similarly, within agriculture, soil temperature is a key factor for crop growth.

### 2. Humidity Sensors

These types of sensors measure the amount of water vapor in the atmosphere of air or other gases. Humidity sensors are commonly found in heating, vents and air conditioning (HVAC) systems in both industrial and residential domains. They can be found in many other areas including hospitals, and meteorology stations to report and predict weather.

### 3. Pressure Sensors

A pressure sensor senses changes in gases and liquids. When the pressure changes, the sensor detects these changes, and communicates them to connected systems. Common use cases include leak testing which can be a result of decay. Pressure sensors are also useful in the manufacturing of water systems as it is easy to detect fluctuations or drops in pressure.

### 4. Proximity Sensors

Proximity sensors are used for non-contact detection of objects near the sensor. These types of sensors often emit electromagnetic fields or beams of radiation such as infrared. Proximity sensors have some interesting use cases. In retail, a proximity sensor can detect the motion between a customer and a product in which he or she is interested. The user can be notified of any discounts or special offers of products located near the sensor. Proximity sensors are also used in the parking lots of malls, stadiums and airports to indicate parking availability. They can also be used on the assembly lines of chemical, food and many other types of industries.

### 5. Level Sensors

Level sensors are used to detect the level of substances including liquids, powders and granular materials. Many industries including oil manufacturing, water treatment and beverage and food manufacturing factories use level sensors. Waste management systems provide a common use case as level sensors can detect the level of waste in a garbage can or dumpster

### 6. Accelerometers

Accelerometers detect an object’s acceleration i.e. the rate of change of the object’s velocity with respect to time. Accelerometers can also detect changes to gravity. Use cases for accelerometers include smart pedometers and monitoring driving fleets. They can also be used as anti-theft protection alerting the system if an object that should be stationary is moved.

### 7. Gyroscope

Gyroscope sensors measure the angular rate or velocity, often defined as a measurement of speed and rotation around an axis. Use cases include automotive, such as car navigation and electronic stability control (anti-skid) systems. Additional use cases include motion sensing for video games, and camera-shake detection systems.

### 8. Gas Sensors

These types of sensors monitor and detect changes in air quality, including the presence of toxic, combustible or hazardous gasses. Industries using gas sensors include mining, oil and gas, chemical research andmanufacturing. A common consumer use case is the familiar carbon dioxide detectors used in many homes.

### 9. Infrared Sensors

These types of sensors sense characteristics in their surroundings by either emitting or detecting infrared radiation. They can also measure the heat emitted by objects. Infrared sensors are used in a variety of different IoT projects including healthcare as they simplify the monitoring of blood flow and blood pressure. Televisions use infrared sensors to interpret the signals sent from a remote control. Another interesting application is that of art historians using infrared sensors to see hidden layers in paintings to help determine whether a work of art is original or fake or has been altered by a restoration process.

### 10. Optical Sensors

Optical sensors convert rays of light into electrical signals. There are many applications and use cases for optical sensors. In the auto industry, vehicles use optical sensors to recognize signs, obstacles, and other things that a driver would notice when driving or parking. Optical sensors play a big role in the development of driverless cars. Optical sensors are very common in smart phones. For example, ambient light sensors can extend battery life. Optical sensors are also used in the biomedical field including breath analysis and heart-rate monitors.

14.Explain analog digital sensor in IOT.

* A signal may fall under two categories, which include digital and analog. **A signal involves information being transmitted between two separate electronic devices**. Keep in mind, however, that signals aren’t associated specifically with electronic devices. Signals also occur with standard thermometers when a temperature is displayed via the expansion or contraction of mercury.
* An analog signal is a continuous signal where the solution will vary based on the time at which the signal is displayed. An example of an analog signal involves the human voice. As for [digital signals](https://sensorex.com/product/ssre-smart-sensor-remote-electronics/), these are considered to be discrete signals that are typically comprised of two values, which are low and high. What sets these signals apart? What types of applications can these signals be used for? All of these questions are answered in the following.



## **Digital Sensors**

* As mentioned previously, digital sensors produce a discrete digital voltage or signal that is considered to be a digital representation of a measurement. This sensor will [display binary output](https://docs.johnsoncontrols.com/bas/api/khub/documents/u9GLBrPy9pHIGOVwLH_tLg/content) in ones and zeros. Digital sensors tend to be considerably less expensive when compared to analog ones. These sensors are known to have a fast transmission rate as well as negligible distortion.
* The main reason that many people prefer using digital sensors is because they don’t have the same limitations as analog sensors. Keep in mind that digital sensors are commonly used across such applications as [wastewater treatment](https://sensorex.com/2021/06/14/benefits-behind-biofiltration/), water purification, and similar industrial processes. If you decide to purchase a digital sensor of any kind, **the item should be comprised of a sensor, a transmitter, and a cable**.

## **Analog Sensors**

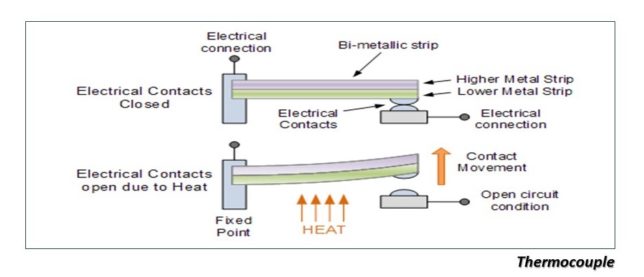
* Analog sensors are much different than digital sensors and typically have less features. These sensors create what is known as an analog signal, which is a continuous signal that represents a quantity. An analog sensor trades efficiency for a more continuous and slightly more accurate signal. While the feature-set of an analog sensor won’t match that of a digital sensor, you can be more confident in the readings you obtain.
* The analog quantities that are **known to be continuous in nature include speed, pressure, displacement, strain, and temperature**. For instance, you can use a thermometer to measure the temperature of a liquid. By obtaining continuous readings, the analog sensor will respond immediately to any changes that occur in the temperature of the liquid as its heats up or cools down.
* While there are many types of analog sensors, among the most common type is a pressure sensor, which is commonly used in industrial and lab settings to manage the pressure of liquids or gases. Pressure is typically measured by identifying the force per unit area. These sensors will act as transducers by generating a signal when pressure is imposed.
* A pressure sensor is used to monitor and control hundreds of applications. Facilities can also use these sensors to indirectly measure such variables as gas and fluid flow, water level, speed, and altitude. Keep in mind that pressure analog sensors may also be referred to as pressure transducers, pressure senders, pressure transmitters, and pressure indicators.

15.explain temperature sensor in IOT.

* A temperature sensor is a device which provides temperature measurement through an electrical signal. The most common types are Thermocouple, Resistance Temperature Detector (RTD) and Thermistor. These are some of the most commonly used in the internet of things.

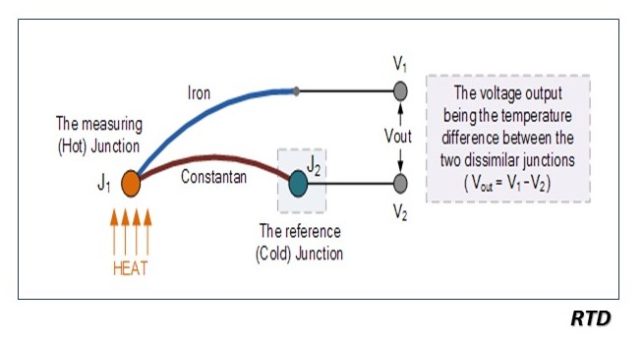
##### ****Thermocouple****

* A thermocouple (T/C) is made from two dissimilar metals that generate electrical voltage in direct proportion to changes in temperature.
* A T/C is made from two dissimilar metal wires. These wires are joined together at one end to form a measuring (hot) junction. (
* A thermocouple will generate a measurement signal not in response to actual temperature, but in response to a difference in temperature between the measuring and reference junctions.
* A small ambient temperature sensor is built into the electronic measuring device near the point where the reference junction is attached. The ambient temperature is then added to the thermocouple differential temperature by the measuring device in order to determine and display the actual measured temperature.
* There are many types of thermocouples, each with its own unique characteristics in terms of temperature range, durability, vibration resistance, chemical resistance, and application compatibility.



##### ****Resistance Temperature Detector (RTD)****

* An RTD is a variable resistor that will change its electrical resistance in direct proportion to changes in temperature in a precise, repeatable and nearly linear manner.
* To greater or lesser degrees, all electrical conducting materials have some amount of resistance to the flow of electricity. When a known electric voltage passes through a conductor, the resistance varies based on the temperature of the conductor. This resistance can be measured and will correspond to a specific temperature. While various elements are affected by temperature in different ways, platinum is commonly used in an RTD due to its purity, linearity and stability over a wide range of temperatures. An electronic readout device, such as a controller or digital indicator designed to measure resistance, is required for use with RTD sensors.
* The most common RTD element material is Platinum, as it is a more accurate, reliable, chemically resistant, and stable material, making it less susceptible to environmental contamination and corrosion than the other metals.



##### ****Thermistor****

* The Thermistor is another type of temperature sensor, whose name is a combination of the words THERM-ally sensitive res-ISTOR.
* A thermistor is a special type of resistor which changes its physical resistance when exposed to changes in temperature. Thermistors are generally made from ceramic materials such as oxides of nickel, manganese or cobalt coated in glass which makes them easily damaged. Their main advantage is their speed of response to any changes in temperature, accuracy and repeatability.
* Most types of thermistor’s have a Negative Temperature Coefficient of resistance or (NTC), that is their resistance value goes DOWN with an increase in the temperature, and of course there are some which have a Positive Temperature Coefficient, (PTC), in that their resistance value goes UP with an increase in temperature.



16.Explain humidity sensor in IOT.

* Humidity sensors are electronic devices that [measure and report the moisture and air temperature of the surrounding environment](https://www.sciencedirect.com/topics/engineering/humidity-sensor) where they are deployed e.g., in air, soil, or confined spaces.
* Humidity measurements indicate the concentration of water vapor presented in the air. They provide their
* measurements in the form of a proper electronic signal. Moreover, they also report relative humidity, i.e., the moisture ratio to the maximum moisture at a given temperature.
* The relative humidity is useful for many applications, like HVAC (Heating Ventilation Air Conditioning) and comfort optimization applications in Smart Buildings and Facilities Management.
* State of the art humidity sensors provide support for internet connectivity and can be flexibly deployed in the Internet of Things (IoT) applications. This facilitates [the integration of humidity measurements with the output of other sensors (e.g., temperature sensors)](https://www.sciencedirect.com/science/article/pii/S221478531733362X) and boosts IoT applications intelligence in various industry applications.
* A humidity sensor’s quality is reflected in its accuracy, reliability, response time, longevity, security, robustness, and ease of deployment. These characteristics also determine the sensor’s cost. Furthermore, they drive the selection of humidity sensors for different applications.

## Applications

* Humidity sensing enables a host of value-added Applications in various industries, including cold storage management, comfort optimization, asset condition tracking, and remote monitoring.

### Humidity Sensors in Cold Storage Management

* In cold storage management, humidity sensing ensures proper storage conditions for temperature-sensitive products such as food, beverage, and pharmaceuticals.
* Humidity sensors contribute to [regulatory compliance](https://www.who.int/medicines/areas/quality_safety/quality_assurance/supplement_6.pdf) and to automating the auditing of the status of the equipment. In conjunction with temperature sensors, they also contribute to increasing product safety, while reducing waste.
* Overall, the combination of [temperature sensors](https://www.iotforall.com/an-introduction-to-iot-sensors) and humidity sensors in cold storage management enables the development of powerful regulatory compliance tools, automation of audits, increased product safety, and improved environmental performance.

### Humidity Sensors in Remote Monitoring and Intelligent Asset Management

* Humidity sensors are also integral elements of remote monitoring and intelligent asset management Applications. They can be deployed on assets (e.g., pumps, compressors, fans, data centers) to facilitate a transition from preventive to predictive maintenance.
* Specifically, humidity sensor data streams can enhance the accuracy of predictive analytics for condition-based monitoring. They also enable the real-time monitoring of humidity to identify problems (e.g., potential leakages) before they occur. In these ways, humidity sensors extend the lifetime of critical assets and maximize their overall efficiency.

17.Explain motion sensor in IOT.

* A motion sensor, or motion detector, is an electronic device that uses a sensor to detect nearby people or objects. Motion sensors are an important component of any security system. When a sensor detects motion, it will send an alert to your security system, and with newer systems, right to your mobile phone. If you have subscribed to an [**alarm monitoring**](https://www.bayalarm.com/commercial/business-alarm-monitoring/) service, motion sensors can even be configured to send an alert to your monitoring team.
* Motion sensors are commonly used to:
* Detect when a potential intruder is near to or inside your home or business.
* Alert you if people enter restricted areas. At home, this might be the basement or garage.
* Save energy by powering lights in an area only when needed.

## **THERE ARE TWO WIDELY USED TYPES OF MOTION SENSORS: ACTIVE ULTRASONIC AND PASSIVE INFRARED (PIR).**

* Active ultrasonic sensors and passive infrared sensors are the two most common motion sensor technologies, both of which are known for their accuracy and reliability.
* Active ultrasonic sensors emit [**ultrasonic sound waves**](https://hyperphysics.phy-astr.gsu.edu/hbase/Sound/usound.html#:~:text=The%20term%20%22ultrasonic%22%20applied%20to,includes%20anything%20over%2020%2C000%20Hz.) at a frequency above the range of human hearing.
* Ultrasonic sensors can detect objects regardless of their color, surface type, or material type (i.e., metallic vs. non-metallic). They can even detect translucent objects, though this is usually reserved for industrial applications.

## **PASSIVE INFRARED SENSORS DETECT FLUCTUATIONS IN INFRARED ENERGY, WHICH HUMANS, ANIMALS, AND OBJECTS RELEASE AS HEAT.**

* PIR sensors are a bit more complex than active ultrasonic sensors, but the result is the same.
* Walls, floors, stairways, windows, cars, dogs, trees, people—you name it—radiate some amount of heat. [**Infrared waves**](https://science.nasa.gov/ems/07_infraredwaves) can detect temperature. Infrared motion sensors detect the presence of a person or object by detecting the change in temperature of a given area.
* A PIR motion sensor uses these temperature changes to detect the presence of a person or object. Like active ultrasonic sensors, PIR sensors can be set to ignore small changes in IR, so you can walk around your home or business without setting off alarms all day and night.

## **THERE ARE A HANDFUL OF LESS COMMONLY USED MOTION SENSOR TECHNOLOGIES.**

* **Tomographic motion sensors** are made up of [**multiple nodes**](https://hometoys.com/tomographic-motion-detection/). The nodes link together, forming a mesh network. These sensors detect the presence of a person or object when the link between two nodes is broken.
* **Vibration motion sensors** detect people and objects via small vibrations caused by things like footsteps.
* **Microwave motion sensors** emit [**microwave pulses**](https://www.sciencedaily.com/terms/microwave.htm). Much like an active ultrasonic sensor, the microwaves bounce off objects and return to the sensor. They actually cover a larger area than PIR sensors, but are more susceptible to electronic interference.
* Some motion sensors are considered “dual technology,” in that they combine two sensor types in one system. Active ultrasonic sensors and PIR sensors are often combined into one unit with the goal of increasing detection accuracy. You can always talk with your alarm installer to make sure your motion sensors are the most suitable options for your home or business.

## **MOTION SENSORS HAVE A LIMITED RANGE. WORK WITH A PROFESSIONAL TO DETERMINE WHERE BEST TO INSTALL THEM TO MAXIMIZE YOUR SECURITY COVERAGE.**

* Typical motion sensors have a range of up to 80 feet, meaning a single motion sensor probably won’t cover a long hallway or an open workspace. You can hire a security company like Bay Alarm to install your security system. Our installers will review the layout of your space to determine where exactly to place motion sensors. As with [**security cameras**](https://www.bayalarm.com/home-security/home-security-cameras/), [**fire alarms**](https://www.bayalarm.com/home-security/residential-monitored-fire-alarms-smoke-detectors/), and [**burglar alarm**](https://www.bayalarm.com/home-security/home-burglar-alarm-systems/) installations, our goal is to ensure your home or business is as secure as possible, with devices and components placed in the most strategic locations.
* Motion sensors are an essential part of any security system: they represent one of the best ways to detect intruders and other suspicious activity. If you’re ready to increase the security of your home or business, give us a call! At Bay Alarm, we’ve been protecting people just like you for over 75 years.

18.Explain light and gas sensor in IOT.

## **What are gas sensors?**

The human nose has natural sensors that detect over 1 trillion distinct odors. However, it is still not sufficient to label or identify gasses in the atmosphere. Devices such as gas sensors are required to identify and calculate the concentration of different gasses in a specified region.

They help detect toxic gasses and prevent mishaps due to them. Several types of gas sensors are based on the gas to be detected. The most common ones are useful for detecting oxygen, carbon dioxide, nitrogen, and methane.

CO2 sensors are helpful for various applications, including environmental monitoring, industrial safety, and security. A gas sensor is mainly used to detect multiple gasses in the atmosphere.

It is a device that responds to the concentration of gasses (in parts per million or ppm) in the environment where it is installed. The device works by creating a potential difference by altering the material's internal sensor's resistance.

The phenomenon is reflected by the output voltage, which, in turn, helps in detecting the concentration along with the type of gas. Now, a single sensor cannot detect all kinds of gasses. The material within the sensor determines the kind of gas it can detect.

These sensors are available as modules with differential comparators. The comparators may be industrial-grade depending upon their usage. Gas sensors can be configured for a specific gas concentration or a threshold value.

Its digital pin swings high when the gas concentration surpasses this level. The gas concentration may be determined using the analog pin. The sensing element of the sensors comprises a heater coil, electrode, gas sensing layer, tubular ceramic, and electrode line.

These sensors are usually vapor-sensitive polymers, semiconducting metal oxides, and other absorbent materials. These sensors are of six types based on the sensing element:

* Optical gas sensor
* Calorimetric gas sensor
* Acoustic-based gas sensor
* Electrochemical gas sensor
* Metal Oxide-based gas sensor
* Capacitance-based gas sensor

## **How do gas sensors detect gas?**

Gas detectors typically use the scaling system to detect harmful gasses. As a dangerous gas exceeds its base level and reaches the threshold limit of the scale, the alarm triggers. Combustible and toxic gasses are the main types that gas sensors detect.

Catalytic sensors can identify combustible gasses. As the concentration of gas at a place increases and it touches the catalytic surface, it causes a change in resistance and thus the alarm sounds off.

Furthermore, an infrared sensor, which is also a light detector, can identify the kind of gas if it travels into the light pathway between the transmitter and receiver. An infrared sensor also detects combustible materials.

Electrochemical sensors are primarily employed to find harmful gasses by producing signals on the electrode. The sensors are tremendously sensitive and are used explicitly for detecting carbon monoxide. These sensors come with a digital display to give the output.

Another method for identifying harmful gasses is metal oxide semiconductors. In this method, a sensitive film is used, which reacts with the toxic and explosive gasses when the threshold limit exceeds. Moreover, these sensors also work well in low humidity conditions.

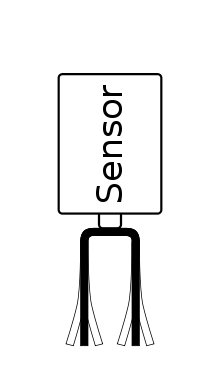
19.Explain level sensor in IOT.

**Level sensors** detect the [level of liquids](https://en.wikipedia.org/wiki/Liquid_level) and other [fluids](https://en.wikipedia.org/wiki/Fluids) and fluidized solids, including [slurries](https://en.wikipedia.org/wiki/Slurry), [granular](https://en.wikipedia.org/wiki/Granular) materials, and [powders](https://en.wiktionary.org/wiki/powders) that exhibit an upper [free surface](https://en.wikipedia.org/wiki/Free_surface). Substances that flow become essentially [horizontal](https://en.wikipedia.org/wiki/Horizontal_plane) in their containers (or other physical boundaries) because of [gravity](https://en.wikipedia.org/wiki/Gravity) whereas most bulk solids pile at an angle of repose to a peak. The substance to be measured can be inside a container or can be in its natural form (e.g., a river or a lake). The level measurement can be either continuous or point values. Continuous level sensors measure level within a specified range and determine the exact amount of substance in a certain place, while point-level sensors only indicate whether the substance is above or below the sensing point. Generally the latter detect levels that are excessively high or low.

There are many physical and application variables that affect the selection of the optimal level monitoring method for industrial and commercial processes.[[1]](https://en.wikipedia.org/wiki/Level_sensor#cite_note-1) The selection criteria include the physical: [phase](https://en.wikipedia.org/wiki/Phase_(matter)) (liquid, solid or slurry), [temperature](https://en.wikipedia.org/wiki/Temperature), [pressure](https://en.wikipedia.org/wiki/Pressure) or [vacuum](https://en.wikipedia.org/wiki/Vacuum), [chemistry](https://en.wikipedia.org/wiki/Chemistry), [dielectric constant](https://en.wikipedia.org/wiki/Dielectric_constant) of [medium](https://en.wikipedia.org/wiki/Transmission_medium), [density](https://en.wikipedia.org/wiki/Density) (specific gravity) of medium, [agitation (action)](https://en.wikipedia.org/wiki/Agitation_(action)), acoustical or electrical noise, [vibration](https://en.wikipedia.org/wiki/Vibration), [mechanical shock](https://en.wikipedia.org/wiki/Shock_(mechanics)), tank or bin size and shape. Also important are the application constraints: price, accuracy, appearance, response rate, ease of [calibration](https://en.wikipedia.org/wiki/Calibration) or [programming](https://en.wikipedia.org/wiki/Mathematical_programming), physical size and mounting of the instrument, monitoring or control of continuous or discrete (point) levels. In short, level sensors are one of the very important sensors and play very important role in a variety of consumer/ industrial applications. As with other types of sensors, level sensors are available or can be designed using a variety of sensing principles. Selection of an appropriate type of sensor suiting to the application requirement is very important.

A variety of sensors are available for point level detection of solids. These include vibrating, rotating paddle, mechanical ([diaphragm](https://en.wikipedia.org/wiki/Diaphragm_(mechanical_device))), [microwave](https://en.wikipedia.org/wiki/Microwave) ([radar](https://en.wikipedia.org/wiki/Radar)), capacitance, optical, pulsed-ultrasonic and [ultrasonic](https://en.wikipedia.org/wiki/Ultrasonic_sensor) level sensors.

### Vibrating point[[edit](https://en.wikipedia.org/w/index.php?title=Level_sensor&action=edit&section=2)]

[](https://en.wikipedia.org/wiki/File:Sensor_prinzip.svg)

Principle of vibration point probe

These detect levels of very fine powders (bulk density: 0.02–0.2 g/cm3), fine powders (bulk density: 0.2–0.5 g/cm3), and granular solids (bulk density: 0.5 g/cm3 or greater). With proper selection of vibration frequency and suitable sensitivity adjustments, they can also sense the level of highly fluidized powders and electrostatic materials.

Single-probe vibrating level sensors are ideal for bulk powder level. Since only one sensing element contacts the powder, bridging between two probe elements is eliminated and media build-up is minimized. The vibration of the probe tends to eliminate build-up of material on the probe element. Vibrating level sensors are not affected by dust, static charge build-up from dielectric powders, or changes in conductivity, temperature, pressure, humidity or moisture content. Tuning-fork style vibration sensors are another alternative. They tend to be less costly, but are prone to material buildup between the tines,

### Rotating paddle[[edit](https://en.wikipedia.org/w/index.php?title=Level_sensor&action=edit&section=3)]

Rotating paddle level sensors are a very old and established technique for bulk solid point level indication. The technique uses a low-speed gear motor that rotates a paddle wheel. When the paddle is stalled by solid materials, the motor is rotated on its shaft by its own torque until a flange mounted on the motor contacts a mechanical switch. The paddle can be constructed from a variety of materials, but tacky material must not be allowed to build up on the paddle. Build-up may occur if the process material becomes tacky because of high moisture levels or high ambient humidity in the hopper. For materials with very low weight per unit volume such as [Perlite](https://en.wikipedia.org/wiki/Perlite), [Bentonite](https://en.wikipedia.org/wiki/Bentonite) or [fly ash](https://en.wikipedia.org/wiki/Fly_ash), special paddle designs and low-torque motors are used. Fine particles or dust must be prevented from penetrating the shaft bearings and motor by proper placement of the paddle in the hopper or bin and using appropriate seals.

### Admittance-type[[edit](https://en.wikipedia.org/w/index.php?title=Level_sensor&action=edit&section=4)]

An RF admittance level sensor uses a rod probe and RF source to measure the change in [admittance](https://en.wikipedia.org/wiki/Admittance). The probe is driven through a shielded coaxial cable to eliminate the effects of changing cable capacitance to ground. When the level changes around the probe, a corresponding change in the dielectric is observed. This changes the admittance of this imperfect capacitor and this change is measured to detect change of level.[[2]](https://en.wikipedia.org/wiki/Level_sensor#cite_note-2)

**20.Explain ultrasonic sensor in IOT.**

* An ultrasonic sensor is an instrument that measures the distance to an object using ultrasonic sound waves.
* An ultrasonic sensor uses a transducer to send and receive ultrasonic pulses that relay back information about an object’s proximity.  High-frequency sound waves reflect from boundaries to produce distinct echo patterns.
* Ultrasonic sensing is one of the best ways to sense proximity and detect levels with high reliability.Our technical support gets emails all of the time about how our sensors work and what environments our sensors work (or don’t work) in.

**How Ultrasonic Sensors Work.**

* Ultrasonic sensors work by sending out a sound wave at a frequency above the range of human hearing.  The transducer of the sensor acts as a microphone to receive and send the ultrasonic sound. Our [ultrasonic sensors](https://www.maxbotix.com/SelectionGuide/Selection-Guide.htm), like many others, use a single transducer to send a pulse and to receive the echo.  The sensor determines the distance to a target by measuring time lapses between the sending and receiving of the ultrasonic pulse.

### Using Multiple Sensors & Avoiding Disruption

### When using multiple sensors in an application, it’s important to connect them in a way that will allow you to avoid issues like crosstalk or any other interference.

### prevent the disruption of the ultrasonic signals coming from your To sensor, it’s important to keep the face of the ultrasonic transducer clear of any obstructions.

Common obstructions include:

* Dirt
* Snow
* Ice
* Other Condensation

### How are Ultrasonic Sensors used?

### Our ultrasonic distance, level, and proximity sensors are commonly used with microcontroller platforms like Raspberry Pi, ARM, PIC, Arduino, Beagle Board, and more.

### Ultrasonic sensors transmit sound waves toward a target and will determine its distance by measuring the time it took for the reflected waves to return to the receiver.

### This sensor is an electronic device that will measure the distance of a target by transmitting ultrasonic sound waves, and then will convert the reflected sound into an electrical signal.

### Our sensors are often used as proximity sensors. Ultrasonic sensors are also used in obstacle avoidance systems, as well as in manufacturing.

### Our [Short Range sensors](https://www.maxbotix.com/product-category/hrlv-shortrange-ez-products) offer the opportunity for closer range detection where you may need a sensor that ranges objects as close to 2cm.  These are also built with very low power requirements in mind, as well as environments where noise rejection is necessary.

### When Not To Use an Ultrasonic Sensor

In some cases, the target object is so small that the reflected ultrasonic signal is insufficient for detection, and the distance cannot be measured correctly.

## Using Your Ultrasonic Sensor in Your Project

#### ****HOOK UP CONTROLLER****

#### We used an Arduino in this example, but you can use another controller and program of you

#### ****2. INSTALL SOFTWARE****

Install*Arduino Sketch* coding software onto your PC. This is where you type the code you want to compile and send to the Arduino board.

#### ****3. SET UP YOUR SENSOR WITH ARDUINO****

Plug your Arduino into the USB cable and into your computer. Once you upload Arduino, you can then compile and activate the code.

#### ****4. COMPILE AND RUN CODE****

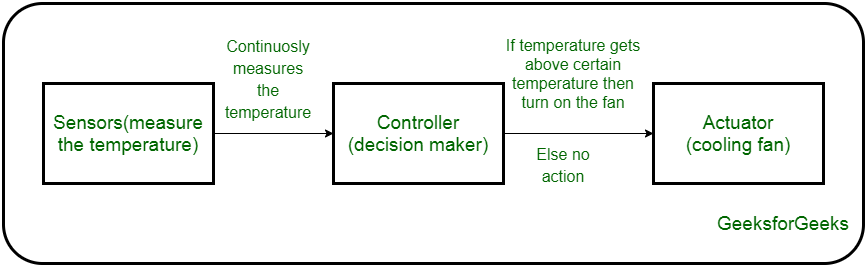
The code below will allow you to read distance in centimeters. Compile and run this code to obtain real-time distance measurements to the closest object. (Please note: this code is not only for Arduino and will run on most controllers)

21.Explain actuator sensor in IOT.

An [IoT](https://www.geeksforgeeks.org/introduction-to-internet-of-things-iot-set-1/) device is made up of a Physical object (“thing”) + Controller (“brain”) + [Sensors + Actuators](https://www.geeksforgeeks.org/difference-between-sensor-and-actuator/) + Networks (Internet). An actuator is a machine component or system that moves or controls the mechanism of the system. Sensors in the device sense the environment, then control signals are generated for the actuators according to the actions needed to perform.

A servo motor is an example of an actuator. They are linear or rotatory actuators, can move to a given specified angular or linear position. We can use servo motors for IoT applications and make the motor rotate to 90 degrees, 180 degrees, etc., as per our need.

The following diagram shows what actuators do, the controller directs the actuator based on the sensor data to do the work.



*Working of IoT devices and use of Actuators*

The control system acts upon an environment through the actuator. It requires a source of energy and a control signal. When it receives a control signal, it converts the source of energy to a mechanical operation. On this basis, on which form of energy it uses, it has different types given below.

**Types of Actuators :**

**1. Hydraulic Actuators –**

A hydraulic actuator uses hydraulic power to perform a mechanical operation. They are actuated by a cylinder or fluid motor. The mechanical motion is converted to rotary, linear, or oscillatory motion, according to the need of the IoT device. Ex- construction equipment uses hydraulic actuators because hydraulic actuators can generate a large amount of force.

**Advantages :**

* Hydraulic actuators can produce a large magnitude of force and high speed.
* Used in welding, clamping, etc.
* Used for lowering or raising the vehicles in car transport carriers.

**Disadvantages :**

* Hydraulic fluid leaks can cause efficiency loss and issues of cleaning.
* It is expensive.
* It requires noise reduction equipment, heat exchangers, and high maintenance systems.

**2. Pneumatic Actuators –**

A pneumatic actuator uses energy formed by vacuum or compressed air at high pressure to convert into either linear or rotary motion. Example- Used in robotics, use sensors that work like human fingers by using compressed air.

**Advantages :**

* They are a low-cost option and are used at extreme temperatures where using air is a safer option than chemicals.
* They need low maintenance, are durable, and have a long operational life.
* It is very quick in starting and stopping the motion.

**Disadvantages :**

* Loss of pressure can make it less efficient.
* The air compressor should be running continuously.
* Air can be polluted, and it needs maintenance.

**3. Electrical Actuators –**

An electric actuator uses electrical energy, is usually actuated by a motor that converts electrical energy into mechanical torque. An example of an electric actuator is a solenoid based electric bell.

**Advantages :**

* It has many applications in various industries as it can automate industrial valves.
* It produces less noise and is safe to use since there are no fluid leakages.
* It can be re-programmed and it provides the highest control precision positioning.

**Disadvantages :**

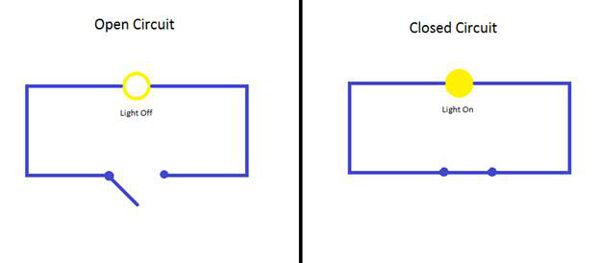
* It is expensive.
* It depends a lot on environmental conditions.

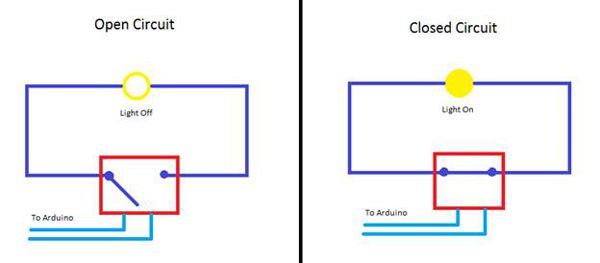
Other actuators are –

* **Thermal/Magnetic Actuators –**  
  These are actuated by thermal or mechanical energy. Shape Memory Alloys (SMAs) or Magnetic Shape‐Memory Alloys (MSMAs) are used by these actuators. An example of a thermal/magnetic actuator can be a piezo motor using SMA.
* **Mechanical Actuators –**   
  A mechanical actuator executes movement by converting rotary motion into linear motion. It involves pulleys, chains, gears, rails, and other devices to operate. Example – A crankshaft.
* Soft Actuators
* Shape Memory Polymers
* Light Activated Polymers
* With the expanding world of IoT, sensors and actuators will find more usage in commercial and domestic applications along with the pre-existing use in industry.

22.Explain relay switch sensor in IOT

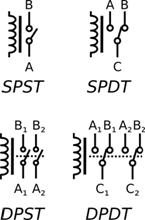
* wanted to turn on a lamp or open your garage door but didn’t know how to interface with it? It is easier than you think when you use relays! Relays allow you to control high-powered electronics with low-powered signals from devices such as Arduino or Raspberry Pi.
* Think of a relay as an electronic light switch. To turn the light on, flick the switch up. To turn the light off, flick the switch down. A light switch simply closes (or completes) an electrical circuit to turn on a light and opens (or breaks) a circuit to turn off the light. A relay does this same exact thing except that the switch is powered not by hand but by a low-power signal. There are different types of relays and they differ by the types of poles and throws, as explained in the following two diagrams.

  
**Figure 1:** Switch Diagram

  
**Figure 2:** Relay Diagram

## Pole and Throw

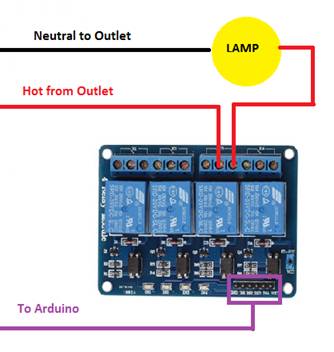
* Pole and throw refers to how many inputs and how many outputs there are, essentially. A common type of relay is called Single Pole Double Throw, written as “SPDT.” This means that there is one incoming path and two possible outgoing paths, depending on the low-level incoming signal. One of the paths is called the “normally closed” path; this means that, without power the circuit is closed. The other path is “normally open” meaning that, when no power is applied, the circuit is open. Figure 3 shows the different types of pole and throws available for relays.

  
**Figure 3:** Types of relay configurations

## Why Use Relays?

* The reason for using relays is simple. A device like an Arduino or Raspberry Pi cannot switch high-powered circuits like lamps or lights. These devices typically have 5v or 3v connections and have no other way to switch other circuits. Another use of relays is switching existing circuity in your house without changing too much: such as a sprinkler system. All the wiring is already run to a location for water sprinklers. Connect the existing power to the solenoid valve wires and use the relay and an Arduino to control your sprinklers. Very simple!
* Lets if we want to control a desk lamp from the cloud. Well, first we need an Arduino or Raspberry Pi. Secondly, you need a relay, as we have discussed. Our first choice is to go out and buy all the individual components to make a reliable relay circuit. This choice is perfectly fine if you are interested in learning everything about a relay circuit.
* The second choice is to buy a pre-made PCB board with all the circuity and relays built on, including screw-down terminals for all connections. This method is the best method for prototyping with relays because nothing is permanent and it is a lower cost.
* The Sainsmart 4-channel Relay Module is a small PCB board with four relays mounted on it with all the connections needed to control the relays. This board also includes an LED on it to display what relays are receiving power, essentially telling you which are switched “on.”

  
**Figure 4:** The SainSmart 4-channel Relay Module

  
**Figure 5:** Basic lamp circuit wiring diagram for the SainSmart 4-channel Relay Module

* There are six header pins required to control all four relays on the board. In order from left to right they are: GND, IN1, IN2, IN3, IN4, and VCC. To control one of the relays, at least three of those connections are needed: GND, IN3, and VCC. GRN stands for ground; this will be connected to the Arduino ground. VCC is for Positive power connection; 5v connection from the Arduino. The IN3 would connect to the Arduino pin you are using to control the device from; for this example, it would be connected to pin 8 on the Arduino. When the Arduino code sets the pin to “HIGH,” power will be applied and the relay module will “close” the circuit then turning on the lamp.

## Use Caution!

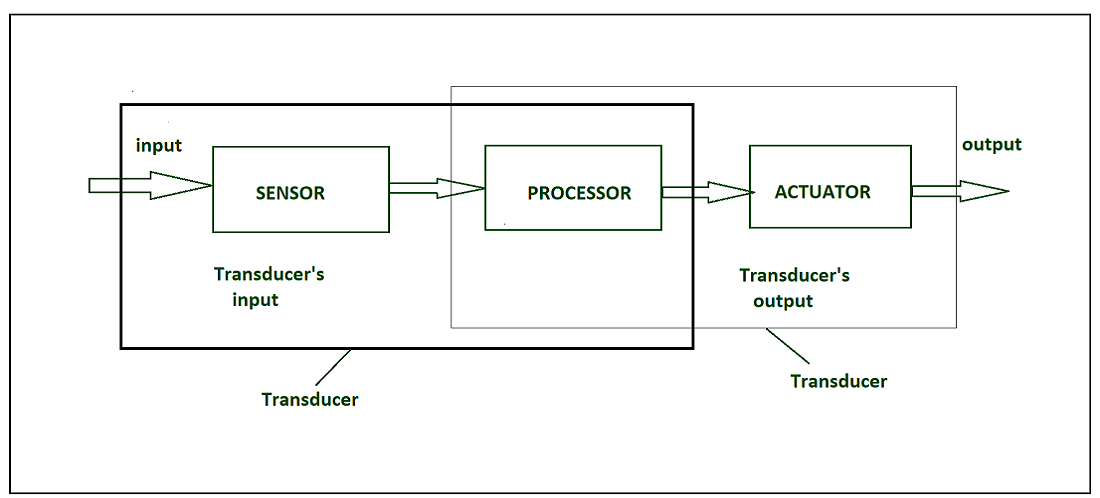
* When working with high power levels, use extreme caution. Never work with wiring that is live; always work with disconnected or powered-down circuits. If needed, turn off the circuit breaker and lock out the panel to prevent someone from accidentally turning it back on.
* Please be aware that there are solder points on the bottom of the relay modules that are in direct contact with the high power. You may have safely connected the power, but there are still connections that are not protected. With this in mind, do not work on metallic surfaces that may short circuit what you are working on.

## Conclusion

* Relays are simple devices that allow an easy way for logic-level power to control very high-powered devices. Adding some relays to items in your home can quickly automate an entire room full of lamps and lights and bring excitement to your Internet of Everything connected home!

23.Explain interface input output sensor in IOT.

Generally, sensors are used in the architecture of IOT devices.    
**Sensors** are used for sensing things and devices etc.  
A device that provides a usable output in response to a specified measurement.  
The sensor attains a physical parameter and converts it into a signal suitable for processing (e.g. electrical, mechanical, optical) the characteristics of any device or material to detect the presence of a particular physical quantity.  
The output of the sensor is a signal which is converted to a human-readable form like changes in characteristics, changes in resistance, capacitance, impedance etc.



*IOT HARDWARE*

**Transducer :**

* A transducer converts a signal from one physical structure to another.
* It converts one type of energy into another type.
* It might be used as actuators in various systems.

**Sensors characteristics :**

1. Static
2. Dynamic

**1. Static characteristics :**  
It is about how the output of a sensor changes in response to an input change after steady state condition.

* **Accuracy  –**  
  Accuracy is the capability of measuring instruments to give a result close to the true value of the measured quantity. It measures errors. It is measured by absolute and relative errors. Express the correctness of the output compared to a higher prior system. Absolute error = Measured value – True value  
  Relative error = Measured value/True value
* **Range –**  
  Gives the highest and the lowest value of the physical quantity within which the sensor can actually sense. Beyond these values, there is no sense or no kind of response.  
  e.g. RTD for measurement of temperature has a range of -200`c to 800`c.
* **Resolution –**  
  Resolution is an important specification towards selection of sensors. The higher the resolution, better the precision. When the accretion is zero to, it is called threshold.  
  Provide the smallest changes in the input that a sensor is able to sense.
* **Precision –**  
  It is the capacity of a measuring instrument to give the same reading when repetitively measuring the same quantity under the same prescribed conditions.  
  It implies agreement between successive readings, NOT closeness to the true value.  
  It is related to the variance of a set of measurements.  
  It is a necessary but not sufficient condition for accuracy.
* **Sensitivity –**  
  Sensitivity indicates the ratio of incremental change in the response of the system with respect to incremental change in input parameters. It can be found from the slope of the output characteristics curve of a sensor. It is the smallest amount of difference in quantity that will change the instrument’s reading.
* **Linearity –**  
  The deviation of the sensor value curve from a particular straight line. Linearity is determined by the calibration curve. The static calibration curve plots the output amplitude versus the input amplitude under static conditions.   
  A curve’s slope resemblance to a straight line describes the linearity.
* **Drift –**  
  The difference in the measurement of the sensor from a specific reading when kept at that value for a long period of time.
* **Repeatability –**  
  The deviation between measurements in a sequence under the same conditions. The measurements have to be made under a short enough time duration so as not to allow significant long-term drift.

**Dynamic Characteristics :**  
Properties of the systems

* **Zero-order system –**  
  The output shows a response to the input signal with no delay. It does not include energy-storing elements.  
  Ex. potentiometer measure, linear and rotary displacements.
* **First-order system –**  
  When the output approaches its final value gradually.  
  Consists of an energy storage and dissipation element.
* **Second-order system –**  
  Complex output response. The output response of the sensor oscillates before steady state.

**Sensor Classification :**

* Passive& Active
* Analog & digital
* Scalar & vector

1. **Passive Sensor –**  
   Can not independently sense the input. Ex- Accelerometer, soil moisture, water level and temperature sensors.
2. **Active Sensor –**  
   Independently sense the input. Example- Radar, sounder and laser altimeter sensors.
3. **Analog Sensor** **–**  
    The response or output of the sensor is some continuous function of its input parameter. Ex- Temperature sensor, LDR, analog pressure sensor and analog hall effect.
4. **Digital sensor –**  
   Response in binary nature. Design to overcome the disadvantages of analog sensors. Along with the analog sensor, it also comprises extra electronics for bit conversion. Example – Passive infrared (PIR) sensor and digital temperature sensor(DS1620).
5. **Scalar sensor –**   
   Detects the input parameter only based on its magnitude. The answer for the sensor is a function of magnitude of  some input parameter. Not affected by the direction of input parameters.  
   Example – temperature, gas, strain, color and smoke sensor.
6. **Vector sensor –**  
   The response of the sensor depends on the magnitude of the direction and orientation of input parameter. Example – Accelerometer, gyroscope, magnetic field and motion detector sensors.

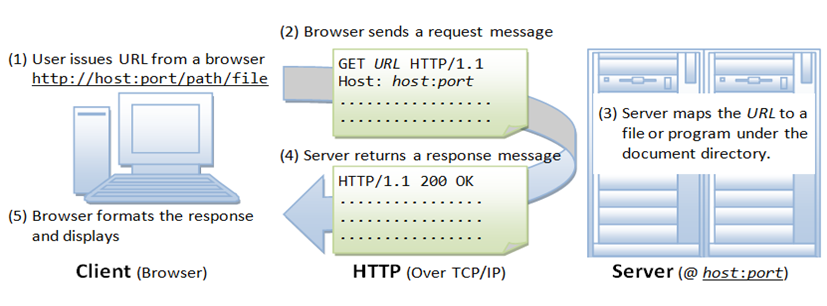
UNIT-3

1. Explain How Web Server use for IoT.

Any computer that can implement http or https is able to play the role of a web server. Http is a protocol, a way of communication which supplies web pages. It is pretty widely used and easy to implement. Through http you can transfer html and create simple user interfaces, it can implement Java Script and make more complicated web pages and it is available in most of the browsers. One of the great qualities of this protocol is that it replaced complicated and heavy displays with user friendly web pages.

How does it work? The browser sends a request to the server who searches the demanded page and returns it to the browser for the user. The request will consist of information about the kind of browser that is used, about the computer or about the document requested. It will have a method, a URL, a query string and the upload body in case you want data to be sent to the server.

The response will include the status, which tells the browser if the page was found or not (the errors among the 400s are about a not found page, 300 are redirections and 200s are confirmations of the page being found).Https has two important security roles.



* It encripts the data. The request and the response will be both encripted on sending and decripted when read.
* The server is always asked for a certificate of authenticity before it is asked for a page. This prevents against stolen data through false web pages.

What does a query consist of? It will always look like this: [http://address:[port]URL?querystring](http://address:[port]url/?querystring). The port can be absent, in which case it will be 80 for http and 443 for https. It has to be specified if it is not one the two. Concerning the URL, when it is not written, the default will be */*. The available methods in http are : get, post, put and delete. The main ones being the first two.

* Get method needs no upload body. It will only ask for data from the server and send only the headers, the address, the URL.
* Post sends important data to the server, which will be uploaded. Post has the role of modifying data on the server. The response of both these methods is the page and any additional information that was requested.
* Put is similar to post, only that in the semantic way, this method only creates an object on the server.
* Delete also plays a semantic part. It needs no upload body and it delets objects on the server. The same action can be performed however using get.

On one server there can be more than one websites, which means that, if the host is not specified in the request, the response may not be the one the browser expects.

Also, the response may have more than text. Any additional feature: images, JavaScript objects and so on will need a new request, so the process will be slowed down

2)Explain how sending/receiving data between web server and IoT device is take place.

When we talk about IoT devices, we are usually describing things like environmental sensors, connected appliances, vehicle trackers, or even assembly line machines. While an IoT device is arguably any electronic device that can communicate with the Internet, we usually don’t mean mobile phones or general use computers.  
   
Typically, we’re focused on devices with a narrower purpose, such as controlling the lights in your home or tracking tank levels for manufacturing chemicals. As an example, the following graphic shows the connectivity between an industrial tank sensor using a [Digi XBee® radio module](https://www.digi.com/xbee), communicating with a gateway that houses a [Digi ConnectCore® System on Module](https://www.digi.com/products/embedded-systems/system-on-modules) (SOM).

### Connecting Wireless Devices

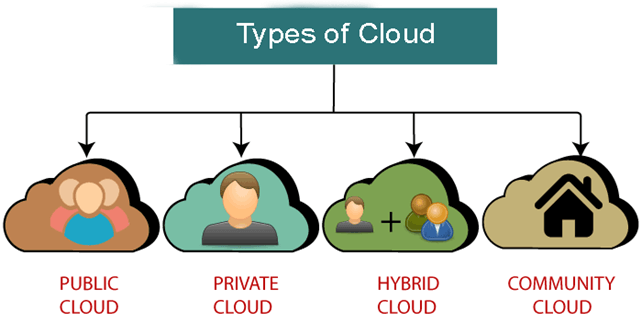
Many of these devices weren’t originally created with Internet capabilities and must be modified with after-market solutions to become connected. However, IoT capabilities are increasingly being designed right into new devices, where they can greatly lower costs and improve functionality.  
   
While IoT devices vary depending on the need they were created to fill, some fundamental components are almost always included. For example:

* There’s typically a sensor to detect physical occurrences, like motion or a water leak.
* There may also be actuators that create physical changes, like turning on a light or closing a valve.
* These sensors and actuators connect with one or more microprocessors running the logic that drives the IoT functionality.
* As a connected device, it must have at least one communication component, either some type of radio or a wired communication method like Ethernet.
* IoT devices are often battery-operated, making power management a key consideration when selecting equipment, designing functionality, and creating communications strategies.

All these components will be housed in some type of enclosure, often quite a small one. Depending on the environment, this enclosure may need to be sealed and watertight, or it may be heavily vented to manage heat. Because IoT devices are often deployed in very large quantities, getting the cost right is critical. Every penny counts when those pennies get multiplied into the millions.

3)Explain cloud use in IoT.

* An IoT cloud is a massive network that supports IoT devices and applications. This includes the underlying infrastructure, servers and storage, needed for real-time operations and processing. An IoT cloud also includes the services and standards necessary for connecting, managing, and securing different IoT devices and applications.
* IoT clouds offer an efficient, flexible, and scalable model for delivering the infrastructure and services needed to power IoT devices and applications for businesses with limited resources. IoT clouds offer on-demand, cost-efficient hyperscale so organizations can leverage the significant potential of IoT without having to build the underlying infrastructure and services from scratch.



Public Cloud

Public cloud is **open to all** to store and access information via the Internet using the pay-per-usage method.

* **Example:** Amazon elastic compute cloud (EC2), IBM SmartCloud Enterprise, Microsoft, Google App Engine, Windows Azure Services Platform.

## **Private Cloud**

Private cloud is also known as an **internal cloud** or **corporate cloud**. It is used by organizations to build and manage their own data centers internally or by the third party. It can be deployed using Opensource tools such as Openstack and Eucalyptus.

## **Hybrid Cloud**

Hybrid Cloud is a combination of the public cloud and the private cloud. we can say:

**Hybrid Cloud = Public Cloud + Private Cloud**

Hybrid cloud is partially secure because the services which are running on the public cloud can be accessed by anyone, while the services which are running on a private cloud can be accessed only by the organization's users.

**Example:** Google Application Suite (Gmail, Google Apps, and Google Drive), Office 365 (MS Office on the Web and One Drive), Amazon Web Services.

## **Community Cloud**

Community cloud allows systems and services to be accessible by a group of several organizations to share the information between the organization and a specific community. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.

**Example:** Health Care community cloud

4)write a short note on RED?

* Node RED is a programming language tool. It is used for wiring together hardware devices, online services and API’s .In other words we can say that Node RED is a visual wiring tool for IoT. Node RED offers a browser based editor.
* The editor easily wire together flows by using the broad range of nodes in the palette that can be deployed too its runtime in a single click.
* Node RED has following features:

1. Browser-based flow editing
2. Built on Node.js
3. Social Development
4. Browser-based flow editing

-Node RED provides a browser-based flow editor .The editor makes it easy to wire together flows using the bond range of nodes in the palette.

-Flows can be then deployed to runtime in a single-click.you can create JavaScript functions within the editor by using a rich text editor. It has built in library that permits you to save useful functions, templates or flows for re-use.

2.Built on Node.js

-The node RED permits the light-weight runtime is built on node.js. It takes the taking advantages of its event-driven, non-blocking model.

-It also makes it ideal to run at the edge of the network on low-cost hardware such as the Raspberry Pi as well as in the cloud.

-You can even extended the range of palette nodes to add new capabilities by using the over 225,000 modules in Node’s package repository.

3. Social Development

-You use JSON to store the flows created in Node.RED. You can import and export the flows very easily for sharing with others.

-There is an online flow library that permits you to share your best flows with the world.

5)Write difference between M2M and IoT Communication Protocols.

|  |  |
| --- | --- |
| **M2M** | **IoT** |
| Simple device-to-device communication usually within an embedded software at the client site. | Devices use IP networks to communicate. |
| Communication directly between machines. | IoT sensors automation. |
| Communication technology techniques and traditional protocols. | Internet protocols like HTTP, FTP and Telnet. |
| Observation of some degree of intelligence. | Objects are responsible for decision-making. |
| Hardware-based. | Hardware and Software-based. |
| Data sharing among communicating parties only. | Data sharing between other applications to improve the end-user experience. |
| Deployed in a closed system. | Connects to a larger network. |
| No open API support. | Supports open API integration. |
| Devices do not rely on internet connection. | An active internet connection is required. |

### Other Big Differences between IoT and M2M

The big difference between IoT and M2M is the connection. IoT is usually any device connected to the internet for enhanced performance. On the other hand, M2M is generally two or more devices connected with the internet for [data sharing and analytics](https://www.airtel.in/blog/business/iot-analytics-benefits-challenges-use-cases/).

IoT is premeditated to be scalable so that devices can be added to a network and integrated into existing systems. M2M networks can be more labour-intensive to set up and maintain since new point-to-point connections must be created for each device.

6)Write short note on Basics of WSNs.

**Wireless Sensor Network (WSN)** is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System.   
Base Station in a WSN System is connected through the Internet to share data.

WSN can be used for processing, analysis, storage, and mining of the data.

**Applications of WSN:** 

1. Internet of Things (IOT)
2. Surveillance and Monitoring for security, threat detection
3. Environmental temperature, humidity, and air pressure
4. Noise Level of the surrounding
5. Medical applications like patient monitoring
6. Agriculture
7. Landslide Detection

**Challenges of WSN:** 

1. Quality of Service
2. Security Issue
3. Energy Efficiency
4. Network Throughput
5. Performance
6. Ability to cope with node failure
7. Cross layer optimisation
8. Scalability to large scale of deployment

**Components of WSN:** 

1. **Sensors:**   
   Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.
2. **Radio Nodes:**   
   It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.
3. **WLAN Access Point:**   
   It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.
4. **Evaluation Software:**   
   The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

7)Write short note on WSNs architecture.

### 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 n/w, we require five layers, namely application, transport, n/w, data link & 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](https://www.elprocus.com/introduction-to-wireless-sensor-networks-types-and-applications/)

### 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: Layered Network Architecture, and Clustered Architecture. These are explained as following below.

* Layered Network Architecture
* Clustered Network Architecture

#### 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:

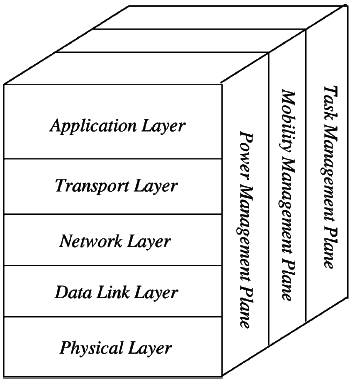
* Application Layer
* Transport Layer
* Network Layer
* Data Link Layer
* Physical Layer

The three cross layers include the following:

* Power Management Plane
* Mobility Management Plane
* 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.

Wireless Sensor Network Architecture



#### 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.

#### 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).

#### 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.

#### 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.

#### 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 & data encryption. IEEE 802.15.4 is suggested as typical for low rate particular areas & 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.

#### 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.

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.

8)Write short note on WSNs types.

There are five types of Wireless Sensor Networks depending on the environment. Different Types of WSNs are:

**1. Terrestrial Wireless Sensor Networks:**Terrestrial WSNs are used for communicating base stations efficiently, and comprise thousands of wireless sensor nodes deployed either in an unstructured (ad hoc) or structured (Pre-planned) manner.

In an unstructured mode (ad hoc), the sensor nodes are randomly distributed within the target area that’s dropped from a set plane.

In WSNs, the battery power is limited, however, the battery is provided with solar cells as a secondary power source. The conservation of energy of the WSNs gets by using low duty cycle operations, optimal routing, minimizing delays, and so on.

**2. Underground Wireless Sensor Networks:** In terms of deployment, maintenance, equipment cost considerations, and careful planning, underground wireless sensor networks are more expensive than terrestrial WSNs.

The Underground Wireless sensor networks UWSNs comprises several sensory nodes that are hidden in the ground to observe underground conditions.

 Additional sink nodes are located above the bottom to transfer information from the sensor nodes to the base station, These underground WSNs deployed into the ground are difficult to recharge.

The sensor battery nodes equipped with limited battery power are also difficult to recharge. Additionally, the underground environment makes wireless communication a challenge because of the high attenuation and signal loss level.

**3. Underwater Wireless Sensor Networks:** About more than 70% of the earth’s planet is occupied with water. These networks contain several sensor nodes and vehicles deployed underwater. Autonomous underwater devices and vehicles are used to collect data from these sensor nodes.

A challenge of underwater communication may be a long propagation delay, and bandwidth and sensor failures. Underwater, WSNs are equipped with a limited battery that can’t be recharged or replaced.

The difficulty of energy conservation for underwater WSNs involves the development of underwater communication and networking techniques.

**4. Multimedia Wireless Sensor Networks:** Multimedia wireless sensor networks are proposed to enable tracking and monitoring of events in the sort of multimedia, like video, imaging, and audio.

These networks contain low-cost sensor nodes equipped with cameras and microphones. These sensory nodes of Multimedia WSNs are interconnected together over a wireless connection for data retrieval, data compression, and correlation.

The challenges with the Multimedia WSNs include high bandwidth requirements, high energy consumption, processing, and compressing techniques. Additionally, multimedia contents need high bandwidth for the content to be delivered properly and easily.

**5. Mobile Wireless Sensor Networks MWSNs:**Mobile WSNs networks comprise a group of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes can also compute sense and communicate respectively.

Mobile wireless sensor networks are way more versatile than static sensor networks. The benefits of Mobile WSNs over Static WSNs include better and improved coverage, superior channel capacity, better energy efficiency, and so on.

9)Explain IoT applications used in the areas of transportation.

IoT in transportation incorporates a wide network of embedded sensors, actuators, smart objects and other intelligent devices. This network collects data about the real-world scenario and transmits it over the specialized software to transform that data into useful information.

## 1. Efficient Traffic Management

Traffic management is the biggest segment within the transportation industry where the adoption of IoT technologies is observed to be the most prominent. Million and Billions of Gigabytes of traffic and vehicle-related data are being generated through CCTV cameras. This data is transferred to traffic management centers for keeping a closer look at the vehicles and punishing the car owners who are violating the traffic rules and regulations. Smart parking, automatic traffic light system and smart accident assistance are the few applications of IoT that help the traffic and patrolling officers in managing the traffic efficiently and reducing the risk of accidents.

## 2. Automated Toll and Ticketing

The traditional tolling and ticketing systems are not only becoming outdated but they are also not proving to be effective for assisting the current flow of vehicles on the road. With the increased number of vehicles on the road, the toll booths have become busy and crowded as well on the highways and the drivers have to spend a lot of time waiting for their turn. The toll booths do not have enough resources and manpower to immediately assist many vehicles. Compared to traditional tolling and ticketing systems, IoT in transportation offers automated tolls. With the help of RFID tags and other smart sensors, managing toll and ticketing have become much easier for traffic police officers.

The majority of advanced vehicles nowadays have IoT connectivity..

## 3. Self-driving Cars

Self-driving cars or autonomous vehicles are the coolest things that have been introduced in the transportation industry. In the past decades, the concept of self-driving cars was just like a dream, but this has been turned into an innovative reality with the support of IoT technologies. Self-driving cars are capable of moving safely by sensing the environment, with little or no human interaction. However, to gather data about the surrounding, self-driving cars use a wide range of sensors. For instance, the self-driving car uses acoustic sensors, ultrasonic sensors, radar, LiDAR (Light detection and ranging), camera and GPS sensors to have information about the surroundings and take the data-driven decision about mobility accordingly. This indicates that the functioning of self-driving cars is dependent on IoT sensors.

## 4. Advanced Vehicle Tracking or Transportation Monitoring

Vehicle tracking or transportation monitoring systems have become the need of many businesses to manage their fleets and supply chain processes effectively. With the help of GPS trackers, transportation companies have smooth access to real-time location, facts and figures about the vehicle. This enables the transportation companies to monitor their important assets in real-time. Apart from location monitoring, IoT devices can also monitor the driver’s behavior and can inform about the driving style and idling time. In fleet management systems, IoT has minimized the operating and fuel expenditures along with the cost of maintenance. As far as transportation monitoring is concerned, then it can be said that real-time tracking has made the implementation of smart decisions much easier, enabling the drivers to identify the issues in the vehicle immediately and take precautions where necessary.

## 5. Enhanced Security of the Public Transport

One of the key areas in which the IoT in transportation is found to be the most useful is focused on the security of public transport. By keeping an eye on every transport with the help of IoT devices, municipalities can track traffic violations and take appropriate actions. Apart from security, IoT in transportation also complements public transport management by providing a wide range of smart solutions. This includes advanced vehicle logistic solutions, passenger information systems, automated fare collection and integrated ticketing. These solutions help in managing public transport and traffic congestion. Real-time management of public transport has become possible with IoT. This has facilitated the transportation agencies to establish better communication with the passengers and provide necessary information through passenger information displays and mobile devices. IoT has undoubtedly made public transport more secure and efficient.

10)Explain IoT applications used in the areas of transportation agriculture.

Smart farming is a capital-intensive and hi-tech method of **growing food cleanly and sustainably**. We can also call it the application of**ICT (Information and Communication Technology)**in Agriculture.

IoT-based smart farming is also beneficial in terms of environmental issues. It can help the farmers to efficiently use water, optimize the inputs and treatments.

Now, having understood the concept of smart farming, we will look at the**major applications of IoT-based smart farming that are revolutionizing the agriculture sector.**

### ****1. Precision Farming****

Precision farming, also known as precision agriculture, is anything that makes the whole process of farming accurate and controlled when it comes to raising livestock and growing crops.

 The key component of this farming technique is the use of Information Technology and various other technologies like sensors, robotics, automation vehicles, control systems, automated hardware, variable rate technology, and so on.

 The key characteristic of precision farming is the adoption of access to high-speed internet, mobile devices, and reliable, low-cost satellites (for imagery and positioning) by manufacturers.

 Precision farming is considered one of the most famous applications of IoT in the agricultural sector and it is being leveraged globally by several organizations. One of the examples is [CropMetrics](https://cropmetrics.com/). It is a precision agriculture organization that focuses on ultra-modern agronomic solutions. Moreover, it specializes in the management of precision irrigation.

### ****2. Agricultural Drones****

Technology has progressed significantly and at a higher rate in the past few years. Agricultural drones are a prime example of this development. Drones are being used in the agricultural sector to enhance many farming practices.

The two types of drones- ground-based and aerial-based drones are being used in agriculture for crop health assessment, crop monitoring, spraying pesticides, irrigation, planting, and analyzing the field. These drones capture multispectral, thermal, and visual imagery during their flight.

The use of drones offers many benefits such as crop health imaging, integrated GIS mapping, saving time, ease of use, and also increasing crop yields. When we combine drone technology with proper strategy and planning based on real-time data collection, we can give a high-tech makeover to the agricultural sector.

### ****3. Livestock Monitoring****

Owners of large farms utilize wireless IoT applications to track the location, health, and well-being of their cattle. This information helps them to identify sick animals and henceforth separate them from the herd, take care of them, and also curb the spread of the disease among other animals. It is also useful for cutting labor costs as owners can locate their cattle with the help of IoT-based sensors.

[JMB North America](http://cowmonitor.com/) is an association that offers cow checking answers for cow makers. One of the arrangements helps the cow proprietors notice cows that are pregnant and going to conceive offspring. From the calf, a sensor fueled by a battery is removed when its water breaks. This sends data to the owner or the farmer. In the time spent with the cattle giving birth, sensors allow the farmers to be more focused.

### ****4. Smart Greenhouses****

Greenhouse farming is concerned with increasing the yields of vegetables, crops, fruits etc. Greenhouses control the environmental factors through manual intervention or a proportional control mechanism. However, manual intervention leads to production loss, energy loss, and labor costs. This makes the whole concept of greenhouses ineffective. So, smart greenhouses are a better alternative. A smart greenhouse can be created with the help of IoT. These smart greenhouses intelligently monitor and control the climate without requiring any sort of manual intervention.

Different kinds of sensors are used in a smart greenhouse that measure the environmental factors and assess their suitability for plants. A remote access is created by connecting the system to a cloud with the help of IoT. This eliminates the need for constant manual monitoring. The cloud server controls the data processing and applies a control action inside the greenhouse.

**The IoT sensors installed inside the greenhouse provide crucial information on temperature, humidity, pressure, and light levels.**These sensors control everything from turning on the lights and opening a window to controlling temperature and cooling off, all through a WiFi signal.

### ****5. Monitor Climate Conditions****

Climate plays an important role in crop production. Different crops require different climate conditions to grow and any little knowledge about climate heavily deteriorates the quantity and quality of crop production. IoT solutions enable the farmers to know real-time weather conditions.

The sensors placed in the agricultural fields collect data from the environment that is used by farmers to choose a crop that can grow in particular climatic conditions.

The whole IoT ecosystem is made up of sensors that detect real-time weather conditions like humidity, rainfall, temperature, all very crucial for crop production. These sensors are able to foresee any drastic change in the climatic conditions that can affect the production. An alert is sent to the server about the change in climate which helps to eliminate the need for physical presence. This ultimately leads to higher yields.

### ****6. Remote sensing****

IoT based remote sensing makes use of sensors placed along the farms such as weather stations for accumulating data that is carried forward to analytical tools for analysis. The crops can be monitored by farmers via analytical dashboards and action can be taken from the insights derived accordingly.

* **Crop Assessment**  
  These sensors placed in different corners of the farms assess the crops to keep track of any alterations in the shape, size, light, humidity and temperature.  Any deviation noted by the sensors is assessed and the farmer is informed. As a result, remote sensing aids in preventing disease spreads as well as in keeping track of the advancement of crops.

* **Weather conditions**  
  The data garnered by sensors in the case of temperature, humidity, moisture precipitation and dew detection aids in concluding the weather pattern in farms so that the cultivation is executed for appropriate crops.

* **Soil quality**

The analysis of soil quality aids in deciding on the nutrient value and parched sections of farms, soil drainage capacity or acidity, that permits to adjust the level of water required for irrigation and the select an advantageous type of cultivation.

### ****7. Computer imaging****

This form of imaging mainly involves using the sensor cameras that are placed in various corners of the farm to generate images that go through digital image processing.

* **Quality control**

Image processing combined with machine learning makes use of images from the database to compare with images of crops for concluding the size, shape, color, and growth, as a result, adjusting the quality.

* **Sorting and grading**

Computer imaging can aid in sorting and grading the produce on the basis of the color, shape and size.

* **Irrigation Monitoring**

Irrigation over a period of time helps in mapping of irrigated lands. This helps in taking the decision in the pre harvest season of harvesting or not harvesting.

11) Explain IoT applications used in the areas of transportation health care.

* Healthcare Applications

-IoT helps in healthcare to enhance the existing technology. It helps to get the data collection of real world cases.

-It helps to improve the accuracy of medical care delivery via more sophisticated integration of the healthcare system.

Research

-Iot opens ups the door to the valuable information for the research through real-time field data, analysis, and testing.

-IoT can send relevant data superior to standard analytics from side to side integrated instruments capable of performing viable research.

-It has integrates into actual practice to offer more key information.

-This helps in healthcare by offering more reliable and practical data, and better leads; which yields better solutions and finding of previously unknown issues.

Devices

-IoT offers the new better medical device solutions. IoT fills gaps between equipment and the way we deliver healthcare by creating a logical system rather than a collection of tools.

-It then tells patterns and missing data in healthcare like obvious necessary improvements or huge flaws.

Care

-IoT offers actual practice of medicine because it empowers healthcare professionals to better use their training and knowledge to solve problems.

-Their organizational decisions also improve because technology provides a better vantage point.

Medical Information Distribution

-Distributing of accurate and current information to patients is a big challenge in medical care.

-IoT devices not only improve facilities and professional practice, but also health in the daily lives of individuals.

-IoT devices give direct,24/7 access to the patient in a less intrusive way than other options. They take healthcare out of facilities and into the home, office, or social space.

Emergency Care

-IoT provides more powerful emergency support services, which suffer from their limited resources and disconnect with the base facility.

-It provides a way to analyze an emergency in a more complete way from miles away. It also gives more provides access to the patient prior to their arrival.

-This reduces the associated losses, and improves emergency healthcare.

12)Explain Edge computing purpose and definition of IoT

1. Explain Edge computing use cases.

**ANS:** Putting compute at the edge allows companies to improve how they manage and use physical assets and create new interactive, human experiences. Some examples of edge use cases include self- driving cars, autonomous robots, smart equipment data and automated retail.

* 1. Autonomous vehicles

Autonomous platooning of truck convoys will likely be one of the first use cases for autonomous vehicles. Here, a group of truck travelclose behind one another in a convoy, saving fuel costs and decreasing congestion. With edge computing, it will be possible to remove the need for drivers in all trucks except the front one, because the trucks will be able to communicate with each other withultra-low latency.

* 1. Remote monitoring of assets in the oil and gas industry

Oil and gas failures can be disastrous. Their assets therefore need tobe carefully monitored.

However, oil and gas plants are often in remote locations. Edge computing enables real-time analytics with processing much closerto the asset, meaning there is less reliance on good quality connectivity to a centralised cloud.

* 1. Smart grid

Edge computing will be a core technology in more widespread adoption of smart grids and can help allow enterprises to better manage their energy consumption Sensors and IoT devices connected to an edge platform in factories, plants and offices are being used to monitor energy use and analyse their consumption in real-time. With real-time visibility, enterprises and energy companies can strike new deals, for example where high- powered machinery is run during off-peak times for electricity demand. This can increase the amount of green energy (like wind power) an enterprise consumes.

* 1. Predictive maintenance

Manufacturers want to be able to analyse and detect changes in their production lines before a failure occurs.

Edge computing helps by bringing the processing and storage of data closer to the equipment. This enables IoT sensors to monitor machine health with low latencies and perform analytics in real-time.

* 1. In-hospital patient monitoring

Healthcare contains several edge opportunities. Currently, monitoring devices (e.g. glucose monitors, health tools and other sensors) are either not connected, or where they are, large amounts of unprocessed data from devices would need to be stored on a 3rd party cloud. This presents security concerns for healthcare providers.

An edge on the hospital site could process data locally to maintain data privacy. Edge also enables right-time notifications to practitioners of unusual patient trends or behaviours (through analytics/AI), and creation of 360-degree view patient dashboards for full visibility.

Submit your edge company and use case

* 1. Virtualised radio networks and 5G (vRAN)

Operators are increasingly looking to virtualise parts of their mobile

networks (vRAN). This has both cost and flexibility benefits. The new virtualised RAN hardware needs to do complex processing with a low

latency. Operators will therefore need edge servers to support virtualising their RAN close to the cell tower.

* 1. Cloud gaming

Cloud gaming, a new kind of gaming which streams a live feed of the game directly to devices, (the game itself is processed and hosted in data centres) is highly dependent on latency.

Cloud gaming companies are looking to build edge servers as close to gamers as possible in order to reduce latency and provide a fully responsive and immersive gaming experience.

* 1. Content delivery

By caching content – e.g. music, video stream, web pages – at the edge, improvements to content deliver can be greatly improved. Latency can be reduced significantly. Content providers are looking to distribute CDNs even more widely to the edge, thus guaranteeing flexibility and customisation on the network depending on user traffic demands.

* 1. Traffic management

Edge computing can enable more effective city traffic management. Examples of this include optimising bus frequency given fluctuations in demand, managing the opening and closing of extra lanes, and, in future, managing autonomous car flows.

With edge computing, there is no need to transport large volumes of traffic data to the centralised cloud, thus reducing the cost of bandwidth and latency.

* 1. Smart homes

Smart homes rely on IoT devices collecting and processing data from around the house. Often this data is sent to a centralised remote server, where it is processed and stored. However, this existing

architecture has problems around backhaul cost, latency, and security.

By using edge compute and bringing the processing and storage closer to the smart home, backhaul and roundtrip time is reduced, and sensitive information can be processed at the edge. As an example, the time taken for voice-based assistant devices such as Amazon’s Alexa to respond would be much faster

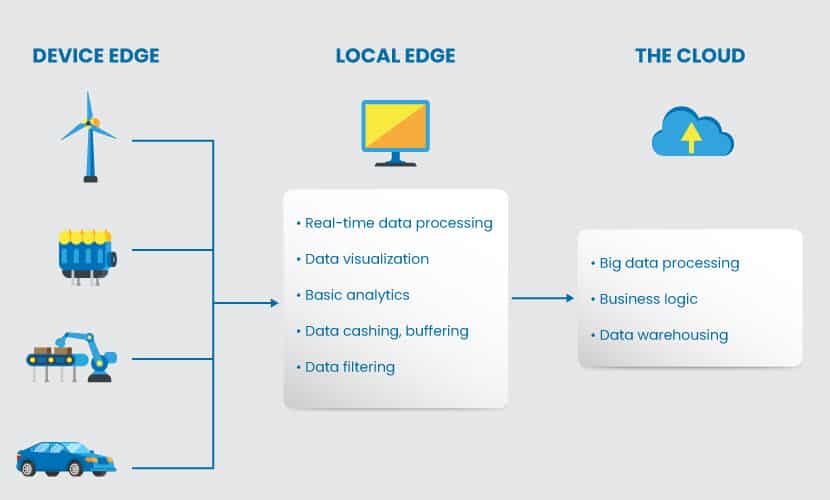
1. Explain Edge computing hardware architectures ANS:

**Edge Computing Architecture Explained**

Here are the key components that form an edge ecosystem:

* **Edge devices:** A special-purpose piece of equipment with limited computing capacity.
* **Edge node:** Any device, server, or [gateway](https://phoenixnap.com/glossary/what-is-gateway) that performs edge computing.
* **Edge server:** A computer located in a facility close to the edge device. These machines run application workloads and shared services, so they need more computing power than edge devices.
* **Edge gateway:** An edge server that performs network functions such as tunneling, [firewall](https://phoenixnap.com/blog/types-of-firewalls) management, protocol translation, and wireless connections. A gateway can also host application workloads.
* **Cloud:** A [public or private cloud](https://phoenixnap.com/blog/public-vs-private-cloud) that acts as a repository for containerized workloads like applications and machine learning models. The cloud also hosts and runs apps that manage edge nodes.

Edge computing has three primary nodes: **the device edge, local edge, and the cloud**.



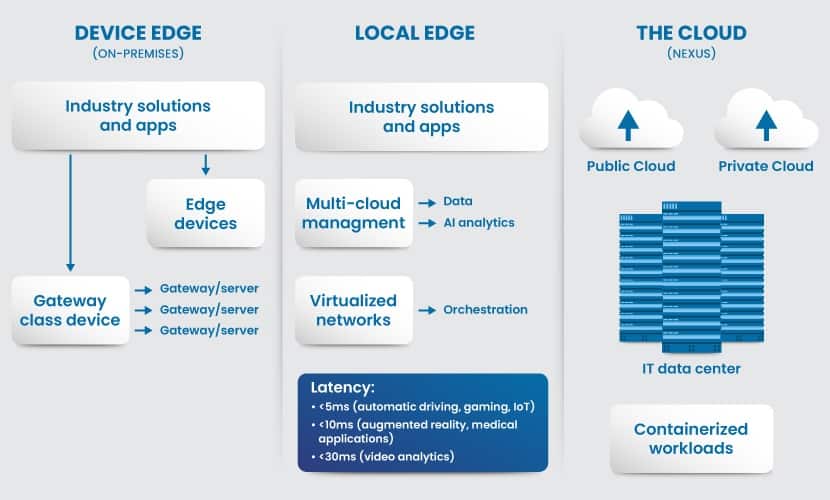
Device edge is the physical location of where edge devices run on-premises (cameras, sensors, industrial machines, etc.). These devices have the processing power to gather and transmit data.

Local edge is a system that supports the applications and the network workloads. The local edge has two layers:

* An application layer that runs apps edge devices cannot handle due to a large footprint (complex video analytics or IoT processing, for example).
* The network layer that runs physical or virtualized network components such as routers and switches.

The cloud (or **the nexus**) runs application and network workloads that manage the processing other edge nodes cannot handle. Despite the name, this edge layer can run either as an in-house data center or in the cloud.

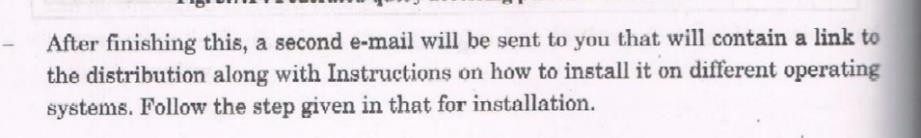
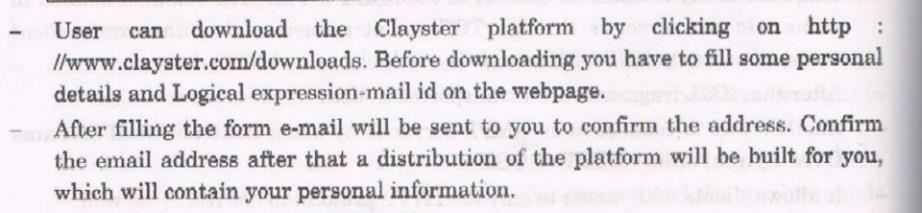
The illustration below presents a more detailed architecture and shows components relevant to each edge node.

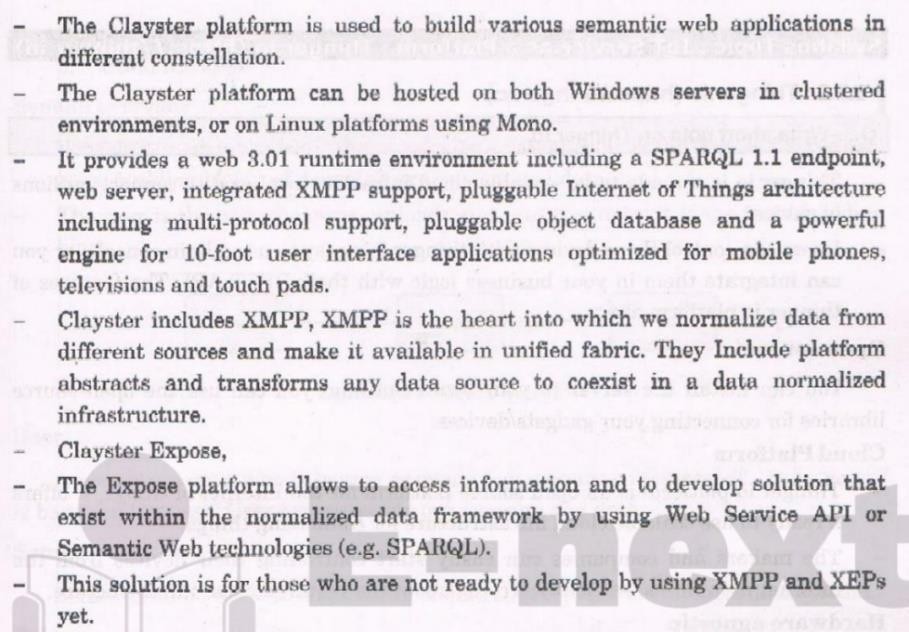


Industry solutions and applications can exist in multiple nodes as specific workloads are more suitable to either the device or local edge. Some other workloads can also dynamically move between nodes under certain circumstances (either manually or automatically).

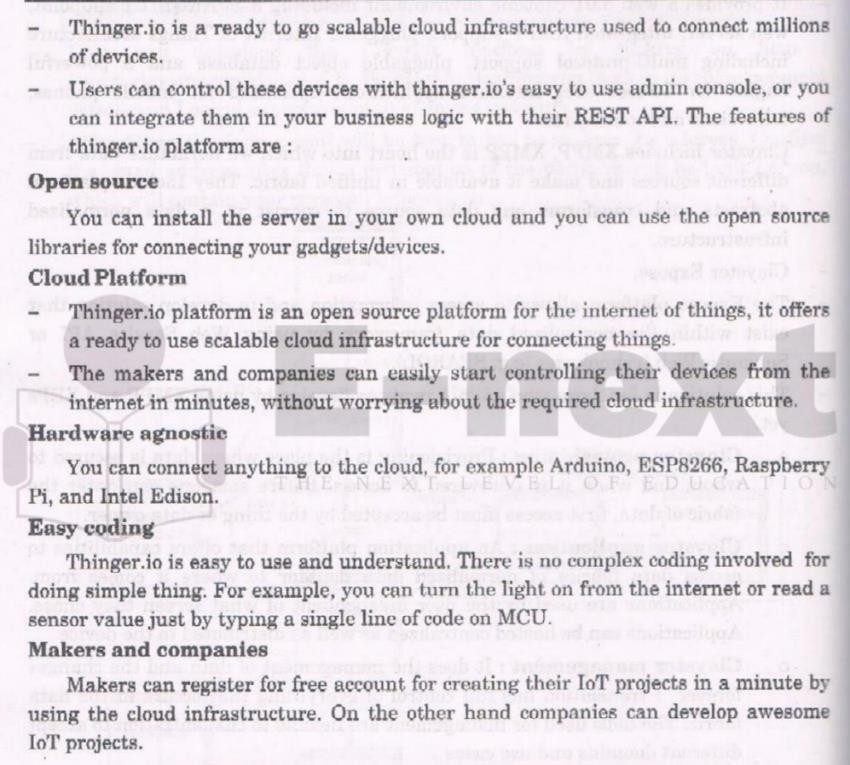
Virtualization is a vital element of a large-scale edge computing setup. This technology makes it easier to deploy and run numerous applications on edge servers.

1. **Explain Edge platforms. ANS:**
2. Clayster

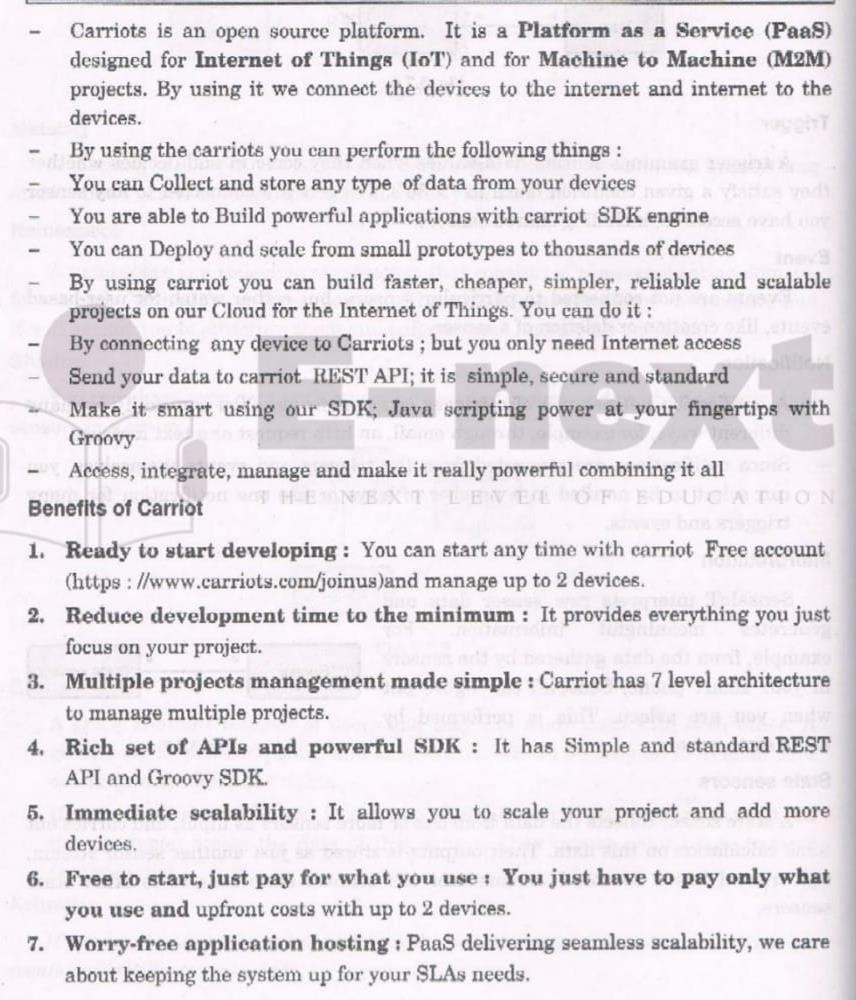




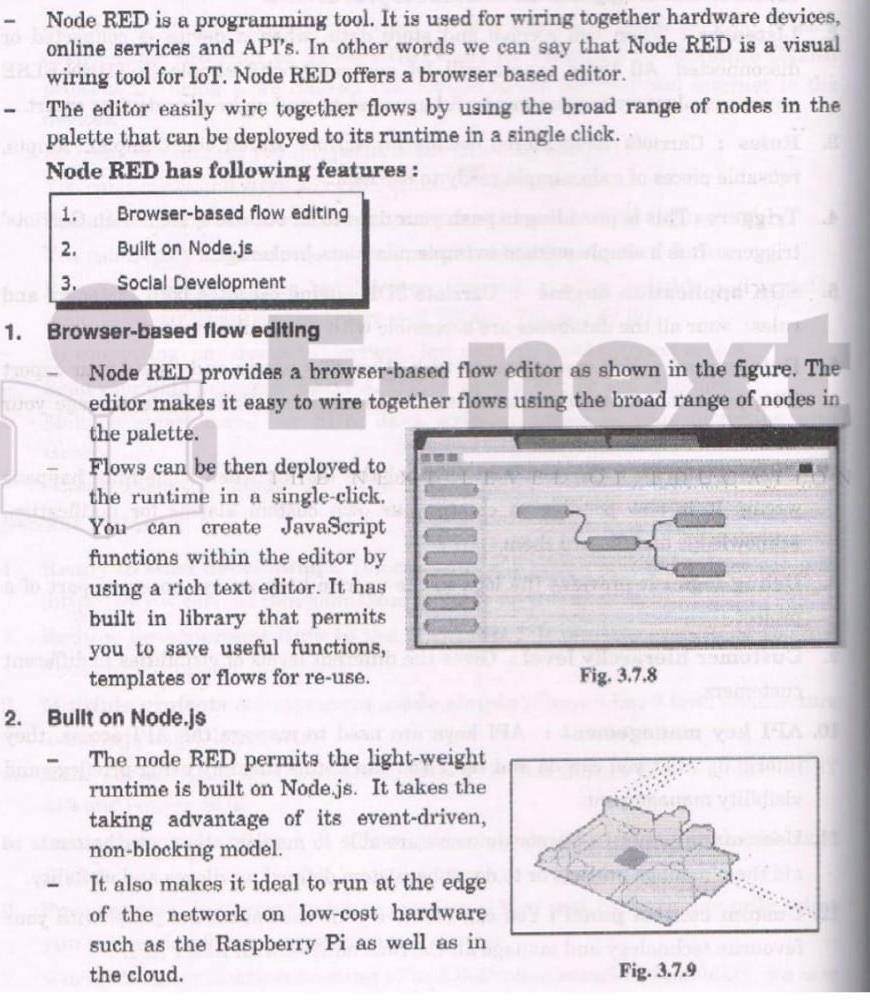
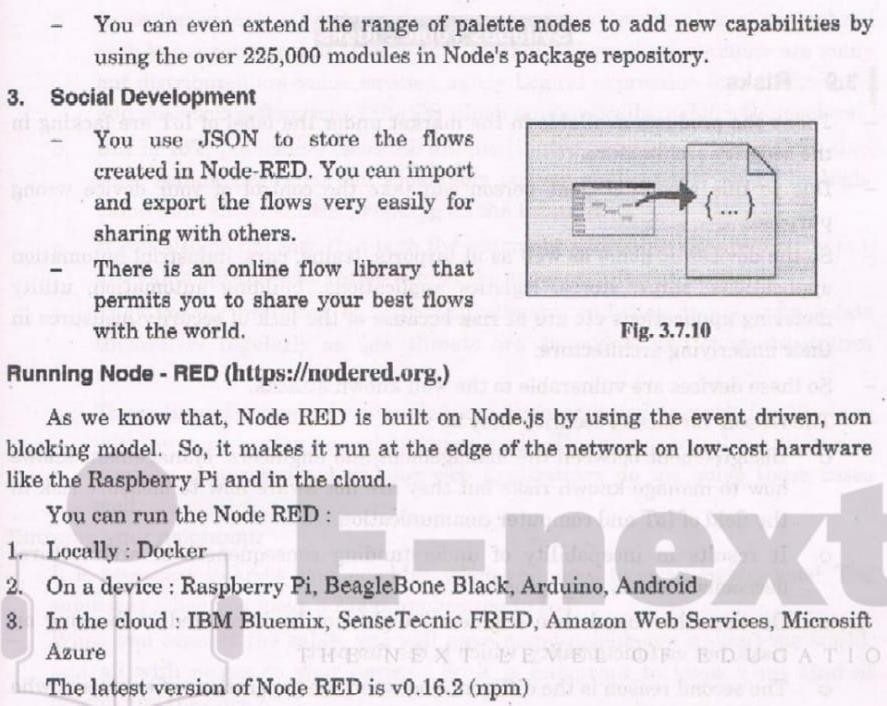
1. **Thinger**



1. Carriots



1. **Node RED**



1. Write difference between Edge and Fog Computing. ANS:

|  |  |  |
| --- | --- | --- |
| **S.NO.** | **EDGE COMPUTING** | **FOG COMPUTING** |
| 01. | Less scalable than fog computing. | Highly scalable when compared to edge computing. |
| 02. | Billions of nodes are present. | Millions of nodes are present. |
| 03. | Nodes are installed far away from the cloud. | Nodes in this computing are installed closer to the cloud(remote database where data is stored). |
| 04. | Edge computing is a subdivision of fog computing. | Fog computing is a subdivision of cloud computing. |
| 05. | The bandwidth requirement is very low. Because data comes from the edge nodes themselves. | The bandwidth requirement is high. Data originating from edge nodes is transferred to the cloud. |
| 06. | Operational cost is higher. | Operational cost is comparatively lower. |
| 07. | High privacy. Attacks on data are very low. | The probability of data attacks is higher. |
| 08. | Edge devices are the inclusion of the IoT devices or client’s network. | Fog is an extended layer of cloud. |
| 09. | The power consumption of nodes is low. | The power consumption of nodes filter important information from the massive amount of data collected from the device and saves it in the filter high. |
| 10. | Edge computing helps devices to get faster results | Fog computing helps in filtering important information from the |

|  |  |  |
| --- | --- | --- |
| **S.NO.** | **EDGE COMPUTING** | **FOG COMPUTING** |
|  | by processing the data simultaneously received from the devices. | massive amount of data collected from the device and saves it in the cloud by sending the filtered data. |

1. **Explain Communication Models -Edge**

**ANS:** In edge computing parlance, when we say model, it loosely refers to machine learning models that are created and trained in the cloud or in a data center and deployed onto the edge devices. An ML model is improved and kept updated through a cycle of continuous re-training and deployment.

Enhanced Data rates for GSM Evolution (EDGE) also known as Enhanced GPRS (EGPRS), IMT Single Carrier (IMT-SC), or Enhanced Data rates for Global Evolution) is a digital mobile phone technology that allows improved data transmission rates as a backward- compatible extension of GSM.

The three models of communication we will discuss are the transmission, interaction, and transaction models.

Although these models of communication differ, they contain some common elements. The first two models we will discuss, the transmission model and the interaction model, include the following parts: participants, messages, encoding, decoding, and channels.

Linear model of communication:

The linear or transmission model of communication. describes communication as a linear, one-way process in which a sender intentionally transmits a message to a receiver (Ellis & McClintock, 1990). This model focuses on the sender and message within a communication encounter. Although the receiver is included in the

model, this role is viewed as more of a target or end point rather than part of an ongoing process.

Interactive model of communication:

The interactive or interaction model of communication. describes communication as a process in which participants alternate positions as sender and receiver and generate meaning by sending messages and receiving feedback within physical and psychological contexts.

Transaction model of communication:

As the study of communication progressed, models expanded to account for more of the communication process. Many scholars view communication as more than a process that is used to carry on conversations and convey meaning. We don’t send messages like

computers, and we don’t neatly alternate between the roles of

sender and receiver as an interaction unfolds.

1. Explain Communication Models Fog

**ANS:** Fog computing or fog networking, also known as fogging, is an architecture that uses edge devices to carry out a substantial amount of computation (edge computing), storage, and communication locally and routed over the Internet backbone.

The term fog computing is also referred to as “edge computing,” which essentially means that rather than hosting and working from a centralized cloud, fog systems operate on network ends. That concentration means that data can be processed locally in smart devices rather than being sent to the cloud for processing. It’s one approach to dealing with the Internet of Things (IoT).

Fog computing, like many IT developments, grew out of the need to address a couple of growing concerns: being able to act in real time to incoming data and working within the limits of available

bandwidth. Today’s sensors are generating 2 exabytes of data. It’s too much data to send to the cloud. There’s not enough bandwidth, and it costs too much money. Fog computing places some of transactions and resources at the edge of the cloud, rather than establishing channels for cloud storage and utilization, it reduces the need for bandwidth by not sending every bit of information over cloud channels, and instead aggregating it at certain access points.

By using this kind of distributed strategy, we can lower costs and improve efficiencies.

Fog Computing extends the cloud computing paradigm to the edge of the network to address applications and services that do not fit the paradigm of the cloud including:

1.Applications that require very low and predictable latency 2.Geographically distributed applications

1. Fast mobile applications
2. Large-scale distributed control systems (smart grid, connected rail, smart traffic light systems)
3. Explain Communication Models M2M.

**ANS:** M2M stands for Machine to Machine communication. It is a direct communication system between the devices using wired or wireless communications channels without any human interaction. It collects the data and shares it with other connected devices. It is a technology that allows devices without the use of the internet to connect between devices. Various applications, such as defense, monitoring and tracking, production and facility management, are provided by M2M communications.

M2M technology may be present in offices, shopping malls, houses, and many other places. A common example of a machine to machine

is controlling electrical devices like fans and bulbs using Bluetooth from the smartphone. Here, the smartphone and electrical devices are the two interacting devices with each other. This is commonly known as Machine to machine communication. It is a concept where two or more than two machines communicate with each other without human interaction using a wired or wireless mechanism.

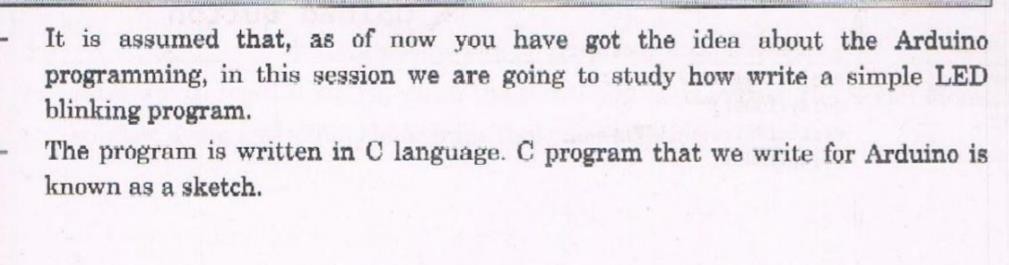
M2M is an technology that helps the devices to connect between devices without using internet. M2M communications offer several applications such as security, tracking and tracing, manufacturing and facility management.

M2M is also named as Machine Type Communication (MTC) in 3GPP ( 3rd Generation Partnership Project).

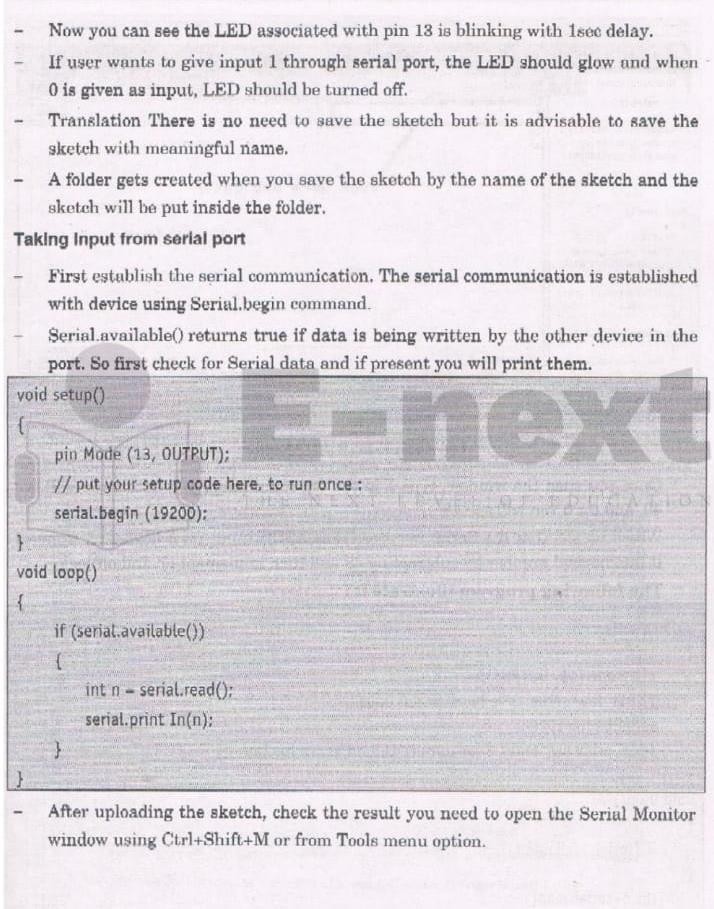
M2M is communication could carried over mobile networks, for ex- GSM-GPRS, CDMA EVDO Networks .

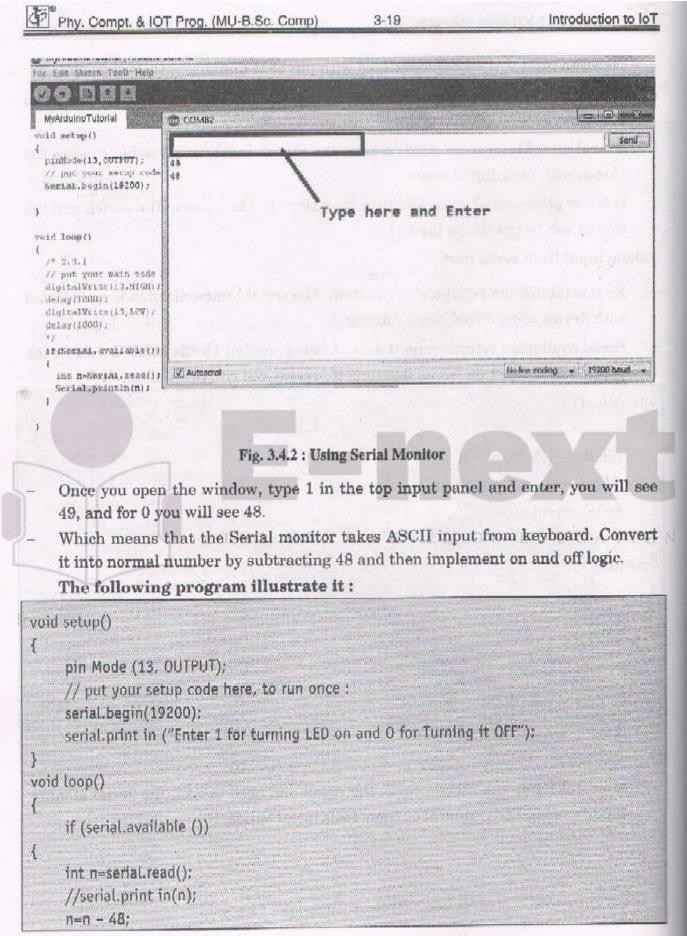
In M2M communication, the role of mobile networks is largely confined to server as a transport networks.

1. Write Simple IoT LED program. ANS:









1. **Explain drawback IoT. ANS:**
2. Increased tracking and privacy issues

All that data pouring in from IoT devices goes somewhere. “There is a tremendous treasure trove of data about us that is outside of our control,” Mustac points out, adding that this data can be misused.

Navigating secure and ethical usage of all that data is a huge deal, and it’s now a subject of regulation at the federal level. The debate around how companies should be allowed to access and utilize user data is ongoing.

1. More weaknesses in network security

On top of concerns over what a company can legally do with IoT data they collect, there are also concerns with illegal access.

“The biggest drawback to IoT has been the lack of security in many devices,” Wills says. “Some manufacturers treat security as an afterthought rather than the essential component it is.” She explains that many IoT devices have glaring vulnerabilities like hardcoded passwords and outdated software components that attackers can easily bypass to gain a foothold in your network. With an ever- growing number of internet-enabled devices, it’s easy to see how this can quickly become a massive problem.

These risks can be alleviated with better protocols, according to Therese Schachner, cybersecurity consultant at VPN Brains. She says secure user authentication and data encryption in IoT devices go a long way.

It’s safe to say that companies and consumers alike want to know the devices that can both see and hear in their boardrooms an

homes are not streaming to just anyone out there. This makes cybersecurity positions more critical than ever.

1. More required bandwidth

The more internet-connected things you have in an environment, the more bandwidth they are going to demand. “As a result, devices on the shared network may experience slower internet speeds,” Schachner says. Since many people are already struggling with the amount of bandwidth they have access to, this can be a serious drawback to IoT implementation.

“The widespread adoption of IoT devices requires networks to be able to support a substantial number of additional connections.”

1. Increased monitoring time

The bandwidth issue also relates to professionals and the time they may have to spend keeping an eye on IoT devices. While it’s unlikely to be a time-drain for individuals with a few home devices, cyber security professionals could find themselves totally bogged down in logging and monitoring for corporate IoT devices, according to Wills.

“Very soon, SOC (security operations center) analysts will likely find themselves triaging alerts from thermostats and coffee makers.”

The future of the internet of things

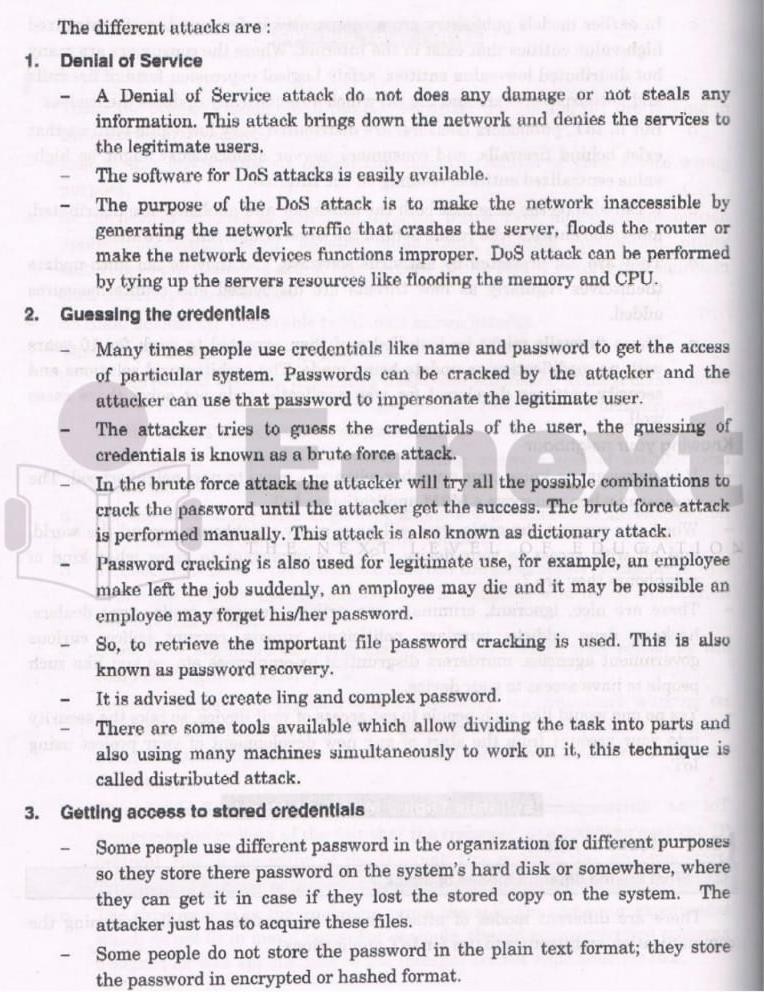
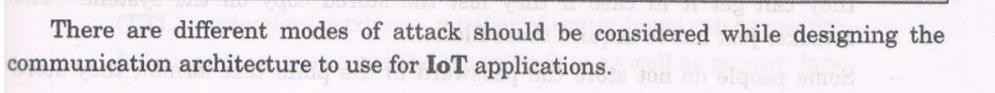
All in all, the internet of things is rife with innovation and potential— and the landscape is changing rapidly. “The possibilities for automation are limitless, and we’re still very much in the early phases of putting IoT to work for us,” Wills says. She points out that even “dumb” appliances can get an upgrade with other devices.

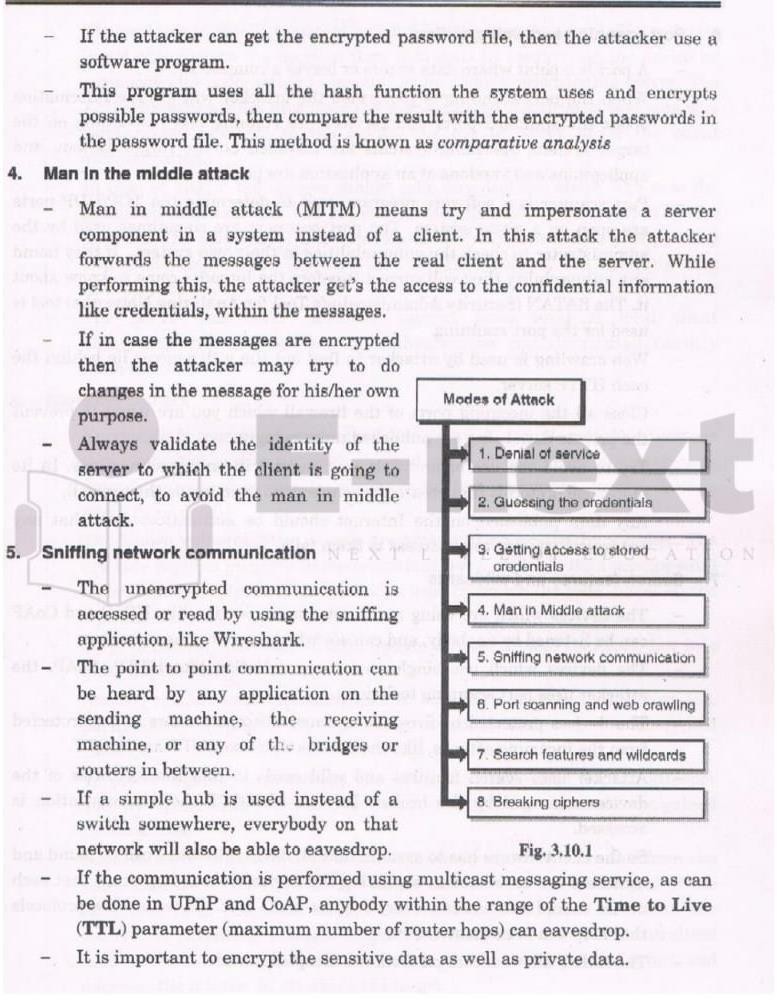
“And there is more to come. Within the next decade, we’ll have IoT devices involved in automated processes we can’t even imagine right now.”

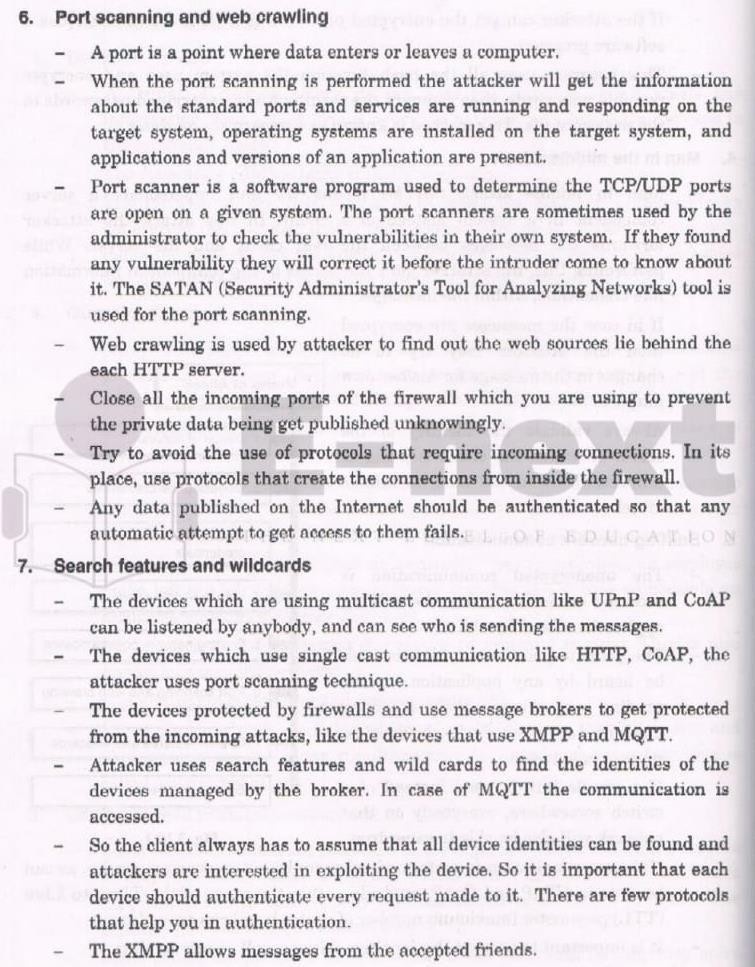
It’s no surprise to anyone that the demand for IoT security roles like penetration tests have been on the rise, Wills says. “This presents a great opportunity for new information security professionals to carve out a niche for themselves in the industry.”

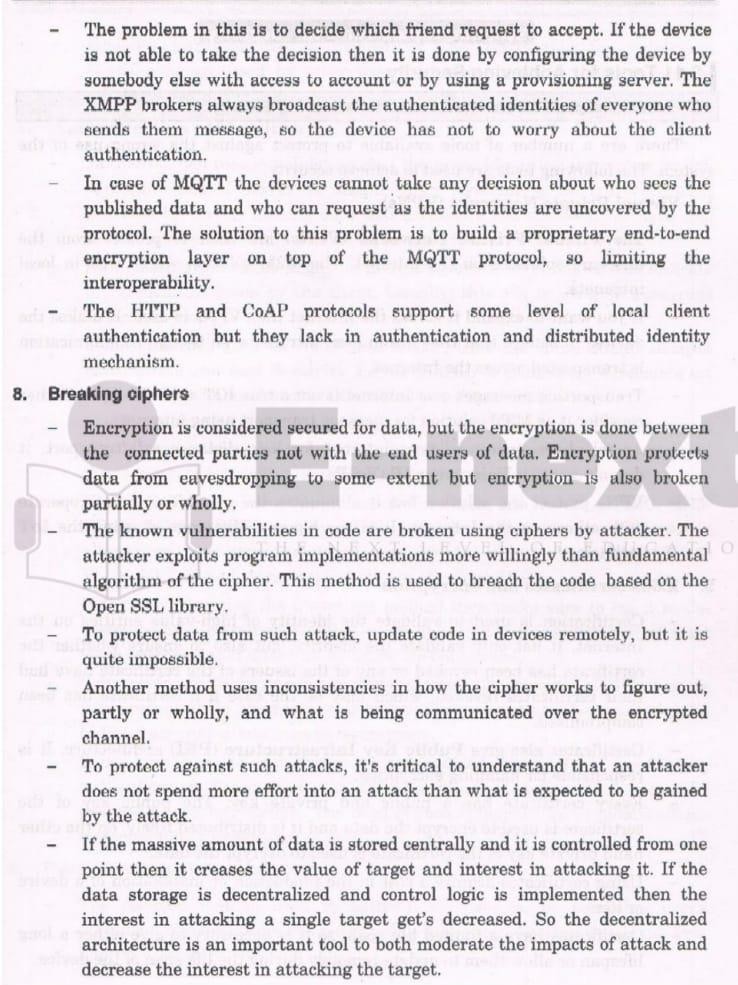
And the internet of things isn’t the only hot cyber security battleground at the moment. The digital landscape is unfolding in so many different directions at once that companies are scrambling to keep up. Check out “9 Cyber Security Problems Nearly Every Organization Struggles With” to find out why.

1. Explain mode of attack. ANS:

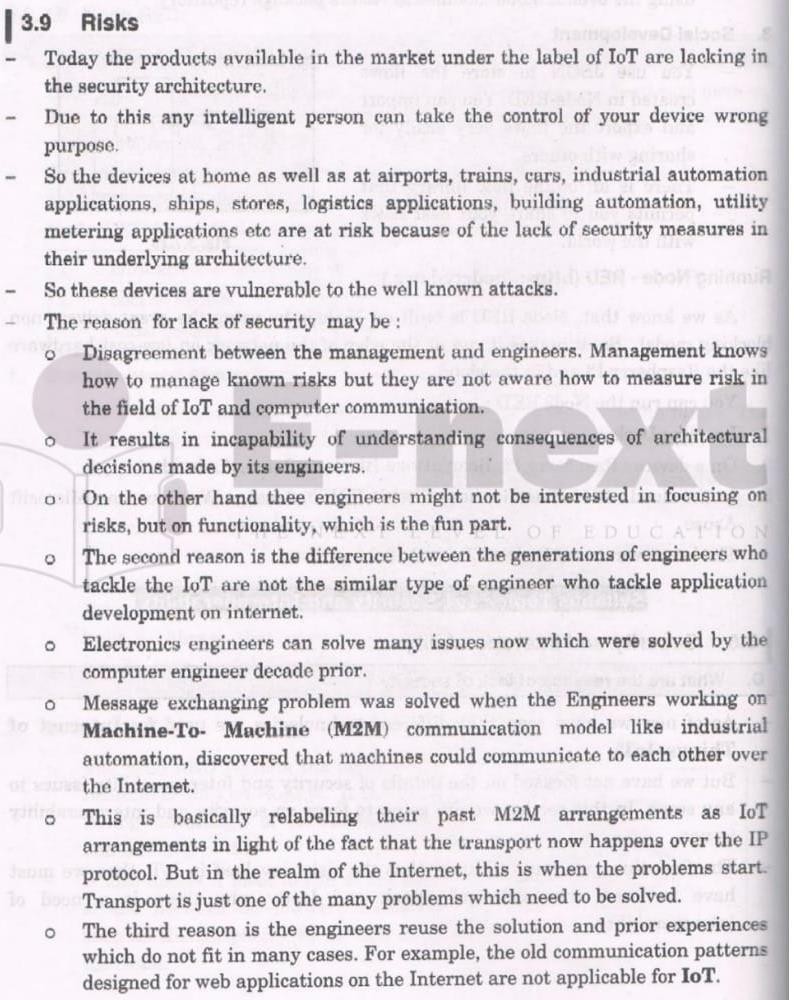


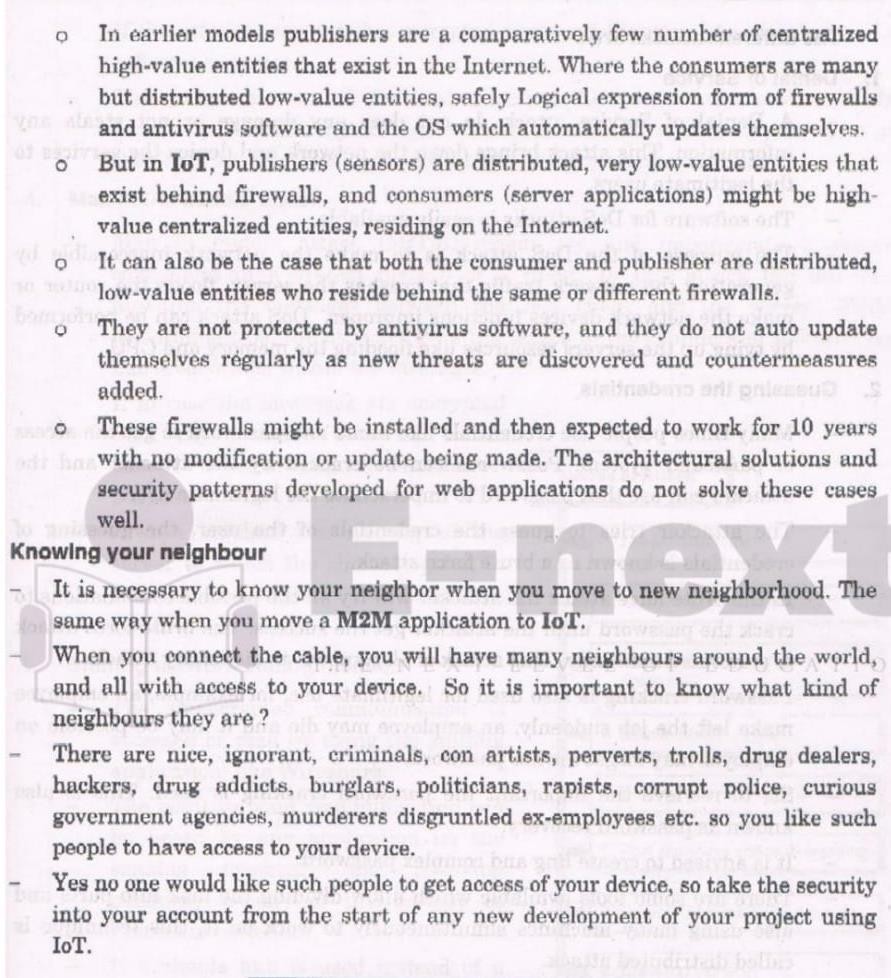






* 1. **Explain IoT risks. ANS:**





* 1. Explain security system IoT

**ANS:** Internet of Things (IoT) devices are computerized Internet- connected objects, such as networked security cameras, smart refrigerators, and WiFi-capable automobiles. IoT security is the process of securing these devices and ensuring they do not introduce threats into a network.

Anything connected to the Internet is likely to face attack at some point. Attackers can try to remotely compromise IoT devices using a variety of methods, from credential theft to vulnerability exploits.

Once they control an IoT device, they can use it to steal data, conduct distributed denial-of-service (DDoS) attacks, or attempt to compromise the rest of the connected network.

IoT security can be particularly challenging because many IoT devices are not built with strong security in place — typically, the manufacturer's focus is on features and usability, rather than security, so that the devices can get to market quickly.

IoT devices are increasingly part of everyday life, and both consumers and businesses may face IoT security challenges.

DDoS attacks: Malicious parties often use unsecured IoT devices to generate network traffic in a DDoS attack. DDoS attacks are more powerful when the attacking parties can send traffic to their target from a wide range of devices. Such attacks are harder to block because there are so many IP addresses involved (each device has its own IP address). One of the biggest DDoS botnets on record, the Mirai botnet, is largely made up of IoT devices.

What are some of the main aspects of IoT device security…

**Software and firmware updates**: IoT devices need to be updated whenever the manufacturer issues a vulnerability patch or software update. These updates eliminate vulnerabilities that attackers could

exploit. Not having the latest software can make a device more vulnerable to attack, even if it is outdated by only a few days. In many cases IoT firmware updates are controlled by the manufacturer, not the device owner, and it is the manufacturer's responsibility to ensure vulnerabilities are patched.

**Credential security**: IoT device admin credentials should be updated if possible. It is best to avoid reusing credentials across multiple devices and applications — each device should have a unique password. This helps prevent credential-based attacks.

**Device authentication**: IoT devices connect to each other, to servers, and to various other networked devices. Every connected device needs to be authenticated to ensure they do not accept inputs or requests from unauthorized parties.

For example, an attacker could pretend to be an IoT device and request confidential data from a server, but if the server first requires them to present an authentic TLS certificate (more on this concept below), then this attack will not be successful.

For the most part, this type of authentication needs to be configured by the device manufacturer.

**Encryption**: IoT device data exchanges are vulnerable to external parties and on-path attackers as they pass over the network — unless encryption is used to protect the data. Think of encryption as being like an envelope that protects a letter's contents as it travels through the postal service.

Encryption must be combined with authentication to fully prevent on-path attacks. Otherwise, the attacker could set up separate encrypted connections between one IoT device and another, and neither would be aware that their communications are being intercepted